Above Property Security Policies, Standards, and Procedures

Security Policies, Standards, and Procedures

Above Property Systems, LLC.

None

Table of contents

1. APS Security Policies, Standards, and Procedures

2. Security Program Overview

`Last Reviewed: 2025-02-17:19:44:43-UTC`

APS is committed to protecting its employees, partners, clients/customers and the company itself from damaging acts either malicious or unintentional in nature. This includes implementation of policies, standards, controls and procedures to ensure the Confidentiality, Integrity, and Availability of systems and data according to their risk level.

The APS security program and policies are developed on the principles that (1) security is everyone's responsibility and (2) self-management is best encouraged by rewarding the right behaviors.

Tldr

Quick Reference / Employee Handbook

2.1 Controls and Procedures

2.2 Information Security Program and Scope

APS has developed a security program and implemented controls to meet and exceed all compliance requirements, including PCI, NIST, and applicable industry best practices.

On a high level, APS's information security program covers:

1. Inventory and protection of all critical assets
2. Visibility into and the management of data lifecycle, from creation to retention to deletion
3. Protection of data-at-rest, data-in-transit, and data-in-use
4. Segmented network architecture
5. Automated security configuration and remediation
6. Centralized identity and access management
7. Secure product development
8. Continuous monitoring and auditing
9. Validated plan and practice for business continuity, disaster recovery, and emergency response
10. End-user computing protection and awareness training

More information about the APS Security and Privacy program can be found at https://compliance.aboveproperty.com and https://compliance.aboveproperty.com/privacy-policy/.

The information security program and its policies and procedures cover all APS workforce members, including full-time and part-time employees in all job roles, temporary staff, contractors and subcontractors, volunteers, interns, managers, executives employees, and third parties.

2.3 Understanding the Policies and Documents

Policies are written in individual documents, each pertaining to a specific domain of concern.

Each document starts with the current version number and/or last updated date, followed by a brief summary. The remaining of the document is structured to contain two main sections:

- Policy Statements
- Controls and Procedures

All policy documents are maintained, reviewed, updated and approved following standards and procedures outlined in Policy Management.

2.4 Review and Reporting

The information security program, policies, procedures and controls are reviewed on a regular basis internally by cross functional team members and externally by qualified assessors.

3. Corporate Governance

`Last Reviewed: 2025-02-17:19:44:43-UTC`

Above Property® is an advanced global travel solution delivered via an always-on multi-cloud, module based platform.

Our vision is to solve the technology and business constraints of today’s legacy based CRS, CCM, RMS, Channel Managers and PMS by leveraging our groundbreaking multi-tenant, rules-based, big-data driven, global Travel Platform.

APS believes in transparent and ethical business practices, and the protection of long-term interests of its employees, customers, shareholders and other stakeholders.

APS has established a Board of Directors (Bod) and appointed qualified members and directors, such that:

- Corporate bylaws are in place that describe board members responsibilities.
- The BoD identifies and accepts its oversight responsibilities in relation to established requirements and expectations.
- Board members are evaluated on a periodic basis to help ensure their skills and expertise are suited to lead senior management and take commensurate action.
- The BoD has sufficient members who are independent from management and are objective in evaluations and decision making.
- The expectations of the BoD and/or senior management are defined and understood at all levels of the organization and its service providers and business partners.

3.1 Controls and Procedures

3.1.1 Board of Directors Responsibilities

The Board of Directors (BoD) meets monthly to discuss financials, operations, business results, strategies and planning. The BoD responsibilities include:

- Evaluate the performance of the Chief Executive Officer (CEO) and the executive management team
- Establish policies, evaluate and approve the compensation of senior management of the company
- Review succession plans and development programs for senior management
- Review and approve long-term strategic and business plans and monitor organization’s performance against the plans
- Review and approve any major risks and the risk remediation/acceptance
- Adopt policies of corporate conduct, including compliance with applicable laws, rules and regulations, maintenance of accounting, financial and other controls, and reviewing the adequacy of compliance systems and controls
- Evaluate the overall effectiveness of the Board and its committees and the individual directors on a periodic basis
- Adopt and implement best practices of corporate governance in full conformity with the letter and spirit of all applicable laws, rules and regulations

4. Policy Management

`Last Reviewed: 2025-02-17:19:44:43-UTC`

APS implements policies and procedures to maintain compliance and integrity of data. The Security Officer is responsible for maintaining policies and procedures and assuring all APS workforce members, business associates, customers, and partners are adherent to all applicable policies. Previous versions of policies are retained at https://github.com/aboveproperty/security-policies to assure ease of finding policies at specific historic dates in time.

4.1 Policy Statements

APS policy requires that:

(a) APS policies must be developed and maintained to adhere to security best practices, to minimally meet the requirements of the following standards:

- PCI DSS 4
- GDPR
- NIST

(b) All policies must be reviewed at least annually.

(c) All policy changes must be approved by APS Security Officer. Additionally,

- Major changes may require approval by APS CEO or designee;
- Changes to policies and procedures related to product development may require approval by the Head of Engineering.

(d) All policy documents must be maintained with version control, and previous versions must be retained for a defined, predetermined timeframe.

(e) Policy exceptions are handled on a case-by-case basis.

- All exceptions must be fully documented with business purpose and reasons why the policy requirement cannot be met.
- All policy exceptions must be approved by both APS Security Officer and COO.
- An exception must have an expiration date no longer than one year from date of exception approval and it must be reviewed and re-evaluated on or before the expiration date.

4.2 Controls and Procedures

4.2.1 Policies and Controls Framework

APS maintains a set of policies and controls that captures standards, regulatory, legal, and statutory requirements relevant to the business needs. The framework and its contents are reviewed at least annually to ensure changes that could affect the business processes are reflected.

Structure

Similar to the concept of “micro-services”, the policies and control procedures are written in individual “micro-docs”. They are mapped to each other via a JSON configuration.

Controls Mapping

A JSON document configures the mapping of each control procedure to one or more security/compliance frameworks, as applicable.

Note that the controls mapping is only between a control/procedure document to the requirement, not at the policy level. This is because we strongly believe that you must have documented controls and procedures to implement and enforce a high level written policy. Having a written policy by itself without implementation or enforcement does not address the risk of any security or compliance requirement.

Compliance standards

At least once a year, APS reviews the regulatory, legal, and statutory requirements relevant to its business needs and adopts any relevant standards into its controls framework and governance program.

The list of applicable standards can be found it the same repository as the policies and controls documentation and/or in the Above Property compliance management application/platform.

4.2.2 Policy Management Process

Document Structure

Policies are written in individual documents, each pertaining to a specific domain of concern.

Each document starts with the current version number in the format of `YYYY.#` (e.g. `2017.1`), followed by a brief summary. The remaining of the document is structured to contain the following subsections:

- Policy Statements
- Applicable Standards
- Controls and Procedures

Versioning

Each APS policy document contains a version and optionally a revision number. The version number is the four digit year followed by a number, to indicate the year and sequence number of the policy at which time it was written or updated.

The version number shall be incremented by one with each material change to the policy content. For example, if a new policy statement is added or a technical control/procedure is updated to `2017.1` version of a policy, the new version should be numbered `2017.2`.

The policy document may also include a revision number, in the format of `rev.#`, immediately following the main version number. A revision number indicate minor, non-material changes to the document, such as formatting changes, fixing typos, or adding minor details.

Numbering

If sequencing numbers are included in the policy headings:

- Policy may be referenced by its statement number, such as `§2.1(a)`, in internal/external communications as well as in other APS policies or technical/business documentation for cross reference.
- As such, to maintain cross referencing integrity, starting from version `2017.2`, all numbering shall remain intact for policy documents and statements.
- When updating, avoid reordering and renumbering of policy documents and statements. For example:
- Append at the end of the list by adding new statement(s) as needed instead of inserting.
- If a policy or policy statement is no longer applicable, mark it deprecated instead of removing the file or statement completely.

Review and Maintenance of Policies

1. All policies are stored and up to date to maintain APS best practice. Updates and version control are done similar to source code control.

2. Policy update requests can be made by any workforce member at any time. Furthermore, all policies are reviewed annually by the Security and Privacy Officer to assure they are accurate and up-to-date.
3. APS employees may request changes to policies using the following process:

a. The APS employee initiates a policy change request by creating an Issue in the Rally Security project. The change request may optionally include a GitHub pull request from a separate branch or repository containing the desired changes.

b. The Security Officer is assigned to review the policy change request.

c. Once the review is completed, the Security Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review and documentation.

d. If the review is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.

e. If the policy change requires technical modifications to production systems, those changes are carried out by authorized personnel using APS's change management process.

f. If the change results in a new version instead of a new revision (see §3.3.1 for definitions), the current version of the policy document(s) must be saved to archive under the corresponding version number prior to the new policy being adopted/published and prior to merging the pull request containing the changes. This allows easy reference to previous versions if necessary.

> **Important**
>
> - Changes are made on the `drafts` (or equivalent) branch instead of on the `master` branch for commits.
> - If multiple authors are working on the changes, additional separate branches and pull requests may be necessary before changes are merged in `drafts`.
> - Changes must not be merged to `master` without the approval of the Security Officer.
> - Changes must not be merged to `master` without archiving the existing version of policy document(s), unless the change is a minor revision.
> - Once the changes are final and approved, a pull request shall be created from the `drafts` branch to the `master` branch and all members of the development team shall be included as approvers. This serves as communication and training of policy updates to the development organization, and the pull request approvals serve as records of training received.
> - Policy update communication and training for non-development staff is conducted separately by the Security team.

4. All policies are made accessible to all APS workforce members. The current master policies are published at https://compliance.aboveproperty.com.

- Changes are automatically communicated to all APS team members through integrations between GitHub and Slack that log changes to a predefined APS Slack Channel.
- The Security Officer also communicates policy changes to all employees via email. These emails include a high-level description of the policy change using terminology appropriate for the target audience.

5. All policies, and associated documentation, are retained for 7 years from the date of its creation or the date when it last was in effect, whichever is later

a. Version history of all APS policies is done via GitHub.

b. Backup storage of all policies is done with AWS S3 and/or internal file share (e.g. Microsoft Office365 SharePoint or Box).

6. The policies and information security policies are reviewed and audited annually, or after significant changes occur to APS's organizational environment, by the security committee members. Issues that come up as part of this process are reviewed by APS

management to assure all risks and potential gaps are mitigated and/or fully addressed. The process for reviewing polices is outlined below:

a. The Security Officer initiates the policy review by creating an Issue in the Rally Security project or via a Pull Request (PR).

b. The Security Committee members and additional reviewers are notified by email or via the PR to review the current policies.

c. If changes are made, the above process is used. All changes are documented in the Issue/PR.

d. Once the review is completed, the Security Officer approves or rejects the Issue/PR. If the Issue/PR is rejected, it goes back for further review and documentation.

e. If the review is approved, the Security Officer then marks the Issue as Done, or merges the PR into master branch, adding any pertinent notes required.

f. Policy review is monitored using Rally or GitHub reporting to assess compliance with above policy.

Additional documentation related to maintenance of policies is outlined in Roles and Responsibilities.

5. Security Architecture and Operating Model

`Last Reviewed: 2025-02-17:19:44:43-UTC`

In the digital age, cyber attacks are inevitable. At APS, we are taking a “zero trust”, “minimal infrastructure” approach to managing risk and information security.

This document describes our guiding principles and aspirations in managing risk and the building blocks of our security model.

5.1 Policy Statements

APS policy requires that:

(a) APS’s security program and operations should be designed and implemented with the following objectives and best practices:

- data-centric, cloud-first
- assume compromise therefore never trust, always verify
- apply controls using least-privilege and defense-in-depth principles
- avoid single point of compromise
- automate whenever possible, the simpler the better, less is more
- prompt self management and reward good behaviors

(b) Security shall remain a top priority in all aspects of APS’s business operations and product development.

5.2 Controls and Procedures

5.2.1 APS Security Principles

(1) Data-centric model; zero-trust architecture

“Zero Trust” is a data-centric security design that puts micro-perimeters around specific data or assets so that more granular rules can be enforced. It remedies the deficiencies with perimeter-centric strategies and the legacy devices and technologies used to implement them. It does this by promoting “never trust, always verify” as its guiding principle. This differs substantially from conventional security models which operate on the basis of “trust but verify.”

In particular, with Zero Trust there is no default trust for any entity — including users, devices, applications, and packets— regardless of what it is and its location on or relative to the corporate network. In addition, verifying that authorized entities are always doing only what they’re allowed to do is no longer optional; it’s now mandatory.

Summary

- No internal network. (Almost) 100% cloud.
- Fully segregated with Granular policy enforcements.
- Individually secured devices. No production access by default.

(2) “Air-Gapped” environments meet short-lived processes

We extend the zero-trust security model with a “Minimal Infrastructure” approach, where we use “Anything-as-a-Service” whenever possible, to harness the full power of the cloud. Cloud services allow us to contain and control access at a much more granular level, compared to operating on-premise infrastructure. Via access to the extensive APIs provided by the cloud services, we would be able to more easily integrate and automate security operations. Additionally, minimizing infrastructure significantly reduces always-on attack surfaces. Services that are not used are turned off, instead of being idly available which opens itself up

to attacks. Together with Zero Trust, this security model and architecture enables a high degree of flexibility for end-user computing while maintaining the highest level of security assurance.

Summary

- No direct administrative or broad network connectivity into production.
- Processes are short-lived and killed after use.
- Minimal persistent attack surface making it virtually impenetrable.

(3) Least-privilege temporary access

Cyber attacks are inevitable. When it comes to preparing for potential attacks, APS security operations take the approach that assumes a compromise can happen at any time, to any device, with little to no indicators. This is also an extension of the “zero trust” model. When building security operations, we carefully perform risk analysis and threat model, to identify potential single point of compromise and to avoid having the “keys to the kingdom”.

In other words, compromise of any single system or user or credential, should not easily lead to a broad or full compromise of the entire infrastructure or operations. For example, if an attacker gains access to a admin credential (e.g. Active Directory domain), it should not directly lead to the compromise of all systems and data in the environment.

Summary

- Need-based access control for both employees and computing services.
- Access to critical systems and resources are closed by default, granted on demand.
- Protected by strong multi-factor authentication.
- No “keys to the kingdom”; no single points of compromise.
- “Secrets” (such as SSH Keys) must remain secret at all times.

(4) Immutable builds and deploys

The APS platform leverages a micro-service architecture. This means that the system has been decomposed into numerous small components that can be built and deployed individually. Before these components get deployed to our *production* environments, we thoroughly test and validate the changes in our *lower* environments which are completely isolated from production. This allows us to test upcoming changes while ensuring there is no impact to our customers.

As a particular build of a component progresses through our environments, it is important that the build does not change thus we ensure that each build is immutable. Once an *immutable build* has been validated in our *lower* (non-production) environments, we then deploy it to our *production* environment where the change will be available to APS customers and end-users.

Changes to our infrastructure (database schema changes, storage buckets, load balances, DNS entries, etc.) are also described in our source code and deployed to our environments just like the applications. This architectural approach to managing infrastructure is referred to as *infrastructure as code* and is a key requirement for fully automated deployments with minimal human touch.

Summary

- Infrastructure as code with active protection.
- Automated security scans and full traceability from code commit to production.
- “Hands-free” deployment ensures each build is free from human error or malicious contamination.

(5) End-to-end data protection and privacy

It is of the utmost importance that APS provides for confidentiality (privacy), integrity and availability of its customer's data. Your data is protected with end-to-end encryption, combined with strong access control and key management. We also prohibit our internal employees to access customer data directly in production. So your data remains safe and private at all times. We will never use or share your data without your prior consent.

We are proud to offer our customers data storage peace of mind with a money-back guarantee. We guarantee your private data stored on our platform is always safe and protected from cyberattacks such as ransomware, and we will reimburse you for certain losses of such data due to unauthorized activity in eligible accounts that resulted through no fault of your own.

Summary

- Data is safe both at rest and in transit, using strong encryption, access control and key management.
- No internal user access is allowed to customer data in production.

(6) Strong yet flexible user access

We all know by now that "Passw0rd" makes a terrible password. Access control is so important we must get it right. That's why we leverage tried-and-true technology such as SAML, OAuth, multi-factor authentication, and fine-grained authorization to provide strong yet intuitive access options, both for our internal staff to access business resources and for our customers to access APS platform and services.

Summary

- OAuth 2.0, OpenID Connect, SAML for customer authentication and single sign-on.
- Multi-factor authentication.
- Fine-grain attribute-based or role-based authorization.

(7) Watch everything, even the watchers

You can't protect what you can't see.

As the famous strategist, Sun Tzu, once said, "Know thy self, know thy enemy. A thousand battles, a thousand victories." It all starts with knowing ourselves. This applies to the infrastructure, environments, operations, users, systems, resources, and most importantly, data. It is important to inventory all assets, document all operations, identify all weaknesses, and visualize/understand all events.

This includes conducting various risk analysis, threat modeling, vulnerability assessments, application scanning, and penetration testing. Not only that, this requires security operations to keep an eye on everything, and someone should also "watch the watchers".

At first, this would require significant manual effort and may seem impossible to keep up-to-date. Our goal is to automate security operations, so that this can be achieved programmatically as our operations evolve to become more complex.

Additionally, APS security team will actively monitor threat intelligence in the community, with feeds and information sharing platform such as NH-ISAC to stay abreast of the attacker activities and methodologies.

Summary

- All environments are monitored; All events are logged; All alerts are analyzed; All assets are tracked.
- No privileged access without prior approval or full auditing.
- We deploy monitoring redundancy to "watch the watchers".

(8) Centralized and automated operations

As much as possible, APS security will translate policy and compliance requirements into reusable code for easy implementation and maintenance. This allows us to truly be able to enforce policy and compliance in a fast and scalable way, rather than relying solely on written policies and intermittent manual audits. For example, end-point device policies may be translated into Chef InSpec code and compliance may be enforced through the agent. Access Control policies for production environments are translated into AWS IAM JSON policies and implemented via Infrastructure as Code (IaC).

Automation makes it truly possible to centralize security operations, including not only event aggregation and correlation, but also the orchestration and management of previously siloed security controls and remediation efforts.

Summary

- API-driven cloud-native security fabric that
- centrally monitors security events,
- visualizes risk management,
- automates compliance audits, and
- orchestrates near real-time remediation.

(9) Usable security

Security benefits from transparency, and should operate as an open-book. This allows the entire organization to take responsibility for and accountability of adopting security best practices. Similar to code reviews and pull requests in the development process, APS security team makes security standards and practices available to all employees for feedback prior to adoption.

We emphasize on the usability and practicality of security. A security solution or process is not effective, if it is not being used, no matter how good it may be. Having impractical security would only generate noise, provide a false sense of security, and incur unnecessary cost. Nothing is perfect, but we embrace an agile mindset to test and try, and to continuously improve.

Summary

- All employees receive security awareness training not annually, but monthly.
- Simple policies, processes, and procedures.
- No “Shadow IT”.
- DevSecOps with common goals and an integrated team.
- Processes that encourage self management and reward good behavior.

(10) Regulatory compliant and hacker verified

Security != Compliance. We cannot have one without the other.

Summary

- Regulatory Compliant;
- Independently assessed and certified;
- Hacker verified.

5.2.2 Security Architecture

APS developed a security architecture on top of its three main infrastructure environments - Cloud (AWS), DevOps, and workforce collaboration / end-user computing.

Architecture Diagrams

Detailed architecture diagrams of the in-scope networks, endpoints, applications as well as the security operations are developed and maintained by Above Property.

Cloud Architecture

CLOUD NATIVE

- Designed for the cloud using true multi-tenant architecture
- Auto scaling across multiple data centers in multiple regions around the world
- APS services deployed inside private subnets of Virtual Private Cloud (VPC)
- Comprehensive security and compliance via AWS certifications
- Ongoing security testing by AWS and AWS customers

CUSTOMER BENEFITS

- Infrastructure is tailored to our customer’s goals and usage patterns
- “Shared use” model reduces cost
- Nearly infinite compute and data capacity via AWS cloud provider
- Customers can focus on solving business problems and not worry about infrastructure
- Automatic backup and recovery
- Continuous improvements via change control process
- Faster adoption of new technology

EVOLUTION OF CLOUD COMPUTING

1. Baremetal
   - A computer in someone else’s data center
2. Virtual Machine
   - A portion of a computer in someone else’s data center
   - In AWS, a Virtual Machine is created from Amazon Machine Image (AMI)
3. Container
   - A package of essential application libraries and code but not the core OS libraries - Simpler to scale a docker image because - No duplication of core OS processes (networking, filesystem, etc) - Typically a Docker container
4. Function
   - Just the application code that runs in a pre-built container

APS strives to leverage functions as the primary building blocks for our platform because:

- functions deploy more quickly than containers and virtual machines
- AWS automatically scales Lambda functions based on the number of incoming invocations
- they are short-lived processes which minimizes attack surface

5.2.3 Metrics, Measurements and Continuous Monitoring

A set of metrics / KPIs have been defined to assist in the measuring, reporting and optimizing the security program and the controls in place.

A security scorecard is produced every with updates to key metrics of the APS information security program, to measure its adoption and effectiveness.

The reports and scorecards are maintained by and can be accessed at Above Property.

5.2.4 Quality of Service

APS strives to provide a high quality of service to all of its customers. This is accomplished through a security architecture that encompasses all of APS’s operations and provides high data confidentiality, integrity, and availability.

An overview of APS’s architecture can be found in Security Architecture. APS uses a highly scalable cloud architecture to provide system quality at all times.

All systems are monitored and measured in real time.

APS uses DevOps methodology as described in Software Development Process to ensure a smooth delivery process of all systems and applications.

6. Roles, Responsibilities and Training

`Last Reviewed: 2025-02-17:19:44:43-UTC`

Security and compliance is everyone’s responsibility. APS is committed to ensuring all workforce members actively address security and compliance in their roles. Statistically, cybersecurity breaches typically start with compromise of end-user computing devices, social engineering, human error or insider threat. Therefore, users are the first line of defense and yet usually the weakest link. As such, training is imperative to assuring an understanding of current best practices, the different types and sensitivities of data, and the sanctions associated with non-compliance.

In this and all related policy documents, the term “employees” and “workforce members” may be used interchangeably to include all full-time and part-time employees in all job roles, contractors and subcontractors, volunteers, interns, managers and executives at APS.

The Security Officer is responsible for facilitating the development, testing, implementation, training, and oversight of all activities pertaining to APS’s efforts to be compliant with the applicable security and compliance regulations and industry best practices. The intent of the Security Officer Responsibilities is to maintain the confidentiality, integrity, and availability of critical and sensitive data. The Security Officer reports to the Board of Directors and/or the CEO.

APS has appointed Pete Ehlke as the Security Officer.

APS has appointed as the Data Protection Officer responsible for all GDPR-related affairs.

An official **Security Committee** has been formed, chaired by the Security Officer, and represented by the select members of the IT team (Security Officer, CTO, CIO, COO, CEO).

6.1 Policy Statements

APS policy requires that:

(a) A Security Officer must be appointed to assist in maintaining and enforcing safeguards towards security, compliance, and privacy.

Additionally, a Data Protection Officer must be appointed to fulfill the tasks and responsibilities specified in GDPR.

(b) Security and compliance is the responsibility of all workforce members (including employees, contractors, interns, and managers/executives). All workforce members are required to:

- Complete all required security trainings, including annual regulatory compliance training, security awareness, and any additional role-based security training as part of the ongoing security awareness program and as required by job role.
- Follow all security requirements set forth in APS security policy and procedures, including but is not limited to access control policies and procedures and acceptable use policy for end-user computing.
- See something, say something: follow the incident reporting procedure to report all suspicious activities to the security team.

(c) All workforce members are required to report non-compliance of APS’s policies and procedures to the Security Officer or designee. Individuals that report violations in good faith may not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

(d) All workforce members are required to cooperate with federal, state and local law enforcement activities and legal investigations. It is strictly prohibited to interfere with investigations through willful misrepresentation, omission of facts, or by the use of threats against any person.

(e) Workforce members found to be in violation of this policy will be subject to sanctions.

(f) Segregation of Duties shall be maintained when applicable to ensure proper checks and balances and minimize conflict of interests. This helps reduces the possibility of fraud and insider threat considerably, and eliminates single points of compromise to critical systems.

6.2 Controls and Procedures

6.2.1 Assignment of Roles and the Security Committee

APS has appointed Pete Ehlke as the Security Officer.

The security committee is chaired by the Security Officer, and represented by the select members of the senior leadership team, including Security Officer, CTO, CIO, COO, CEO, in addition to the Security Officer.

General Responsibilities of the Security Officer

The authority and accountability for APS's information security program and privacy program is delegated to the Security and Privacy Officer. The Security Officer and the security team are required to perform or delegate the following responsibilities:

- Build and maintain security and privacy program to satisfy regulatory and contractual requirements.
- Establish, document, distribute and update security policies, standards and procedures.
- Oversee, enforce and document all activities necessary to maintain compliance and verifies the activities are in alignment with the requirements;
- Monitor, analyze, distribute and escalate security alerts and information.
- Develop and maintain security incident response and escalation procedures to ensure timely and effective handling of all situations.
- Administer user accounts, including additions, deletions, and modifications.
- Monitor and control all access to critical systems and data.
- Perform risk assessment, remediation, and ongoing risk management.
- Provide regular security awareness and compliance training, as well as periodic security updates and reminder communications for all workforce members.
- Maintains a program that incentivizes right behaviors, supports timely and proper reporting and investigation of violations, implements effective and practical mitigation, and applies fair sanctions when necessary.
- Assist in the administration and oversight of business associate agreements.
- Facilitate audits to validate compliance efforts throughout the organization.
- Work with the CFO to ensure that any security objectives have appropriate consideration during the budgeting process.

Workforce Supervision Responsibilities

Although the Security Officer is responsible for implementing and overseeing all activities related to maintaining compliance, it is everyone's responsibility (i.e. team leaders, supervisors, managers, co-workers, etc.) to supervise all workforce members and any other user of APS's systems, applications, servers, workstations, etc. that contain sensitive data.

1. Monitor workstations and applications for unauthorized use, tampering, and theft and report non-compliance according to the Security Incident Response policy.
2. Assist the Security Officers to ensure appropriate role-based access is provided to all users.
3. Take all reasonable steps to hire, retain, and promote workforce members and provide access to users who comply with the Security regulation and APS's security policies and procedures.

Segregation of Duties

APS has dedicated team/personnel assigned the job function of security and compliance. Segregation of duties are achieved via a combination of assignment of roles and responsibilities to different personnel, and automation enforcement for software-defined processes.

Checks and balances are ensured via such segregation of duties and related review/approval processes. When applicable, reviews and approvals must be obtained from designated personnel separate from the individual performing the work.

6.2.2 Policy and Compliance Training

1. The Security Officer facilitates the training of all workforce members as follows:

a. New workforce members within their first month of employment;

b. Existing workforce members annually;

c. Existing workforce members whose functions are affected by a material change in the policies and procedures, within a month after the material change becomes effective;

d. Existing workforce members as needed due to changes in security and risk posture of APS.

2. Documentation of the training session materials and attendees is retained for a minimum of seven years.

3. The training session focuses on, but is not limited to, the following subjects defined in APS's security policies and procedures:

a. SOC 2 Security Principals and Controls;

b. NIST Security Rules;

c. PCI DSS requirements;

d. Risk Management procedures and documentation;

e. Auditing. APS may monitor access and activities of all users;

f. Workstations may only be used to perform assigned job responsibilities;

g. Users may not download software onto APS's workstations and/or systems without prior approval from the Security Officer;

h. Users are required to report malicious software to the Security Officer immediately;

i. Users are required to report unauthorized attempts, uses of, and theft of APS's systems and/or workstations;

j. Users are required to report unauthorized access to facilities

k. Users are required to report noted log-in discrepancies (i.e. application states users last log-in was on a date user was on vacation);

l. Users may not alter sensitive data maintained in a database, unless authorized to do so by a APS Customer;

m. Users are required to understand their role in APS's contingency plan;

n. Users may not share their user names nor passwords with anyone;

o. Requirements for users to create and change passwords;

p. Users must set all applications that contain or transmit sensitive data to automatically log off after 15 minutes of inactivity;

q. Supervisors are required to report terminations of workforce members and other outside users;

r. Supervisors are required to report a change in a users title, role, department, and/or location;

s. Procedures to backup sensitive data;

t. Procedures to move and record movement of hardware and electronic media containing sensitive data;

u. Procedures to dispose of discs, CDs, hard drives, and other media containing sensitive data;

v. Procedures to re-use electronic media containing sensitive data;

w. Secrets management (such as SSH key) and sensitive document encryption procedures.

6.2.3 Ongoing Awareness Training

APS leverages KnowBe4 to deliver innovative, fun and engaging security awareness contents to all employees monthly. This security awareness training shall include modules on

- phishing,
- social engineering,
- proper internet use (social media, email, clicking, etc),
- access control (proper passwords, 2FA, screen locking, etc),
- mobile device security,
- data protection, and
- system security (anti-malware, patches, secure configuration, etc).

Progress is tracked individually for each employee and reported on KnowBe4’s cloud-managed learning platform.

7. Risk Management

`Last Reviewed: 2025-02-17:19:44:43-UTC`

This policy establishes the scope, objectives, and procedures of APS's information security risk management process. The risk management process is intended to support and protect the organization and its ability to fulfill its mission.

7.1 Policy Statements

APS policy requires that:

(a) A thorough risk assessment must be conducted to evaluate the potential threats and vulnerabilities to the confidentiality, integrity, and availability of sensitive, confidential and proprietary electronic information it stores, transmits, and/or processes.

(b) Risk assessments must be performed with any major change to APS's business or technical operations and/or supporting infrastructure, no less than once per year.

(c) Strategies shall be developed to mitigate or accept the risks identified in the risk assessment process.

(d) Maintain documentation of all risk assessment, risk management, and risk mitigation efforts for a minimum of seven years.

7.2 Controls and Procedures

7.2.1 Risk Management Objectives

APS has established formal risk analysis and risk management processes to

- identify risks that may impact its business operations or the confidentiality, integrity and availability of its critical data; and
- reduce risk to an acceptable level by implementation of mitigation controls.

Unmitigated risk above the pre-defined acceptable level must be reviewed, approved and accepted by senior management.

Acceptable Risk Levels

Risks that are either low impact or low probability are generally considered acceptable.

All other risks must be individually reviewed and managed.

7.2.2 Risk Management Process

Risk analysis and risk management are recognized as important components of APS's corporate compliance and information security program.

Risk assessments are done throughout product life cycles:

- Before the integration of new system technologies and before changes are made to APS physical and technical safeguards; and (Note that these changes do not include routine updates to existing systems, deployments of new systems created based on previously configured systems, deployments of new Customers, or new code developed for operations and management of the APS Platform)
- While making changes to APS physical equipment and facilities that introduce new, untested configurations.

APS performs periodic technical and non-technical assessments of the security rule requirements as well as in response to environmental or operational changes affecting the security of sensitive data.

APS implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:

1. Ensure the confidentiality, integrity, and availability of all sensitive data APS receives, maintains, processes, and/or transmits for its Customers;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of Customer data and/or sensitive data;
3. Protect against any reasonably anticipated uses or disclosures of Customer data and/or sensitive data that are not permitted or required; and
4. Ensure compliance by all workforce members.

In addition, APS risk management process requires that:

1. Any risk remaining (residual) after other risk controls have been applied, requires sign off by the senior management and APS's Security Officer.
2. All APS workforce members are expected to fully cooperate with all persons charged with doing risk management work, including contractors and audit personnel. Any workforce member that violates this policy will be subject to disciplinary action based on the severity of the violation, as outlined in the APS Roles Policy.
3. The implementation, execution, and maintenance of the information security risk analysis and risk management process is the responsibility of APS's Security Officer (or other designated employee), and the identified Risk Management Team.
4. All risk management efforts, including decisions made on what controls to put in place as well as those to not put into place, are documented and the documentation is maintained for six years.
5. The details of the Risk Management Process, including risk assessment, discovery, and mitigation, are outlined in detail below. The process is tracked, measured, and monitored using the following procedures:

a. The Security Officer initiates the Risk Management Procedures by creating an Issue in Rally.

b. The Security Officer is assigned to carry out the Risk Management Procedures.

c. All findings are documented and linked to the Issue.

d. Once the Risk Assessment steps are complete, along with corresponding documentation, the Security Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review and documentation.

e. If the review is approved, the Security Officer then marks the Issue as Released, adding any pertinent notes required.

6. The Risk Management Procedure is monitored on a quarterly basis using Rally reporting to assess compliance with above policy.

Third party risk management details including procurement and systems acquisition can be found in §vendor.

Risk Management Schedule

The two principle components of the risk management process - risk assessment and risk mitigation - will be carried out according to the following schedule to ensure the continued adequacy and continuous improvement of APS's information security program:

- Scheduled Basis - an overall risk assessment of APS's information system infrastructure will be conducted annually. The assessment process should be completed in a timely fashion so that risk mitigation strategies can be determined and included in the corporate budgeting process.
- Throughout a System's Development Life Cycle - from the time that a need for a new, untested information system configuration and/or application is identified through the time it is disposed of, ongoing assessments of the potential threats to a system and its vulnerabilities should be undertaken as a part of the maintenance of the system.
- As Needed - the Security Officer (or other designated employee) or Risk Management Team may call for a full or partial risk assessment in response to changes in business strategies, information technology, information sensitivity, threats, legal liabilities, or other significant factors that affect APS's Platform.

Data Protection Impact Assessment (DPIA)

As required by GDPR, APS performs a data protection impact analysis as part of each risk assessment.

7.2.3 Risk Assessment and Analysis

The intent of completing a risk assessment is to determine potential threats and vulnerabilities and the likelihood and impact should they occur. The output of this process helps to identify appropriate controls for reducing or eliminating risk.

- Step 1. System Characterization
- The first step in assessing risk is to define the scope of the effort. To do this, identify where sensitive data is received, maintained, processed, or transmitted. Using information-gathering techniques, the APS Platform boundaries are identified.
- Output - Characterization of the APS Platform system assessed, a good picture of the Platform environment, and delineation of Platform boundaries.
- Step 2. Threat Identification
- Potential threats (the potential for threat-sources to successfully exercise a particular vulnerability) are identified and documented. All potential threat-sources through the review of historical incidents and data from intelligence agencies, the government, etc., to help generate a list of potential threats.
- Output - A threat list containing a list of threat-sources that could exploit Platform vulnerabilities.
- Step 3. Vulnerability Identification
- Develop a list of technical and non-technical Platform vulnerabilities that could be exploited or triggered by potential threat-sources. Vulnerabilities can range from incomplete or conflicting policies that govern an organization’s computer usage to insufficient safeguards to protect facilities that house computer equipment to any number of software, hardware, or other deficiencies that comprise an organization’s computer network.
- Output - A list of the Platform vulnerabilities (observations) that could be exercised by potential threat-sources.
- Step 4. Control Analysis
- Document and assess the effectiveness of technical and non-technical controls that have been or will be implemented by APS to minimize or eliminate the likelihood / probability of a threat-source exploiting a Platform vulnerability.
- Output - List of current or planned controls (policies, procedures, training, technical mechanisms, insurance, etc.) used for the Platform to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event.
- Step 5. Likelihood Determination
- Determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls.
- Output - Likelihood rating of low (.1), medium (.5), or high (1). Refer to the NIST SP 800-30 definitions of low, medium, and high.
- Step 6. Impact Analysis
- Determine the level of adverse impact that would result from a threat successfully exploiting a vulnerability. Factors of the data and systems to consider should include the importance to APS’s mission; sensitivity and criticality (value or importance); costs associated; loss of confidentiality, integrity, and availability of systems and data.
- Output - Magnitude of impact rating of low (10), medium (50), or high (100). Refer to the NIST SP 800-30 definitions of low, medium, and high.
- Step 7. Risk Determination
- Establish a risk level. By multiplying the ratings from the likelihood determination and impact analysis, a risk level is determined. This represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk rating also presents actions that senior management must take for each risk level.
- Output - Risk level of low (1-10), medium (>10-50) or high (>50-100). Refer to the NIST SP 800-30 definitions of low, medium, and high.

- Step 8. Control Recommendations
- Identify controls that could reduce or eliminate the identified risks, as appropriate to the organization’s operations to an acceptable level. Factors to consider when developing controls may include effectiveness of recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, and safety and reliability. Control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.
- Output - Recommendation of control(s) and alternative solutions to mitigate risk.
- Step 9. Results Documentation
- Results of the risk assessment are documented in an official report, spreadsheet, or briefing and provided to senior management to make decisions on policy, procedure, budget, and Platform operational and management changes.
- Output - A risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.

7.2.4 Risk Mitigation and Monitoring

Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the Risk Assessment process to ensure the confidentiality, integrity and availability of APS Platform data. Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of the organization consistent with its goals and mission.

- Step 1. Prioritize Actions
- Using results from Step 7 of the Risk Assessment, sort the threat and vulnerability pairs according to their risk-levels in descending order. This establishes a prioritized list of actions needing to be taken, with the pairs at the top of the list getting/requiring the most immediate attention and top priority in allocating resources
- Output - Actions ranked from high to low
- Step 2. Evaluate Recommended Control Options
- Although possible controls for each threat and vulnerability pair are arrived at in Step 8 of the Risk Assessment, review the recommended control(s) and alternative solutions for reasonableness and appropriateness. The feasibility (e.g., compatibility, user acceptance, etc.) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended controls should be analyzed. In the end, select a “most appropriate” control option for each threat and vulnerability pair.
- Output - list of feasible controls
- Step 3. Conduct Cost-Benefit Analysis
- Determine the extent to which a control is cost-effective. Compare the benefit (e.g., risk reduction) of applying a control with its subsequent cost of application. Controls that are not cost-effective are also identified during this step. Analyzing each control or set of controls in this manner, and prioritizing across all controls being considered, can greatly aid in the decision-making process.
- Output - Documented cost-benefit analysis of either implementing or not implementing each specific control
- Step 4. Select Control(s)
- Taking into account the information and results from previous steps, APS’s mission, and other important criteria, the Risk Management Team determines the best control(s) for reducing risks to the information systems and to data confidentiality, integrity, and availability. These controls may consist of a mix of administrative, physical, and/or technical safeguards.
- Output - Selected control(s)
- Step 5. Assign Responsibility
- Identify the workforce members with the skills necessary to implement each of the specific controls outlined in the previous step, and assign their responsibilities. Also identify the equipment, training and other resources needed for the successful implementation of controls. Resources may include time, money, equipment, etc.
- Output - List of resources, responsible persons and their assignments

- Step 6. Develop Safeguard Implementation Plan
- Develop an overall implementation or action plan and individual project plans needed to implement the safeguards and controls identified. The Implementation Plan should contain the following information:
- Each risk or vulnerability/threat pair and risk level;
- Prioritized actions;
- The recommended feasible control(s) for each identified risk;
- Required resources for implementation of selected controls;
- Team member responsible for implementation of each control;
- Start date for implementation
- Target date for completion of implementation;
- Maintenance requirements.
- The overall implementation plan provides a broad overview of the safeguard implementation, identifying important milestones and timeframes, resource requirements (staff and other individuals' time, budget, etc.), interrelationships between projects, and any other relevant information. Regular status reporting of the plan, along with key metrics and success indicators should be reported to APS Senior Management.
- Individual project plans for safeguard implementation may be developed and contain detailed steps that resources assigned carry out to meet implementation timeframe and expectations. Additionally, consider including items in individual project plans such as a project scope, a list deliverables, key assumptions, objectives, task completion dates and project requirements.
- Output - Safeguard Implementation Plan
- Step 7. Implement Selected Controls
- As controls are implemented, monitor the affected system(s) to verify that the implemented controls continue to meet expectations. Elimination of all risk is not practical. Depending on individual situations, implemented controls may lower a risk level but not completely eliminate the risk.
- Continually and consistently communicate expectations to all Risk Management Team members, as well as senior management and other key people throughout the risk mitigation process. Identify when new risks are identified and when controls lower or offset risk rather than eliminate it.
- Additional monitoring is especially crucial during times of major environmental changes, organizational or process changes, or major facilities changes.
- If risk reduction expectations are not met, then repeat all or a part of the risk management process so that additional controls needed to lower risk to an acceptable level can be identified.
- Output - Residual Risk documentation

7.2.5 Cyber Liability Insurance

APS holds cyber liability insurance with sufficient coverage based on the organization's risk profile.

Our current cyber policy is covered by Acord.

8. Compliance Audits and External Communications

`Last Reviewed: 2025-02-17:19:44:43-UTC`

APS may be requested occasionally to share additional details regarding its compliance, privacy and security program by an external entity such as a customer, media, legal or law enforcement. Such external communication, beyond what is already publicly published, needs to comply with the following policies and procedures.

8.1 Policy Statements

APS policy requires that:

(a) APS operations must comply with all applicable laws, regulations, security standards and frameworks. External audits shall be conducted accordingly to each applicable compliance requirement.

- GDPR. APS must protect the personal data and privacy of EU citizens according to the regulatory requirements set forth in the European Union General Data Protection Regulation (GDPR).
- NIST. APS security shall implement the applicable controls outlined in NIST Special Publication 800-53.
- PCI. APS must protect the payment card data processed and/or stored according to the requirements in the latest Payment Card Industry Data Security Standard (PCI DSS).

(b) All external communications related to compliance and customer/employee privacy must follow pre-established procedures and handled by approved personnel. This includes but is not limited to distribution of audit reports, assessment results, incidents and breach notification.

(c) Audit and compliance reports may be shared with an external party only when under signed NDA and approved by APS Security Officer.

8.2 Controls and Procedures

8.2.1 Compliance Program Management

APS management and security/compliance team has identified and regularly reviews all relevant statutory, regulatory, and contractual requirements.

APS’s compliance policy includes requirements to meet any and all applicable compliance requirements.

Additionally, the Vendor Risk Management policies and procedures specify the details related to contractual agreements with clients, partners and vendors, as well as requirements and process related to intellectual property rights and the use of proprietary software products.

8.2.2 Requesting Audit and Compliance Reports

APS, at its sole discretion, shares audit reports, including any Corrective Action Plans (CAPs) and exceptions, with customers on a case by case basis. All audit reports are shared under explicit NDA in APS format between APS and party to receive materials. Audit reports can be requested by APS workforce members for Customers or directly by APS Customers.

The following process is used to request audit reports:

1. A request may be sent by email to compliance@aboveproperty.com or by submitting a request via APS Internal Support Portal or Email. In the request, please specify the type of report being requested and any required timelines for the report.
2. An Issue with the details of the request is entered into the APS Infrastructure Project on Rally, which is used to track requests status and outcomes.
3. APS security team will confirm if a current NDA is in place with the party requesting the audit report. If there is no NDA in place, APS will send one for execution.
4. Once it has been confirmed that an NDA is executed, APS staff will begin to review the Rally Issue.
5. The APS Security Officer must Approve or Reject the Issue. If the Issue is rejected, APS will notify the requesting party that we cannot share the requested report.
6. If the Issue has been Approved, APS will send the customer the requested audit report and complete the Rally Issue for the request.

See detailed policy and procedures in Breach Notification

External Audits of Information Access and Activity

Prior to contracting with an external audit firm, APS shall:

- Outline the audit responsibility, authority, and accountability
- Choose an audit firm that is independent of other organizational operations
- Ensure technical competence of the audit firm staff
- Require the audit firm's adherence to applicable codes of professional ethics
- Assign organizational responsibility for supervision of the external audit firm
- Obtain a signed GDPR data processing agreement, if any personal data will be shared/accessed during the audit

Whenever possible, a third party auditing vendor should not be providing the organization IT oversight services (e.g., vendors providing IT services should not be auditing their own services to ensure separation of duties).

Contacts for External Communications Requests

Direct all other communication requests to one of the following:

- For incident reporting, vulnerability disclosure and other security related inquiries:
- security@aboveproperty.com
- https://compliance.aboveproperty.com
- For privacy concerns, including report of violation:
- privacy@aboveproperty.com
- https://compliance.aboveproperty.com/privacy-policy/
- For all compliance related issues, including request of audit reports:
- compliance@aboveproperty.com

8.2.3 Continuous Compliance Monitoring

The status of compliance is tracked via AWS SecurityHub. Compliance dashboards are configured with applicable internal and external standards and frameworks. Any potential gaps detected are reported on the compliance dashboards.

9. System Audits, Monitoring and Assessments

`Last Reviewed: 2025-02-17:19:44:43-UTC`

APS shall audit, monitor, and assess the access and activity of systems and applications that process or store production and/or sensitive data such as personally identifiable information (PII) in order to ensure compliance.

Audit activities may be limited by application, system, and/or network auditing capabilities and resources. APS shall make reasonable and good-faith efforts to safeguard information privacy and security through a well-thought-out approach to auditing that is consistent with available resources.

It is the policy of APS to safeguard the confidentiality, integrity, and availability of applications, systems, and networks. To ensure that appropriate safeguards are in place and effective, APS shall audit access and activity to detect, report, and guard against:

- Network vulnerabilities and intrusions;
- Breaches in confidentiality and security of sensitive information;
- Performance problems and flaws in applications;
- Improper alteration or destruction of sensitive information;
- Out of date software and/or software known to have vulnerabilities.

This policy applies to all APS systems that store, transmit, or process sensitive information.

9.1 Policy Statements

APS policy requires that:

(a) All critical computing systems and software, both virtual and physical, must enable audit logging.

(b) Audit logs must include sufficient information to identify who did what, when, where.

9.2 Controls and Procedures

9.2.1 Types of System Audits

APS’s auditing processes include the following.

1. **Configuration and Activity Monitoring:** This refers to the logging, monitoring, scanning and alerting of a system, account, or environment, which may be achieved using real-time automated scripts/software or a manual review/testing. This type of auditing is performed *continuously* as part of APS operations.

> **Examples include:**
>
> - User: User and account-level audit trails generally monitor and log all commands directly initiated by the user, all identification and authentication attempts, and data and services accessed.
> - Application: Application-level audit trails generally monitor and log all user activities, including data accessed and modified and specific actions.
> - System: System-level audit trails generally monitor and log user activities, applications accessed, file integrity, and other system-defined specific actions.
> - Network: Network-level scans or audit trails generally monitor information on what is operating, perform penetrations, and identify vulnerabilities.
> - Traffic: Traffic refers to the incoming and outgoing traffic into and out of production/restricted environments. For example, firewall logs or VPC flow logs in AWS.
> - Data: Data includes all successful and failed attempts at production data access and editing.
>
> *Data associated with above events will include origin, destination, action performed, timestamp, and other relevant details available.*

2. **Access Review:** This refers to the review of all user and service accounts and permissions across APS operational environments, including on-premise systems, cloud environments such as AWS accounts, and other applications such as collaboration software, ticketing system and code repos.

- APS developed an internal tool to automatically pull configurations from our cloud based environments, including
- AWS access configuration from IAM policies, EC2 VPC and security group settings, S3 bucket policies, Lambda and API Gateway resources, etc.;
- Users, groups, application access from Microsoft 365 IdP;
- Network access settings from Cisco Meraki, etc.
- The data is collected either on demand triggered by security team or by changes in the operational environment.
- The data is used by the tool to aggregate and analyze user and application access.
- Access to other systems and applications that are not covered by this automated tool are reviewed manually on a quarterly basis or with any significant change to the target environment.
- As a result of each review, unused or invalid access will be removed.

3. **Compliance and Controls Audit:** This refers to the audit performed against the Technical, Administrative, and/or Physical controls as defined in APS policies and procedures, to measure their adoption and effectiveness. This type of auditing is typically performed by either a designated internal audit team or an external audit firm, at *defined intervals* or prompted by a *trigger event*.

> **Potential trigger events include:**
>
> - Scheduled compliance audit/assessment (e.g. annual risk assessment)
> - High risk or problem prone incidents or events, or as part of post-incident activities
> - Business associate, customer, or partner complaints
> - Identification of significant security vulnerabilities
> - Atypical patterns of activity
> - Failed authentication attempts
> - Remote access use and activity
> - Activity post termination
> - Random audits

9.2.2 Security Events Analysis

Security logs, events, and audit trails are reviewed by the security team with the assistance of automated systems and processes.

- Auditing logs are automatically analyzed and correlated by the monitoring solutions and/or a centralized security information and event management system.
- The systems are configured with rules/policies to identify suspicious activities, vulnerabilities and misconfigurations.
- Alerts are triggered upon identification of an issue based on the policy configuration.
- The alerts are sent immediately to the responsible staff (e.g. security team) for analysis. The alerts may be sent via email, Slack messaging, or as notification on the monitoring dashboard.
- Analysis is prioritized based on alert severity. High severity alerts are typically reviewed within 24 hours.
- Incident response process is followed, as needed.
- Patches and updates will be applied to all systems in a timely manner.

9.2.3 Internal/Manual Auditing Activities

Additional manual reviews, such as user accounts and access auditing, may be necessary from time to time. These activities may be triggered by the events listed above.

- Responsibility for audit activity is assigned to APS’s Security Officer. The Security Officer shall:
- Assign the task of generating reports for audit activities to the workforce member responsible for the application, system, or network;
- Assign the task of reviewing the audit reports to the workforce member responsible for the application, system, or network, or any other individual determined to be appropriate for the task;
- Organize and provide oversight to a team structure charged with audit compliance activities (e.g., parameters, frequency, sample sizes, report formats, evaluation, follow-up, etc.).
- All connections to APS are monitored. Access is limited to certain services, ports, and destinations. Exceptions to these rules, if created, are reviewed on an annual basis.
- The manual review process shall define and include:
- Description of the activity as well as rationale for performing the audit.
- Identification of personnel to perform the review (workforce members shall not review audit logs that pertain to their own system activity).
- Frequency of the auditing process.
- Determination of significant events requiring further review and follow-up.
- Identification of appropriate reporting channels for audit results and required follow-up.
- Manual audits and reviews activities are tracked in Rally.
- Auditing, reviews and testing may be carried out internally or provided through an external third-party vendor. Whenever possible, a third party auditing vendor should not be providing the organization IT oversight services (e.g., vendors providing IT services should not be auditing their own services to ensure separation of duties).

9.2.4 Audit Requests

1. A request may be made for an audit for a specific cause. The request may come from a variety of sources including, but not limited to, Security Officer, Customer, Partner, or an Application owner or application user.
2. A request for an audit for specific cause must include time frame, frequency, and nature of the request.

3. A request for an audit must be reviewed and approved by APS's Privacy Officer and/or Security Officer before proceeding. Under no circumstances shall detailed audit information be shared with parties without proper permissions and access to see such data.

- Should the audit disclose that a workforce member has accessed sensitive data inappropriately, the minimum necessary/least privileged information shall be shared with APS's Security Officer to determine appropriate sanction/corrective disciplinary action.
- Only de-identified information shall be shared with Customer or Partner regarding the results of the investigative audit process. This information will be communicated to the appropriate personnel by APS's Privacy Officer or designee. Prior to communicating with customers and partners regarding an audit, it is recommended that APS consider seeking guidance from risk management and/or legal counsel.

9.2.5 Review and Reporting of Audit Findings

1. Audit information that is routinely gathered must be reviewed in a timely manner, at least monthly, by the responsible workforce member(s). Additional reviews are performed as needed to assure the proper data is being captured and retained.
2. The reporting process shall allow for meaningful communication of the audit findings to relevant workforce members, Customers, or Partners.

- Significant findings shall be reported immediately in a written format. APS's security incident response form may be utilized to report a single event.
- Routine findings shall be reported to the sponsoring leadership structure in a written report format.

3. Reports of audit results shall be limited to internal use on a minimum necessary/need-to-know basis. Audit results shall not be disclosed externally without administrative and/or legal counsel approval.
4. Security audits constitute an internal, confidential monitoring practice that may be included in APS's performance improvement activities and reporting. Care shall be taken to ensure that the results of the audits are disclosed to administrative-level oversight structures only and that information which may further expose organizational risk is shared with extreme caution. Generic security audit information may be included in organizational reports (individually-identifiable information shall not be included in the reports).
5. Whenever indicated through evaluation and reporting, appropriate corrective actions must be undertaken. These actions shall be documented and shared with the responsible workforce members, Customers, and/or Partners.

9.2.6 Remediation of Control Deficiencies

Most controls are continuously monitored and reported via automation on the Jira platform.

Control deficiencies identified as a result of an internal or external system audit are documented and reviewed with management.

Security team works with the corresponding control owner to prioritize and mitigate the control deficiency, including applying corrective actions, implementing additional controls or adjusting existing controls as needed.

9.2.7 Audit Trails and Application Security Events Logging Standard

APS logging standards requires application and system logs to contain sufficient information to determine **who did what, when, where** to ensure recording of security and audit events and to generate evidence for unauthorized activities.

All systems and software developed at APS must have the following security events logging enabled as part of or in addition to standard application logging.

1. All security log events must have the following attributes at minimum:
   - Timestamp of the event (synchronized to approved time server)
   - Identifier of the principal performing the action (such as user ID)
   - Location including both origin (such as hostname/IP) and target (such as host/service/resource)
   - Activity or action (such as log in, log out, create, read, update, delete of a resource)
   - the action may be logged as and determined by the HTTP request method and the API endpoint
   - Event description and additional details may be logged depending on the system or application
2. The following types of security events must be logged at minimum:
   - User and group administration activities (user or group added, updated, deleted, access granted/revoked)
   - All login attempts, successful and unsuccessful including the source IP address
   - All interactive logoffs
   - Privileged actions (configuration changes, application shutdown/restart, software update etc)
   - Major application events (e.g. application failure, start and restart, shutdown)
   - Any and all actions performed on critical resources such as production data
3. All application and system logs must not include (removed or masked):
   - Any sensitive information, including
     personally identifiable information (PII)
   - except for IP addresses
   - usernames/logins may/should be logged as part of authentication logging
   - for user action auditing, opaque IDs should be used instead of usernames/logins whenever possible
   - Authentication and session tokens, user credentials
4. Security events and audit logs must be:
   - Always accessible to the monitoring system/team
   - Protected from any changes
   - Monitored with alerting mechanism in place (including alert for not receiving log events for a certain period of time)
5. All APS IT infrastructure must have system clock synchronized

Examples of recommended application events for logging and their auditing purpose:

Events	**Purpose**
Client requests and server responses	forensics and debugging - details level is defined by application
Successful and unsuccessful login attempts	authentication
Successful and failed access to application resources	authorization, escalation of privileges
Excessive amount of requests from the client	brute-forcing, malicious bots, denial of service attacks
E-mails sent by an application	spamming, social engineering

Details of the logging configuration is documented at

- Application Logging - documented on the Engineering Wiki
- Identity and Access Activity Logs via Microsoft 365
- AWS Cloudtrail
- AWS S3 Server Access Logs

9.2.8 Audit Trail Integrity - Security Controls and Log Retention

1. Audit logs shall be protected from unauthorized access or modification, so the information they contain will be made available only if needed to evaluate a security incident or for routine audit activities as outlined in this policy.
2. All audit logs are protected in transit and encrypted at rest to control access to the content of the logs.
3. Whenever possible, audit logs shall be stored on a separate system to minimize the impact auditing may have on the privacy system and to prevent access to audit trails by those with system administrator privileges.

- Separate systems are used to apply the security principle of “separation of duties” to protect audit trails from hackers.
- APS logging servers may include Elasticsearch, Logstash, and Kibana (ELK) as part of their baseline configuration to ease reviewing of audit log data. The ELK toolkit provides message summarization, reduction, and reporting functionality.

4. Reports summarizing audit activities shall be retained for a period of seven years.
5. Audit log data is retained locally on the audit log server or in the source environment for a period of one month. Beyond that, log data is encrypted and moved to warm storage (currently S3) using automated scripts, and is retained for a minimum of one year.
6. Raw event data may be purged after one month / 30 days as long as the required details are sufficiently covered in aggregated audit logs/reports.

9.2.9 Auditing Customer and Partner Activity

1. Periodic monitoring of Customer and Partner activity shall be carried out to ensure that access and activity is appropriate for privileges granted and necessary to the arrangement between APS and the 3rd party. APS will make every effort to assure Customers and Partners do not gain access to data outside of their own environments.
2. If it is determined that the Customer or Partner has exceeded the scope of access privileges, APS’s management and security must remedy the problem immediately.

9.2.10 Auditing and Assessment Tools

APS’s Security Officer is authorized to select and use assessment tools that are designed to detect vulnerabilities and intrusions. Use of such tools against APS systems and environments are prohibited by others, including Customers and Partners, without the explicit authorization of the Security Officer. These tools may include, but are not limited to:

- Scanning tools and devices;
- Password cracking utilities;
- Network “sniffers”;
- Security agents installed locally on servers and endpoints;
- Passive and active intrusion detection systems; and
- Penetration testing tools.

Vulnerability testing software may be used to probe the network to identify what is running (e.g., operating system or product versions in place), whether publicly-known vulnerabilities have been corrected, and evaluate whether the system can withstand attacks aimed at circumventing security controls.

10. HR and Personnel Security

`Last Reviewed: 2025-02-17:19:44:43-UTC`

APS is committed to ensuring all workforce members actively address security and compliance in their roles at APS. We encourage self management and reward the right behaviors. This policy specifies acceptable use of end-user computing devices and technology. Additionally, training is imperative to assuring an understanding of current best practices, the different types and sensitivities of data, and the sanctions associated with non-compliance.

10.1 Policy Statements

In addition to the roles and responsibilities stated earlier, APS policy requires all workforce members to comply with the Acceptable Use Policy for End-use Computing and HR Security Policy.

APS policy requires that:

(a) Background verification checks on all candidates for employees and contractors should be carried out in accordance with relevant laws, regulations, and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risk.

(b) Employees, contractors and third party users must agree and sign the terms and conditions of their employment contract, and comply with acceptable use.

(c) Employees will go through an onboarding process that familiarizes them with the environments, systems, security requirements, and procedures APS has in place. Employees will also have ongoing security awareness training that is audited.

(d) Employee offboarding will include reiterating any duties and responsibilities still valid after terminations, verifying that access to any APS systems has been removed, as well as ensuring that all company owned assets are returned.

(e) APS and its employees will take reasonable measures to ensure no sensitive data is transmitted via digital communications such as email or posted on social media outlets.

(f) APS will maintain a list of prohibited activities that will be part of onboarding procedures and have training available if/when the list of those activities changes.

(g) A fair disciplinary process will be utilized for employees are suspected of committing breaches of security. Multiple factors will be considered when deciding the response such as whether or not this was a first offense, training, business contracts, etc. APS reserves the right to terminate employees in the case of serious cases of misconduct.

10.2 Controls and Procedures

10.3 HR Management and Reporting

APS uses TriNet to manage its workforce personnel records.

10.3.1 Organization Structure

A reporting structure has been established that aligns with the organization’s business lines and/or individual’s functional roles. The organizational chart is available to all employees via the TriNet and/or posted on the internal web portal.

10.3.2 Job Functions and Descriptions

Position / Job descriptions are documented and updated as needed that define the skills, responsibilities, and knowledge levels required for certain jobs.

10.3.3 Acceptable Use of End-user Computing

APS requires all workforce members to comply with the following acceptable use requirements and procedures, such that:

(a) Per APS security architecture, all workforce members are primarily considered as remote users and therefore must follow all system access controls and procedures for remote access.

(b) Use of APS computing systems is subject to monitoring by APS IT and/or Security team.

(c) Employees may not leave computing devices (including laptops and smart devices) used for business purpose, including company-provided and BYOD devices, unattended in public.

(d) Device encryption must be enabled for all mobile devices accessing company data, such as whole-disk encryption for all laptops.

(e) Use only legal, approved software with a valid license installed through a pre-approved application store. Do not use personal software for business purposes and vice versa.

(f) Encrypt all email messages containing sensitive or confidential data.

(g) Employees may not post any sensitive or confidential data in public forums or chat rooms. If a posting is needed to obtain technical support, data must be sanitized to remove any sensitive or confidential information prior to posting.

(h) Anti-malware or equivalent protection and monitoring must be installed and enabled on all endpoint systems that may be affected by malware, including workstations, laptops and servers.

(i) All data storage devices and media must be managed according to the APS Data Classification specifications and Data Handling procedures.

(j) It is strictly forbidden to download or store any sensitive data on end-user computing devices, including laptops, workstations and mobile devices.

10.3.4 Employee Onboarding Procedures

A master checklist for employee onboarding is maintained by HR/Facilities.
It is published in the HR system or the HR folder on APS's internal file sharing site.

The HR Representative / Facility Manager is responsible to create an Issue in the Rally via Help Desk to initiate and track the onboarding process. The onboarding process should include the following IT/Security items:

1. Training.
   - New workforce member is provided training on APS security policy, acceptable use policy, and given access to the Employee Handbook.
   - Records of training and policy acceptance is kept in the HR system.
   - The training and acceptance must be completed within 30 days of employment.
2. Access.
   - Standard access is provisioned according to the job role and approval as specified in the HR onboarding Rally ticket.
   - Non-standard access requires additional approval following the access request procedures.
   - Request for modifications of access for any APS employee can be made using the procedures outlined in the Access Establishment and Modification policy and procedures.
3. System configuration.
   - The end-user computing device (e.g. workstation or laptop) may be provisioned by IT to install necessary software, malware protection, security agents, and setting system configurations.
   - Users in a technical role, such as Development, may choose to self configure their system. In this case, the user is given configuration guidelines defined by IT and Security. The system must have the required security configuration and endpoint agents installed for monitoring and to ensure compliance.

10.3.5 Employee Exiting/Termination Procedures

A master checklist for employee existing/termination is maintained by HR/Facilities. It is published in the HR system or the HR folder on APS's internal file sharing site.

1. The Human Resources Department (or other designated department), users, and their supervisors (HR) are required to notify Security upon completion and/or termination of access needs and facilitating completion of the "Termination Checklist".
2. HR are required to notify Security to terminate a user's access rights if there is evidence or reason to believe the following (these incidents are also reported on an incident report and is filed with the Security Officer):

- The user has been using their access rights inappropriately;
- A user's password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password);
- An unauthorized individual is utilizing a user's User Login ID and password (a new password may be provided to the user if the user is not identified as providing the unauthorized individual with the User Login ID and password).

3. Security will terminate users' access rights immediately upon notification, and will coordinate with the appropriate APS employees to terminate access to any non-production systems managed by those employees.
4. Security audits and may terminate access of users that have not logged into organization's information systems/applications for an extended period of time.

10.3.6 Employee Issue Escalation

APS workforce members are to escalate issues using the procedures outlined in the Employee Quick Reference. Issues that are brought to the Escalation Team are assigned an owner. The membership of the Escalation Team is maintained by the Chief Executive Officer or a delegate.

Security incidents, particularly those involving sensitive data, are handled using the process described in Incident Response. If the incident involves a breach of sensitive data, the Security Officer will manage the incident using the process described in Breach Notification. Refer to Incident Response for a list of sample items that can trigger APS's incident response procedures; if you are unsure whether the issue is a security incident, contact the Security team immediately.

It is the duty of the incident owner to follow the process outlined below:

1. Create an Issue in the Rally Security Project.
2. The Issue is investigated, documented, and, when a conclusion or remediation is reached, it is moved to Review.
3. The Issue is reviewed by another member of the Escalation Team. If the Issue is rejected, it goes back for further evaluation and review.
4. If the Issue is approved, it is marked as Done, adding any pertinent notes required.
5. The workforce member that initiated the process is notified of the outcome via email.

10.4 Continuous Education and Skills Development

APS provides employees the opportunity to attend conferences, trade shows, and/or ongoing training/studies relevant to their job function and business objectives.

10.5 Non-Compliance Investigation and Sanctions

All APS officers, employees, and associates are expected to review the complete set of policies at least annually, and to read and understand individual new policies or policy changes as they are communicated by company management.

10.5.1 Compliance Measurement

The APS management team will verify compliance with policies through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

10.5.2 Procedures

Workforce members shall report non-compliance of APS's policies and procedures to the Security Officer or other individual as assigned by the Security Officer. Individuals that report violations in good faith may not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

1. The Security Officer promptly facilitates a thorough investigation of all reported violations of APS's security policies and procedures. The Security Officer may request the assistance from others.
   - Complete an audit trail/log to identify and verify the violation and sequence of events.
   - Interview any individual that may be aware of or involved in the incident.
   - All individuals are required to cooperate with the investigation process and provide factual information to those conducting the investigation.
   - Provide individuals suspected of non-compliance of the Security rule and/or APS's policies and procedures the opportunity to explain their actions.
   - The investigator thoroughly documents the investigation as the investigation occurs. This documentation must include a list of all employees involved in the violation.
2. Violation of any security policy or procedure by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including business associates, customers, and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.
   - A fair disciplinary process will be utilized for employees are suspected of committing breaches of security. Multiple factors will be considered when deciding the response such as whether or not this was a first offense, training, business contracts, etc.
   - APS reserves the right to terminate employees in the case of serious cases of misconduct.
   - A violation resulting in a breach of confidentiality (i.e. release of sensitive data to an unauthorized individual), change of the data integrity, or inability to access data by other users, requires immediate termination of the workforce member from APS.
3. The Security Officer facilitates taking appropriate steps to prevent recurrence of the violation (when possible and feasible).
4. In the case of an insider threat, the Security Officer is to set up a team to investigate and mitigate the risk of insider malicious activity. APS workforce members are encouraged to come forward with information about insider threats, and can do so anonymously.
5. The Security Officer maintains all documentation of the investigation, sanctions provided, and actions taken to prevent reoccurrence for a minimum of seven years after the conclusion of the investigation.
6. When the Security Officer identifies a violation and begins a formal sanction process, they will notify the appropriate management or supervisors within 24 hours. That notification will include 1) identifying the individual sanctioned, 2) the reason for the sanction, and 3) specific procedures for service or account restriction / revocation or other disciplinary actions as required.

Warning Notice Template

11. Access

`Last Reviewed: 2025-02-17:19:44:43-UTC`

Access to APS systems and application is limited for all users, including but not limited to workforce members, volunteers, business associates, contracted providers, consultants, and any other entity, is allowable only on a minimum necessary basis. All users are responsible for reporting an incident of unauthorized user or access of the organization’s information systems.

11.1 Policy Statements

11.1.1 Access Control Policy

APS policy requires that

(a) Access to all computing resources, including servers, end-user computing devices, network equipment, services and applications, must be protected by strong authentication, authorization, and auditing.

(b) Interactive user access must be associated to an account or login unique to each human user.

(c) All credentials, including user passwords, service accounts, and access keys, must meet the length, complexity, age, and rotation requirements defined in APS security standards.

(d) Use strong password and multi-factor authentication (MFA) whenever possible to authenticate to all computing resources (including both devices and applications).

(e) MFA is required to access any critical system or resource, including but not limited to resources in APS production environments.

(f) Unused accounts, passwords, access keys must be removed within an established timeframe.

(g) A unique access key or service account must be used for different application or user access.

(h) Authenticated sessions must time out after a defined period of inactivity.

11.1.2 Access Authorization and Termination

APS policy requires that

(a) Access authorization shall be implemented using role-based access control (RBAC) or similar mechanism.

(b) Standard access based on a user’s job role may be pre-provisioned during employee onboarding. All subsequent access requests to computing resources must be approved by the requestor’s manager, prior to granting and provisioning of access.

(c) Access to critical resources, such as production environments, must be approved by the security team in addition to the requestor’s manager.

(d) Access must be reviewed on a regular basis and revoked if no longer needed.

(e) Upon termination of employment, all system access must be revoked and user accounts terminated within the defined, predetermined timeframe.

(f) All system access must be reviewed at least annually and whenever a user’s job role changes.

11.1.3 Shared Secrets Management

APS policy requires that

(a) Use of shared credentials/secrets must be minimized and approved on an exception basis.

(b) If required by business operations, secrets/credentials must be shared securely and stored in encrypted vaults that meet the APS data encryption standards.

(c) Usage of a shared secret to access a critical system or resource must be supported by a complimenting solution to uniquely identify the user.

11.1.4 Privileged Access Management

APS policy requires that

(a) Users must not log in directly to systems as a privileged user.

- A privileged user is someone who has administrative access to critical systems, such as a Active Directory Domain Administrator, root user to a Linux/Unix system, and Administrator or Root User to an AWS account.

(b) Privilege access must only be gained through a proxy, or equivalent, that supports strong authentication (such as MFA) using a unique individual account with full auditing of user activities.

(c) Direct administrative access to production systems must be kept to an absolute minimum.

11.2 Controls and Procedures

11.2.1 Standards for Access Provisioning

Workforce Clearance

1. The level of security assigned to a user to the organization’s information systems is based on the minimum necessary amount of data access required to carry out legitimate job responsibilities assigned to a user’s job classification and/or to a user needing access to carry out treatment, payment, or healthcare operations.
2. All access requests are treated on a “least-privilege” principle.
3. APS maintains a minimum necessary approach to access to Customer data.

Access Authorization

1. Role based access categories for each APS system and application are pre-approved by the Security Officer.
2. APS utilizes hardware-defined and/or software-defined boundaries to segment data, prevent unauthorized access, and monitor traffic for denial of service attacks.

Person or Entity Authentication

1. Each workforce member has and uses a unique user ID and password that identifies him/her as the user of the information system.
2. Each Customer and Partner has and uses a unique user ID and password or OpenID Connect that identifies him/her as the user of the information system. This is enforced through the use of **AWS Cognito**.
3. All customer support interactions must be verified before APS support personnel will satisfy any request having information security implications.

Unique User Identification

1. Access to the APS Platform systems and applications is controlled by requiring unique User Login IDs and passwords for each individual user and developer.
2. Passwords requirements mandate strong password controls (see below).
3. Passwords are not displayed at any time and are not transmitted or stored in plain text.
4. Default accounts on all production systems and environments, including root, are disabled/locked.
5. Shared accounts are not allowed within APS systems or networks.

Automatic Logon and Logoff

1. Automated log-on configurations that store user passwords or bypass password entry are not permitted for use with APS workstations or production systems.
   - Automatic log-on may only be permitted for low-risk systems such as conference room PCs connecting to a Zoom Room.
   - Such systems are configured on separate network VLANs.
2. Users are required to make information systems inaccessible by any other individual when unattended by the users (ex. by using a password protected screen saver or logging off the system).
3. Information systems automatically lock users such as enabling password-protected screensaver after 10 minutes or less of inactivity.

11.2.2 Password Management

1. User IDs and passwords are used to control access to APS systems and may not be disclosed to anyone for any reason.
2. Users may not allow anyone, for any reason, to have access to any information system using another user's unique user ID and password.
3. On all production systems and applications in the APS environment, password configurations are set to require:
   - a minimum length of 8 characters;
   - a mix of upper case characters, lower case characters, and numbers or special characters;
   - prevention of password reuse using a history of the last 24 passwords;
   - where supported, modifying at least 6 characters when changing passwords;
   - account lockout after 5 invalid attempts.

> **Exceptions**
>
> Password expiration may be set to a greater interval if an account is always protected by MFA.

4. All system and application passwords must be stored and transmitted securely.
   - Where possible, passwords should be stored in a hashed format using a salted cryptographic hash function (SHA-256 or stronger NIST compliant standard).
   - Passwords that must be stored in non-hashed format must be encrypted at rest pursuant to the requirements in Data Protection.
   - Transmitted passwords must be encrypted in flight pursuant to the requirements in Data Protection.
5. Each information system automatically requires users to change passwords at a pre-determined interval as determined by the system owner and/or Security, based on the criticality and sensitivity of the data contained within the network, system, application, and/or database.
6. Passwords are inactivated immediately upon an employee's termination (refer to the Employee Termination Procedures in HR policy).
7. All default system, application, and Vendor/Partner-provided passwords are changed before deployment to production.
8. Upon initial login, users must change any passwords that were automatically generated for them.
9. Password change methods must use a confirmation method to correct for user input errors.
10. All passwords used in configuration scripts are secured and encrypted.
11. If a user believes their user ID has been compromised, they are required to immediately report the incident to the Security team.
12. In cases where a user has forgotten their password, password reset procedures provided by the IdP shall be followed. The exact process depends on the system or application. If help is needed, users shall contact Helpdesk or Security

13. An approved password manager is used for to store or share non-critical business application passwords that are not integrated with our primary IdP through SSO.
    - The password manager locally encrypts the password vault with the user's master password before synchronizing to the cloud.
    - The master password must follow the password requirements listed above.
    - MFA must enabled in the password manager configuration.
    - Enrollment of the password manager is configured as an application in Google Workspaces.
14. An automated process/tool is implemented to ensure compromised passwords or common dictionary words are not used as passwords. This is currently implemented in Google Workspaces.

11.2.3 Single Sign On

- APS selected Google Workspaces as its primary Identity Provider (IdP) to control user access to systems and business applications.
- Single sign-on (SSO) should be used whenever possible instead of local authentication. This centralized approach improves user experience and simplifies access management.
- SSO is configured via industry standard SAML protocol between the IdP (Google Workspaces) and the target application.
- APS will not configure SSO to target applications unless they score a "B" rating or higher on the Qualys SSL Labs benchmark.
- Security team is responsible for the administration of the IdP / SSO system, including user and access provisioning. Security team may delegate administrative privilege to a subset of the system, such as a specific application.

11.2.4 Multi-factor Authentication

Multi-factor authentication (MFA) is a standard control used by APS to provide strong access control to critical systems and applications, and should be enabled whenever possible.

Purpose
The purpose of this policy is to provide guidelines for the use of multi-factor authentication (MFA) when accessing Above Property resources. These standards are designed to minimize the potential security exposure to Above Property from damages which may result from unauthorized use of APS resources. MFA adds a layer of security that helps deter the use of compromised credentials.

Scope
The policy applies to all members of the Above Property community, including all employees, contractors, board members, and affiliates who connect to Above Property associated network or technology resources. This policy applies to any system accessing Above Property or customer data where MFA can be utilized.

Definitions

- Multi-factor authentication: Using two or more factors to validate the identity of a user.
- Factor (of authentication): There are five are types of factors used in combination together resulting in multi-factor authentication. They are:
- Something the user knows (username and password)
- Something the user has (an item the user physically carries with them)
- Something the user is (biometrics: fingerprints, face scan, etc.)
- Somewhere the user is (geo location, on premises)
- Something the user does (keystroke patterns)

Policy
All individuals are required to engage in one additional step beyond the typical username/password login process to access Above Property and affiliated systems. Individuals are required to register and to use an approved MFA device (sometimes called a security key) wherever such devices are supported. If physical devices are not supported, individuals are required to make use of MFA software, such as Google Authenticator or Authy. Individuals must not use SMS (text message) based MFA unless the

affiliated resource supports no other option. In the case that an affiliated resource only supports SMS based MFA, the individual must report this to the Information Security Officer.

MFA is required for all externally-exposed enterprise or third-party applications, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this safeguard.

MFA is required for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.

Responsibilities
Above Property will supply each covered individual with one MFA device. Individuals may supply their own backup devices if desired. It is the individual's responsibility to promptly report compromised credentials to the Information Security team. It is the individual's responsibility to promptly report a lost or stolen MFA device to the Information Security team.

Exemptions
There may be situations in which an individual has a legitimate need to utilize technology resources outside the scope of this policy. The Information Security team must approve, in advance, exception requests based on balancing the benefit versus the risk to the company.

Enforcement
This policy regulates the use of all MFA access to APS network, software, and external resources. All users users must comply with this policy, as directed in the Policy Compliance Policy. Services will be disabled immediately if any suspicious activity is observed. Service will remain disabled until the issue has been identified and resolved.
Any covered individual found to have intentionally violated or ignored this policy will be subject to loss of privileges or other actions, as specified in the Policy Compliance Policy.

Important

Approved MFA methods include:

- Passkeys (preferred. See the Passkey section below.)
- Hardware MFA token (preferred where passkeys are not available; APS provides Yubikey tokens for all staff, contractors, and board members)
- A unique cryptographic certificate tied to a device
- Time-based One-Time Password (TOTP) delivered through a mobile app, such as Google Authenticator
- One-time passcode delivered through SMS text message (if and only if it is the only supported option)
- Secure physical facility (if the system or application can only be accessed at that location)

11.2.5 Authentication via passkey

APS strongly encourages users to make use of passkeys wherever they are available. Passkeys use public key cryptography to generate strong user credentials that are tied to a single web site or application. To make sure only the rightful owner can use a passkey, the system will ask them to unlock their device. This may be performed with a biometric sensor (such as a fingerprint or facial recognition), PIN, or pattern.

Passkeys are suppored directly in Google Chrome, Android devices, iPhone and MacOS and in the 1Password password manager. As of September 2023, the Firefox browser does not support passkey operations, and as a result APS discourages the use of Firefox.

Passkey authentication is significantly stronger and more robust than username/password + MFA authentication, and is the preferred method of authentication at APS for all sites and applications that support it.

11.2.6 Role Based Access Control (RBAC)

By default, user access is granted based on the user's job function / role. For example:

- Developer
- Security
- IT
- Administrative
- Marketing / Sales

This is defined as **user groups** in Google Workspaces.

Access to sensitive data and production customer data is highly restricted and further defined in its own section.

11.2.7 Temporary Access to AWS Accounts and Resources

Access to APS AWS accounts are permissible through temporary credentials / sessions only. No persistent users, passwords or access keys are allowed in AWS IAM configurations for end-user access, either to the AWS console or AWS CLI. This is achieved with the following processes:

AWS Console Access

- An organization master account (`APS-master`) in AWS is configured with IAM roles such as Developer and Security.
- SAML SSO and trust relationship is established between the roles in `APS-master` and an "AWS application" provisioned in AWS Identity Center.
- Users are assigned their corresponding roles through application and role assignment in Google Workspaces.
- Via SSO, Users authenticate through Google Workspaces by using their APS Google username, password, and MFA.
- Upon successful authentication and MFA validation, users are logged into `APS-master` using AWS Assume Role capability.
- The roles in `APS-master` by default has highly restricted access. For example, the `Developer` role does not have access to any services and resources in the master account.
- The user is required to Assume a Role in a sub-account, connected via cross-account trust policy defined at account bootstrap or through an approved change management process. For example, a Developer may be able assume the `Administrator` role in `APS-dev`, which is the sandboxed development environment in a separate AWS account.
- Assume Role access to a production AWS account is highly restricted.
- Developers can only assume the `Developer` role in production which only has access to read CloudWatch logs, XRay system traces/service maps, CloudWatch metrics, resource group inventories, and CloudWatch dashboards.
- Security can only assume the `Auditor` role in production which has the default Auditor IAM policy managed by AWS. This policy allows read-only access to account and resource configurations, but does not allow read access to any data such as S3 objects.

AWS CLI/SDK Access

- granted/assume is used to obtain temporary credentials (access keys) for developers to connect to AWS using the CLI or SDK.
- Using granted/assume, users are prompted to authenticate to Google Workspaces using their APS credentials and MFA token/ app.
- Upon successful authentication and MFA validation, a temporary session token is inserted into the user's local environment.
- This temporary credential expires after one hour and a new temporary credential must be obtained for access.
- Additional details are documented on the Development Wiki.

IAM Safety

- APS implements **AWS Security Hub** to monitor and protect its AWS environments.
- AWS Access Analyzer works by defining a set of risky actions, such as adding/remove IAM users to an **Explicit Deny** policy. The policy is attached to an IAM Group, and protected Users and/or Roles are assigned to this Group.
- Because explicit deny rules always take precedence in AWS IAM policy, this effectively restricts access and prohibits execution of the risky actions as defined in the policy, even if the user/role may have administrative privilege.
- Privilege Roles, such as Security role in master account and Administrator role in production account, are protected by IAM Safety.

Troubleshooting / Support Access

In normal operations, troubleshooting is performed with log analysis in DataDog, outside of the production environments in AWS. A separate Support role is created for temporary troubleshooting and support access when log access is insufficient to determine the cause. Support access should be minimized and is designed to involve manual approval and provision process.

- The Support role by default is NOT assigned to anyone.
- The Support role is configured with Read level access to the services used by APS platform services and applications. It does NOT have permission to make any configuration changes and does NOT have access to production data.
- An Infrastructure (IN) ticket is used to request temporary support access and must be approved by Head of Engineering and Security.
- Upon approval of the support access IN ticket, Security grants the requestor temporary access to by assigning the Support role to that particular individual user in Microsoft 365.
- The Support role is protected by Azure Active Directory and it must be explicitly allowed by the Security team for it to assume the Support role in the target production environment.
- By default, temporary Support access is limited to one hour. This can be extended by the Security team.
- The role assignment is removed from Microsoft 365 immediately after the support session.

11.2.8 Remote Access / VPN

- VPN remote access to non-production and non-privileged environments in AWS are permissible and implemented using **AWS VPN**.

11.2.9 Platform Customer Access to Systems

APS does not allow direct system access by customers. Access is only available through the Web UI or API interface, with valid authentication and authorization detailed in the Product Security, Architecture, and Security pages of the engineering wiki.

11.2.10 Access Establishment, Modification and Termination

1. Requests for access to APS Platform systems and applications is made formally using the following process:

a. An access request is created in Rally through either the new employee onboarding request or a specific access request from APS Internal Support site.

b. The Security team will grant standard access to per job role as part of new employee onboarding. A standard set of accounts that are default for all employees are created as part of the onboarding process. This includes

- User account for local system/laptop
- Microsoft 365 user in the Everyone group, and additional group based on role such as Development, IT, Security
- Google Workspaces account for access to email, documents, etc.
- HR accounts for paperwork, benefits management, payroll, expense reporting, etc.
- Additional role based access (e.g. GitHub and Jenkins access for a developer)

c. Standard access may be provisioned at any time by account owners/administrators at any time during or after onboarding with approval of account owners and/or manager.

d. If additional access is needed in addition to the above, a separate access request (through Rally) is required and the requester must include a description and justification as part of the access request.

e. Once the review is completed, the Security team approves or rejects the Issue. If the Issue is rejected, it goes back for further review and documentation.

f. If the review is approved, IT or Security team provisions access, then marks the Issue as Done, adding any pertinent notes required.

- New accounts will be created with a temporary secure password that meets all password requirements, which must be changed on the initial login.
- All password exchanges must occur over an authenticated channel.
- For on-premise systems, access grants are accomplished by adding the appropriate user account to the corresponding LDAP/AD group.
- For cloud accounts, access grants are provisioned in Microsoft 365 or using the access control mechanisms built into those services/applications.
- Account management for non-production systems may be delegated to a APS employee at the discretion of the Security Officer.

2. Special access, including access to production environments, is not granted until receipt, review, and approval by the APS Security Officer.
3. The request for access is retained for future reference.
4. Temporary accounts are not used unless absolutely necessary for business purposes.

- Accounts are reviewed every 90 days to ensure temporary accounts are not left unnecessarily.
- Accounts that are inactive for over 90 days are removed.

5. In the case of non-personal information, such as generic educational content, identification and authentication may not be required.

Access Termination

IT Manager or Security team receives access termination requests in one of the following conditions and processes it accordingly:

- Employee existing/termination, as defined by the process in HR & Employee Security;
- Employee access to a system is no longer required as a result of job role change or similar event, in which case a access termination request may be submitted by the employee or his/her manager via the Internal Help portal or an email request to Security team;
- As the result of a Access Review, as defined in System Auditing.
- Non-standard access is revoked by default after 30 days of inactivity, unless an exception/extension is requested and approved.

11.2.11 Access Reviews

- All access to APS systems and services are reviewed and updated following the procedures specified in System Auditing to ensure proper authorizations are in place commensurate with job functions.
- In cases of increased risk or known attempted unauthorized access, immediate steps are taken by the Security Officer to limit access and reduce risk of unauthorized access.

11.2.12 Service Accounts

- All application to application communication using service accounts is restricted and not permitted unless absolutely needed. Automated tools are used to limit account access across applications and systems.
- Services that are part of APS platform leverage AWS IAM policy configurations and/or OAuth for authorization.
- Generic accounts are not allowed on APS systems.
- Direct system to system, system to application, and application to application authentication and authorization are limited and controlled to restrict access.
- In AWS, service accounts are implemented in the form of IAM Roles, and their access defined by the corresponding IAM policies. The creation of these IAM roles and policies is implemented as code, which follows the secure development, review and production change approval process.
- An inventory of all Service accounts is maintained by AWS IAM and CloudFormation and reviewed periodically.

11.2.13 Employee Workstation / Endpoints Access and Usage

All workstations at APS are company owned, using one the following approved hardware vendors and operating systems:

- Apple, Dell, or Lenovo
- macOS, Linux (Ubuntu or Debian), or Windows 10

1. Workstations may not be used to engage in any activity that is illegal or is in violation of organization’s policies.
2. Access may not be used for transmitting, retrieving, or storage of any communications of a discriminatory or harassing nature or materials that are obscene or “X-rated”. Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual’s race, age, disability, religion, national origin, physical attributes, sexual preference, gender identification, or health condition shall be transmitted or maintained. No abusive, hostile, profane, or offensive language is to be transmitted through organization’s system.
3. Information systems/applications also may not be used for any other purpose that is illegal, unethical, or against company policies or contrary to organization’s best interests. Messages containing information related to a lawsuit or investigation may not be sent without prior approval.
4. Solicitation of non-company business, or any use of organization’s information systems/applications for personal gain is prohibited.
5. Users may not misrepresent, obscure, suppress, or replace another user’s identity in transmitted or stored messages.
6. Workstation hard drives will be encrypted using FileVault (macOS), BitLocker (Windows) or equivalent.
7. All workstations must have host firewalls enabled to prevent unauthorized access unless explicitly granted.
8. All workstations must have endpoint security software installed and actively running, if supported by the operating system.

11.2.14 Production Access and Secrets Management

APS leverages a combination of Jenkins credentials store, Amazon Secrets Manager, and Amazon EC2 Systems Manager Parameter Store to securely store production secrets. Secrets are always encrypted; access to secrets is always controlled and audited.

Details and usage are documented on the APS Engineering Wiki.

11.2.15 Production Data Access

The following requirements and controls are in place for accessing production data by internal personnel:

- There is no pre-provisioned, persisted “internal” access to production data stores. Access such as direct SSH to the production database servers and direct access to data objects in production S3 buckets are prohibited.
- Access to customer data is granted on a per-account basis.
- Access requests follow the same production access processes. Access must be approved by both the data owner and the security team.
- Access to production data is granted only through an approved platform with strong centralized access control, with MFA.
- An audit list of who has access to which customer data is maintained and reviewed monthly. Access is revoked when no longer needed.

11.2.16 Password Reset and other Helpdesk Requests

APS employees have the ability to obtain self-service support directly from supported business applications, such as password reset via the SSO/IdP tool.

If needed, users may use our internal service desk or email request to obtain IT and Security support.

A ticket is opened in Rally for each support request and assigned to the appropriate personnel. The person assigned must verify the identity of the requester and ensure the ticket has appropriate approval before implementing or providing support. The verification step and confirmation of “User identity verified” should be included as a comment in the ticket by the support personnel. Additionally, if a password or security credential has been created or supplied, confirm user has received it via another channel like slack/email/phone/zoom and document receipt in the ticket.

12. Facility Access and Physical Security

`Last Reviewed: 2025-02-17:19:44:43-UTC`

It is the goal of APS to provide a safe and secure environment for all employees. Access to the APS facilities is limited to authorized individuals only.

APS works with Subcontractors (e.g. property management companies and facilities management) to assure restriction of physical access to systems used as part of the APS Platform.

Physical Access to all of APS facilities is limited to only those authorized in this policy. All workforce members are responsible for reporting an incident of unauthorized visitor and/or unauthorized access to APS's facility.

12.1 Policy Statements

APS policy requires that

(a) Physical access to APS facilities is restricted.

(b) All employees are required to wear employee badges at secure facilities (such as server rooms, data centers, labs).

(c) All employees must follow physical security requirements and procedures documented by facility management.

(d) On-site visitors and vendors must be escorted by a APS employee at all times while on premise.

(e) All workforce members are responsible for reporting an incident of unauthorized visitor and/or unauthorized access to APS's facility.

(f) Retain a record for each physical access, including visits, maintenance and repairs to APS production environments and secure facilities.

- Details must be captured for all maintenance and repairs performed to physical security equipment such as locks, walls, doors, surveillance cameras; and
- All records must be retained for the defined, predetermined timeframe.

(g) Building security, such as fire extinguishers and detectors, escape routes, floor warden responsibilities, shall be maintained according to applicable laws and regulations.

12.2 Controls and Procedures

12.2.1 Physical Security

Access Requirements Overview

- Physical access is restricted using badge readers and/or smart locks that track all access.
- Restricted areas and facilities are locked when unattended (where feasible).
- Only authorized workforce members receive access to restricted areas (as determined by the Security Officer).
- Access and keys are revoked upon termination of workforce members.
- Workforce members must report a lost and/or stolen key(s) or badge(s) to his/her manager, local Site Lead, or the Facility Manager.
- The Facility Manager or designee is responsible to revoke access to the lost/stolen badge(s) or access key(s), and re-provision access as needed.
- The Facility Manager or designee facilitates the changing of the lock(s) within 7 days of a physical key being reported lost/stolen.

- Enforcement of Facility Access Policies
- Report violations of this policy to the restricted area’s department team leader, supervisor, manager, or director, or the Security Officer.
- Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.
- Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services from APS.
- Workstation Security
- Workstations may only be accessed and utilized by authorized workforce members to complete assigned job/contract responsibilities.
- All workforce members are required to monitor workstations and report unauthorized users and/or unauthorized attempts to access systems/applications as per the System Access Policy.
- All workstations purchased by APS are the property of APS and are distributed to users by the company.

Building Standards per Location

All entry points are secured by card readers and have cameras for additional monitoring as needed.

- **Naples, FL** Office
- The building is unlocked Monday-Friday from 9am-4pm
- After hours the building is secured and requires an access code for entry
- The main entry to our office suite is open during normal business hours (M-F 8am-5pm)
- APS office space is secured and requires a key entry for after hours access

Facility Access Control Process

Keys are stored in a locked cabinet until they are issued.

NEW HIRES

New Hire access is assigned based on new hire notice issued through Rally.

- New Hire access is typically activated the day prior to start date
- Once activated the key is stored in a locked cabinet until issued to new hire.

SEPARATIONS

Separation notices are issued through Rally.

- Immediate separation notices are processed when issued
- Future separation notices are pre-scheduled for deactivation prior to termination date

SPECIAL ACCESS REQUESTS

Special access areas require additional approvals for access. If documented approver is unavailable, COO may act as approver.

Maintenance & Repairs

All maintenance, repairs and modifications to our access control system will be handled by the local vendor that supports our system.

All documents regarding maintenance, repair or modification will be stored in the physical security folder located on the APS Google Workspace site.

Reporting and Auditing

Records are owned reviewed and maintained by the Facility Manager.

12.2.2 Data Center Security

Physical security of data centers is ensured by the cloud infrastructure service provided, AWS.

Clean Desk Policy and Procedures

Employees must secure all sensitive/confidential information in their workspace at the conclusion of the work day and when away from their workspace. This includes both electronic and physical information such as:

- computer workstations, laptops, and tablets
- removable storage devices including CDs, DVDs, USB drives, and external hard drives
- printed materials

Computer workstations/laptops must be locked (password protected) when physically unattended. Portable devices such as laptops and tablets should be taken home at the conclusion of the work day.

Removable storage devices and printed documents must be treated as sensitive material and locked in a drawer or similar when not in use. Printed materials must be immediately removed from printers or fax machines. Passwords must not be written down or stored physically.

Keys and access cards used for access to sensitive or restricted information/areas must not be left unattended anywhere in the office.

This same policy applies for the work area of remote workers.

13. Asset Inventory Management

`Last Reviewed: 2025-02-17:19:44:43-UTC`

You can't protect what you can't see. Therefore, it is imperative for APS to maintain an accurate and up-to-date inventory of both its physical and digital assets.

More details on data inventory and data lifecycle management is documented separately in Data Management.

13.1 Policy Statements

APS policy requires that:

(a) IT and/or Security must maintain an inventory of all critical company assets, both physical and logical.

(b) All assets should have identified owners and be tagged with a risk/data classification.

13.2 Controls and Procedures

13.2.1 Physical Asset Inventory

APS IT leverages a SaaS-based IT asset management system, NetSuite, to maintain inventory of all company owned physical computing equipment, including but not limited to:

- servers
- workstations
- laptops
- printers
- networking equipment

Each record includes details of the physical device such as manufacturer, model serial number as well as ownership details and location.

The movement of computing hardware and electronic media is maintained as part of the records, including media re-use and ownership reassignment.

APS IT manager is responsible for ensuring each physical asset is entered into and an up-to-date record is maintained in the IT asset management system.

All company-owned devices are subject to a complete data wipe if deemed necessary, such as in the case of device infection or re-purpose. This data wipe will be carried out by the IT manager. Such a wipe would occur without access to or backup of the system.

Plausible deniability is maintained through the following procedure:

- When equipment is shipped the full disk encryption (Bitlocker, or other) key is disabled
- When equipment is unpacked a full disk wipe is performed without backup
- Upon completion full disk encryption master key is destroyed
- Latest version of approved operating system is reloaded and updates are performed
- Unit is entered back into corporate inventory

13.2.2 Digital Asset Inventory

APS Security team uses an automated system to query across our cloud-based infrastructure, including but is not limited to AWS, to obtain detailed records of all digital assets, including but not limited to:

- Virtual machines
- AWS EC2 instances
- AWS S3 repositories
- AWS Lambda functions
- Security agents
- Source code repositories
- User accounts

The records are stored in a database system maintained by APS security team. Records are tagged with owner/project and classification when applicable. All records are kept up to date via automation.

13.2.3 Paper Records

APS does not use paper records for any sensitive information. Use of paper for recording and storing sensitive data is against APS policies.

14. Data Management Policy

`Last Reviewed: 2025-02-17:19:44:43-UTC`

This policy outlines the requirements and controls/procedures APS has implemented to manage the end-to-end data lifecycle, from data creation/acquisition to retention and deletion.

Additionally, this policy outlines requirements and procedures to create and maintain retrievable exact copies of

PII and other critical customer/business data.

Data backup is an important part of the day-to-day operations of APS. To protect the confidentiality, integrity, and availability of sensitive and critical data, both for APS and APS Customers, complete backups are done daily to assure that data remains available when it needed and in case of a disaster.

14.1 Policy Statements

APS policy requires that

(a) Data should be classified at time of creation or acquisition according to the APS data classification model, by labeling or tagging the data.

(b) Maintain an up-to-date inventory and data flows mapping of all critical data.

(c) All business data should be stored or replicated to a company controlled repository, including data on end-user computing systems.

(d) Data must be backed up according to its level defined in APS data classification.

(e) Data backup must be validated for integrity.

(f) Data retention period must be defined and comply with any and all applicable regulatory and contractual requirements. More specifically,

- Data and records belonging to APS platform customer must be retained per APS product terms and conditions and/or specific contractual agreements.

(g) By default, all security documentation and audit trails are kept for a minimum of seven years, unless otherwise specified by APS data classification, specific regulations or contractual agreement.

14.2 Controls and Procedures

14.2.1 Data Classification Model

APS defines the following four classifications of data:

- **Critical**
- **Confidential**
- **Internal**
- **Public**

Definitions and Examples

Critical data includes data that must be protected due to regulatory requirements, privacy, and/or security sensitivities.

Unauthorized disclosure of critical data may result in major disruption to business operations, significant cost, irreparable reputation damage, and/or legal prosecution to the company.

External disclosure of critical data is strictly prohibited without an approved process and agreement in place.

Example Critical Data Types includes

- PII
- PCI or CHD (cardholder data)
- Production Security data, such as
- Production secrets, passwords, access keys, certificates, etc.
- Production security audit logs, events, and incident data

Confidential and proprietary data represents company secrets and is of significant value to the company.

Unauthorized disclosure may result in disruption to business operations and loss in value.

Disclosure requires the signing of NDA and management approval.

Example Confidential Data Types includes

- Business plans
- Employee/HR data
- News and public announcements (pre-announcement)
- Patents (pre-filing)
- Specialized source codes
- Non-production Security data, including
- Non-prod secrets, passwords, access keys, certificates, etc.
- Non-prod security audit logs, events, reports, and incident data
- Audit/compliance reports, security architecture docs, etc.

Internal data contains information used for internal operations.

Unauthorized disclosure may cause undesirable outcome to business operations.

Disclosure requires management approval. NDA is usually required but may be waived on a case-by-case basis.

Example Internal Data Types includes

- Internal documentation
- Policies and procedures
- Product roadmaps
- Most source codes

Public data is Information intended for public consumption. Although non-confidential, the integrity and availability of public data should be protected.

Example Internal Data Types includes

- News and public announcements (post-announcement)
- Marketing materials
- Product documentation
- Contents posted on company website(s) and social media channel(s)

14.2.2 Data Handling Requirements Matrix

Requirements for data handling, such as the need for encryption and the duration of retention, are defined according to the APS Data Classifications.

Data	Labeling or Tagging	Segregated Storage	Endpoint Storage	Encrypt At Rest	Encrypt In Transit	Encry Use
Critical	Required	Required	Prohibited	Required	Required	Requi
Confidential	Required	N/R	Allowed	Required	Required	Requi
Internal	Required	N/R	Allowed	N/R	N/R	N/R
Public	N/R	N/R	Allowed	N/R	N/R	N/R

N/R = Not Required

† customer-owned data is stored for as long as they remain as a APS customer, or as required by regulations, whichever is longer. Customer may request that their data be deleted at any time unless retention is required by law or regulation.

14.2.3 Backup and Recovery

Customer Data

APS stores data in a secure production account in AWS, using a combination of S3 and EBS By default, Amazon S3 provides durable infrastructure to store important data and is designed for durability of 99.999999999% of objects.

APS performs automatic backup of all customer and system data to protect against catastrophic loss due to unforeseen events that impact the entire system. An automated process will back up all data to a separate AWS region in the same country (e.g. US East to US West). By default, data will be backed up daily. The backups are encrypted in the same way as live production data.

Customers can also utilize the APS Application Programming Interface (API) to extract and store their data elsewhere. Standard API usage fees will apply.

Source code

APS stores its source in git repositories hosted by GitHub.

Source code repositories are backed up to APS's AWS S3 infrastructure account on a weekly basis with a common set of configuration for each repository to enforce SDLC processes.

In the event that GitHub suffers a catastrophic loss of data, source code will be restored from the backups in AWS S3.

Because AWS and GitHub can both host git repositories, we are able to leverage git's ability to maintain a full history of all changes to our git repos via the commit log.

Business records and documents

Each data owner/creator is responsible for maintaining a backup copy of their business files local on their laptop/workstation to the appropriate location on APS Google Workspace site. Examples of business files include, but are not limited to:

- Documents (e.g. product specs, business plans)
- Presentations
- Reports and spreadsheets
- Design files/images/diagrams
- Meeting notes/recordings
- Important records (e.g. approval notes)

Unless the local workstation/device has access to **Critical** data, backups of user workstations/devices are self managed by the device owner. Backups may be stored on an external hard drive or using a cloud service such as iCloud if and only if the data is both encrypted and password protected (passwords must meet APS requirements).

15. Data Protection

`Last Reviewed: 2025-02-17:19:44:43-UTC`

APS takes the confidentiality and integrity of its customer data very seriously. As stewards and partners of APS Customers, we strive to assure data is protected from unauthorized access and that it is available when needed. The following policies drive many of our procedures and technical controls in support of the APS mission of data protection.

Production systems that create, receive, store, or transmit Customer data (hereafter “Production Systems”) must follow the requirements and guidelines described in this section.

15.1 Policy Statements

APS policy requires that:

(a) Data must be handled and protected according to its classification requirements and following approved encryption standards, if applicable.

(b) Whenever possible, store data of the same classification in a given data repository and avoid mixing sensitive and non-sensitive data in the same repository. Security controls, including authentication, authorization, data encryption, and auditing, should be applied according to the highest classification of data in a given repository.

(d) All Production Systems must disable services that are not required to achieve the business purpose or function of the system.

(e) All access to Production Systems must be logged, following the APS Auditing Policy.

(f) All Production Systems must have security monitoring enabled, including activity and file integrity monitoring, vulnerability scanning, and/or malware detection, as applicable.

15.2 Controls and Procedures

15.2.1 Data Protection Implementation and Processes

Data is classified and handled according to the APS Data Handling Specifications and Data Classification document.

Critical, confidential and internal data will be tagged upon creation, if tagging is supported. Each tag maps to a data type defined in the data classification scheme, which then maps to a protection level for encryption, access control, backup, and retention. Data classification may alternatively be identified by its location/repository. For example, source codes in APS’s GitHub repos are considered “Internal” by default, even though a tag is not directly applied to each source file.

Critical and confidential data is always stored and transmitted securely, using approved encryption standards. More details are specified in APS’s Data Classification and Handling document.

All IT systems that process and store sensitive data follow the provisioning process, configuration, change management, patching and anti-malware standards as defined in Configuration and Change Management document.

Customer/Production Data Protection

APS hosts on Amazon Web Services in the US-East region by default. Data is replicated across multiple availability zones for redundancy and disaster recovery.

All APS employees, systems, and resources adhere to the following standards and processes to reduce the risk of compromise of Production Data:

1. Implement and/or review controls designed to protect Production Data from improper alteration or destruction.
2. Ensure that confidential data is stored in a manner that supports user access logs and automated monitoring for potential security incidents.
3. Ensure APS Customer Production Data is segmented and only accessible to Customer authorized to access data.
4. All Production Data at rest is stored on encrypted volumes using encryption keys managed by APS. Encryption at rest is ensured through the use of automated deployment scripts referenced in Configuration and Change Management.
5. Volume encryption keys and machines that generate volume encryption keys are protected from unauthorized access. Volume encryption key material is protected with access controls such that the key material is only accessible by privileged accounts.
6. Encrypted volumes use approved cipher algorithms, key strength, and key management process as defined in §12.3.1 above.

Access

APS employee access to production is guarded by an approval process and by default is disabled. When access is approved, temporary access is granted that allows access to production. Production access is reviewed by the security team on a case by case basis.

Separation

Customer data is logically separated at the database/datastore level using a unique identifier for the institution. The separation is enforced at the API layer where the client must authenticate with a chosen institution and then the customer unique identifier is included in the access token and used by the API to restrict access to data to the institution. All database/datastore queries then include the institution identifier.

Backup and Recovery

For details on the backup and recovery process, see controls and procedures defined in Data Management.

Monitoring

APS uses AWS CloudWatch/CloudTrail to monitor the entire cloud service operation. If a system failure and alarm is triggered, key personnel are notified by text, chat, and/or email message in order to take appropriate corrective action. Escalation may be required and there is an on-call rotation for major services when further support is necessary.

APS uses a security agent to monitor production systems. The agents monitor system activities, generate alerts on suspicious activities and report on vulnerability findings to a centralized management console.

15.2.2 Protecting Data At Rest

Encryption of Data at Rest

All databases, data stores, and file systems are encrypted with AES-256 and hardware keys.

Local Disk/Volume Encryption

Encryption and key management for local disk encryption of end-user devices follow the defined best practices for Windows, macOS, and Linux/Unix operating systems, such as Bitlocker and FileVault.

15.2.3 Protecting Data In Transit

1. All external data transmission is encrypted end-to-end using encryption keys managed by APS. This includes, but is not limited to, cloud infrastructure and third party vendors and applications.

2. Transmission encryption keys and systems that generate keys are protected from unauthorized access. Transmission encryption key materials are protected with access controls, and may only be accessed by privileged accounts.
3. Transmission encryption keys use a minimum of 2048-bit RSA keys, or keys and ciphers of equivalent or higher cryptographic strength (e.g., 256-bit AES session keys in the case of IPSec encryption).
4. Transmission encryption keys are limited to use for one year and then must be regenerated.
5. For all APS APIs, enforcement of authentication, authorization, and auditing is used for all remote systems sending, receiving, or storing data.
6. System logs of all transmissions of Production Data access are kept. These logs must be available for audit.

Algorithm Requirements

- Ciphers in use must meet or exceed the set defined as “AES-compatible” or “partially AES-compatible” according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.
- Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-3 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

Signature Algorithms

- Algorithm: ECDSA
- Key Length (minumum): P-256
- Additional Comment: Cisco Legal recommends RFC6090 compliance to avoid patent infringement.
- Algorithm: RSA
- Key Length (minumum): 2048
- Additional Comment: Must use a secure padding scheme. PKCS#7 padding scheme is recommended. Message hashing required.
- Algorithm: LDWM
- Key Length (minumum): SHA256
- Additional Comment: Refer to LDWM Hash-based Signatures Draft

Hash Function Requirements

In general, APS adheres to the NIST Policy on Hash Functions.

Key Agreement and Authentication

- Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).
- End points must be authenticated prior to the exchange or derivation of session keys.
- Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.
- All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.
- All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

Key Generation

- Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.
- Key generation must be seeded from an industry standard random number generator (RNG). For examples, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.

Encryption of Data in Transit

All network connections, whether covered by regulations or not, whether transiting public networks or not, are encrypted and authenticated using at least TLS 1.2 (a strong protocol), at least ECDHE_RSA with P-256 (a strong key exchange), and at least AES_128_GCM (a strong cipher). Connections to and within the Amazon Web Services cloud occur in the context of either the CloudFront content distribution network (CDN) or Application Load Balancers (ALBs). ALBs and CloudFront distributions must be configured with at least the TLSv1.2_2019 security policy as defined here. APS recognizes that a majority of its business partners in the hospitality industry are slow to adopt the significantly stronger protocols and ciphers specified in the TLSv1.2_2021 policy. It is APS policy to strongly encourage all business partners to upgrade their technology stacks in support of stronger encryption.

Reduced strength cryptography is available for customers with older equipment upon request and with approval from the Security Team. In these cases the transport **MUST NOT** be used for transmission of sensitive data.

Special note on email

It must be noted that regular email is **not** encrypted, and as such, **must not** be used to transmit sensitive data such as credit card details.

Data protection via end-user messaging channels

Restricted and sensitive data **must not** be sent over electronic end-user messaging channels such as email or chat, unless end-to-end encryption is enabled.

15.2.4 Protecting Data In Use

Data in Use, sometimes known as Data in Process, refers to active data being processed by systems and applications which is typically stored in a non-persistent digital state such as in computer random-access memory (RAM), CPU caches, or CPU registers.

Protection of data in use relies on application layer controls and system access controls. See the Production Security / SDLC and Access sections for details.

APS applications implement logical account-level data segregation to protect data in a multi-tenancy deployment. In addition, APS applications may incorporate advanced security features such as Runtime Application Self Protection (RASP) modules and Attribute Based Access Control (ABAC) for protection of data in use.

15.2.5 Encryption Key Management

APS uses AWS Key Management Service (KMS) for encryption key management.

- KMS keys are unique to APS environments and services.
- KMS keys are automatically rotated yearly.

15.2.6 Certificate Management

APS uses AWS Certificate Manager (ACM) and LetsEncrypt for certificate management.

- Certificates are renewed automatically.
- Security team monitors the certificates for expiration, potential compromise and use/validity. Certificate revocation process is invoked if the certificate is no longer needed or upon discovery of potential compromise.

15.2.7 Data Integrity Protection

When appropriate, APS engineering should implement “Versioning” and “Lifecycle”, or equivalent data management mechanism, such that direct edit and delete actions are not allowed on the data to prevent accidental or malicious overwrite. This protects against human errors and cyberattacks such as ransomware.

In AWS, the IAM and S3 bucket policy in production will be implemented accordingly when the environments are configured. When changes must be made, a new version is created instead of editing and overwriting existing data.

- All edits create a new version and old versions are preserved for a period of time defined in the lifecycle policy.
- Data objects are “marked for deletion” when deleted so that they are recoverable if needed within a period of time defined according to the data retention policy.
- Data is archived offsite – i.e. to separate AWS account availability zone and/or region.

Additionally, all access to sensitive data is authenticated, and audited via logging of the infrastructure, systems and/or application.

16. Secure Software Development and Product Security

`Last Reviewed: 2025-02-17:19:44:43-UTC`

APS development team follows the latest security best practices when developing software, and automates security testing throughout development lifecycle whenever possible.

- Remediation:
- Follows defined vulnerability management lifecycle
- Ensures no high risk security vulnerability is in production

Details about the APS software application architecture and security are documented on the product development / engineering wiki.

16.1 Policy Statements

APS policy requires that:

1. APS software engineering and product development is required to follow security best practices. Product should be “Secure by Design” and “Secure by Default”.
2. Quality assurance activities must be performed. This may include
    - peer code reviews prior to merging new code into the main development branch (e.g. master branch); and
    - thorough product testing before releasing to production (e.g. unit testing and integration testing).
1. Risk assessment activities (i.e. threat modeling) must be performed for a new product or major changes to an existing product.
2. Security requirements must be defined, tracked, and implemented.

1. All critical or high severity security findings must be remediated prior to each release.
2. All critical or high severity vulnerabilities discovered post release must be remediated in the next release or within the defined, predetermined timeframe.
3. Any exception to the remediation of a finding must be documented and approved by the security team.

16.2 Controls and Procedures

16.2.1 Software Development Process

Overview

Software development at APS follows a release strategy that provides traceability for production software changes. Features, enhancements, and bugs are written up as Issues in Rally. An engineer on a small team proposes changes necessary and creates a review for the team (GitHub). Continuous integration (Jenkins) kicks off unit and functional tests which pass before changes are deployed to the development environment where Product Owner tests are run before the new code replaces the existing in-service code (test then deploy model).

APS practices continuous delivery of code into production through multiple environments: development and production. The deploy process and infrastructure roll-out are written as code (using technologies such as AWS CloudFormation) and managed under source control.

APS’s lower environment (dev) provides an ecosystem of sample data sets that exercise the application and services when test automation is run. The test environment is where the system is stressed for performance and scalability. Performance and

scalability changes are driven by metric data captured through monitoring and logging (metrics before and after change – typically captured as part of the issue description/writeup).

Deployments to production are gated by change control process where an issue is opened which identify what is new/changed (Rally). Sign-offs are recorded by development, product owner, and product management. Production roll-outs happen on a regular basis without impact to service. This continuous process allows for security updates to roll out regularly and with urgency. If there is impact to production, a rollback is performed to restore service and whatever caused the problem is reverted from source. This restarts the re-proposal approval process of source changes. This process keeps the set of differences between the development environment and the production environment as low as possible.

In the continuous delivery mindset, features are not released by the deployment of code into production, instead features are enabled in production at the appropriate time (dark launching). Feature toggle enablement in production is gated by a change control ticket (Rally) that follows the software roll-out approval process. Feature toggle enablement in production can have a few more dependencies than code. Those dependencies include things like external documentation, early access programs, and internal playbooks for supporting the feature.

Secure Development Standards

Traceability of code changes allow for our software to be a living entity. Our current system for documenting changes is Rally. Every commit should have a Rally supplied that describes contextually why this change is necessary and reasonable. These artifacts over time allow for one to trace the lineage of why our production software and services change over time.

All APS `git` repositories have a company standard configuration from a GitHub perspective. This standard is a guideline and can be relaxed when those exceptions are needed. One example of an exception, is the `wiki` repository, as editing a wiki and always requiring a PR in this setting slows down ‘flow’.

- Code: <#>
- Repo settings: <#>
- Build: <#>

NOTE: Not all projects (and repos) follow this standard, certain projects might be excluded (e.g. `wiki`).

Developers follow the master branch strategy and code review process below:

1. All development uses the main branch used for the current release. Any changes required for a new feature or defect fix are committed to that branch.
- These changes must be covered under 1) a unit test where possible, or 2) integration tests.
- Integration tests are *required* if unit tests cannot reliably exercise all facets of the change.
2. Developers are strongly encouraged to follow the commit message conventions suggested by GitHub.
- Commit messages should be wrapped to 72 characters.
- Commit messages should be written in the present tense. This convention matches up with commit messages generated by commands like git merge and git revert.
- Additionally, the commit messages should start with the Rally Issue ID when applicable.
3. Code reviews are performed as part of the peer review swim lane. Once a change is ready for review, the author(s) will notify other engineers using an appropriate mechanism, typically by adding reviewers to the ticket.
- Other engineers will review the changes, using the guidelines above.
- Engineers should note all potential issues with the code; it is the responsibility of the author(s) to address those issues or explain why they are not applicable.
- If changes/commits are made, it should reset previous approvals and require review and approvals again before the code can be deployed.

1. If the feature or defect interacts with sensitive data, or controls access to sensitive data, or contains security/risky infrastructure changes to the target environment, the code changes must be reviewed by the Security team before the feature is marked as complete.
- This review must include a security analysis for potential vulnerabilities such as those listed in the OWASP Top 10.
- This review must also verify that any actions performed by authenticated users will generate appropriate audit log entries.

Release Strategy

Features, enhancements, and bugs are written up as issues (Rally). An engineer on a small team proposes changes necessary and creates a review for the team (GitHub). Continuous integration (Jenkins) kicks off unit and functional tests which pass before changes are deployed to the development environment. Small teams can decide to follow a source-control branching strategy that makes sense: git-flow, github flow.

APS practices continuous delivery of code into production through multiple environments: development then production. The deploy process and infrastructure roll-out are written as code (IaC) and managed under source control.

APS's lower environment (dev) provides an ecosystem of sample data sets that can be used to exercise the application and services when test automation is run. The test environment is where the system is stressed for performance and scalability. Performance and scalability changes are driven by metric data captured through monitoring and logging (metrics before and after change - typically captured as part of the issue description/writeup).

Deployments to production are gated by change management process where an issue is opened which identify what is new/changed (Rally). Sign-offs are recorded by development, testing, security, and product management. Production roll-outs happen on a regular basis without impact to service. This continuous process allows for security updates to roll out regularly and with urgency. If there is impact to production, a rollback is performed to restore service and whatever caused the problem is reverted from source. This restarts the re-proposal approval process of source changes.

This process keeps set of differences between the development environment and the production environment as low as possible.

Features may be released via code deployments or features may be enabled in production at an appropriate time (dark launching). Feature toggle enablement in production is gated by the same change management ticket (Rally) that follows the software roll-out approval process. Feature toggle enablement in production can have a few more dependencies than code. Those dependencies include things like external documentation, early access programs, and internal playbooks for supporting the feature.

Detailed process and procedures for code promotion and production release: See Configuration and Change Management.

16.2.2 Source Code Management

APS development/engineering team uses GitHub for source code management. Access to GitHub and its configuration standards include:

- All developers must authenticate to gain access to GitHub and code repos hosted on GitHub according to standards and procedures defined in the Access Policy:
- Access control to the GitHub web interface must be enabled, via SSO and/or MFA if applicable
- SSH public/private key access may be used for command line or `git` access to the code repos
- All code repos in GitHub follow these configuration standards:
- All repos must have an owner identified and listed
- All repos are by default `private`

16.2.3 High Level Application Security Requirements

All APS software must be developed to include the following general application security principles and requirements. Web applications must also protect itself against the OWASP Top 10 vulnerabilities.

1. Protect sensitive customer data such as PII and account passwords. Encrypt data stored (at rest).
2. Secure data in transit and customer communications via TLS.
3. Provision strong access control (authentication and authorization). Prevent and report unauthorized access.
4. Log all transactions and activities to be able to tell who did what, when, where, and how. Mask or remove sensitive data in logs.
5. Implement client security at application endpoints (e.g. browser, mobile app).
6. Communicate securely across application endpoints and between service consumers/producers.
7. Use secure defaults to ensure security when in all error conditions.
8. Check and maintain the security of all third party and open source libraries/components/dependencies.
9. Validate all data inputs; encode data outputs when appropriate.
10. Deploy and configure applications securely to production.
11. Perform regular vulnerability analysis and apply security patches promptly.
12. Secure privileged access to production environments and ensure ongoing application monitoring.

All software code must complete a set of security scans/testing prior to being deployed to production, including open source dependency scanning, static and dynamic application security testing, as well as periodic penetration testing.

Pre-production testing is performed with nonproduction data in nonproduction environments. Health checks are performed regularly or automated in production.

Software vulnerability identified through any of the above processes shall be reported and tracked following APS Vulnerability Management process as defined in the Vulnerability Management Policy and Procedures.

16.2.4 Secure Design and Application Threat Modeling

APS Security Team in collaboration with development team performs full Application Threat Modeling and Risk Assessment on per-application basis using a custom approach that relies on industry standards and best practices.

Major application updates are captured via an **RFC** process. The RFC template includes **Security Consideration** as a required section. This section is used to document abuse cases including:

- risks identified,
- attack vectors, and
- mitigating controls.

Each RFC is required to capture sufficient details of the feature/component to be developed, including use cases, motivation and outcome, and the following design details as applicable:

- authentication/authorization mechanisms,
- network communications,
- data encryption,
- cloud services used,
- logging/auditing,
- data flow diagram/description,
- edge cases, drawbacks, and alternatives.

The RFC must be approved prior to implementation. Security team is included in RFC reviews via email.

Platform Design and DevOps Security Details

Documentation on the APS Engineering Wiki may include additional security specifications as well as the security design and implementation details of the APS Platform and its supporting operations.

16.2.5 Access Control of the Application (Identification, Authentication, Authorization, Accounting)

APS external software application that is customer facing with access to customer specific data, including sensitive information such as PII , implements strong access control, covering the Identification, Authentication, Authorization, and Accounting/ Auditing (IAAA) of access and user activity.

The implementation ensures that

- the user requesting access is the one claimed (Identification and Authentication);
- only users authorized to access specific data are allowed to (Authorization); and
- their access activities are logs (Accounting/Auditing) according to the APS auditing standards.

The current implementation leverages AWS Cognito for user identity management and access.

The backend platform implements granular Attribute-Based Access Control (ABAC) for granting access to specific services and data based on the attribute(s) of a principal (i.e. user requesting access – an attribute could be the role or group membership or organization the user belongs to) and the attribute(s) of the requested resource (i.e. data or service – an attribute could be the project this data belongs to).

More implementation details are documented on the internal Engineering wiki.

16.2.6 Penetration Testing

External Penetration Testing

An external penetration testing is performed at least once a year by a qualified security researcher / ethical hacker on the security team internally and/or with an external security consulting firm.

16.2.7 Outsourced Software Development

APS requires all outsourced software development to follow the same rigor and process as internal engineering. Outsourced developers must develop in our secure environment, accept and follow our security policies and procedures, and comply with the same secure coding standards, including:

- Receive regular OWASP or equivalent secure coding training.
- Follow the same source control, code review, and security code scanning procedures as defined.
- Install endpoint compliance agent that checks to make sure firewall, encryption, patching, password policy, screensaver password, and other required protection is properly configured.

Additionally, the third party firm providing outsourced development services must demonstrate that they have conducted the appropriate screening during hiring.

16.2.8 Production System Monitoring and Paging

Software and systems deployed in production are monitored 24/7 for health check and other major/critical error conditions. The on call team is paged via PagerDuty in the event an error or failure is detected.

Notifications via additional channels such as Slack and email are also configured.

17. Configuration and Change Management

`Last Reviewed: 2025-02-17:19:44:43-UTC`

APS standardizes and automates configuration management through the use of automation scripts as well as documentation of all changes to production systems and networks. Automation tools automatically configure all APS systems according to established and tested policies, and are used as part of our Disaster Recovery plan and process.

17.1 Policy Statements

APS policy requires that:

(a) All production changes, including but not limited to software deployment, feature toggle enablement, network infrastructure changes, and access control authorization updates, must be invoked through approved change management process.

(b) Each production change must maintain complete traceability to fully document the request, including requestor, date/time of change, actions taken and results.

(c) Each production change must be fully tested prior to implementation.

(d) Each production change must include a rollback plan to back out the change in the event of failure.

(e) Each production change must include proper approval.

- The approvers are determined based on the type of change.
- Approvers must be someone other than the author/executor of the change.
- Approvals may be automatically granted if certain criteria is met. The auto-approval criteria must be pre-approved by the Security Officer and fully documented and validated for each request.

17.2 Controls and Procedures

17.2.1 Configuration Management Processes

1. Configuration management is automated using industry-recognized tools.
2. All changes to production systems, network devices, and firewalls are reviewed and approved by Security team before they are implemented to assure they comply with business and security requirements.
3. All changes to production systems are tested before they are implemented in production.
4. Implementation of approved changes are only performed by authorized personnel.
5. Tooling is used to generate an up to date system inventory.

- All systems are categorized and labeled by their corresponding environment, such as *dev*, *test*, and *prod*.
- All systems are classified and labeled based on the data they store or process, according to APS data classification model.
- The Security team maintains automation which monitors all changes to IT assets, generates inventory lists, using automatic IT assets discovery, and services provided by each cloud provider.
- IT assets database is used to generate the diagrams and asset lists required by the Risk Assessment phase of APS's Risk Management procedures
- APS Change Management process ensures that all asset inventory created by automation is reconciled against real changes to production systems. This process includes periodic manual audits and approvals.
- During each change implementation, the change is reviewed and verified by the target asset owner as needed.

6. APS uses the Security Technical Implementation Guides (STIGs) published by the Defense Information Systems Agency as a baseline for hardening systems.

```
* EC2 instances in AWS are provisioned using only hardened and approved
  Amazon Machine Images (AMIs).
* Docker containers are launched using only approved Docker images that have
  been through security testing.
```

1. All IT assets in APS have time synchronized to a single authoritative source.
   - On-premise systems are configured to point to an internal NTP server.
   - The internal NTP server and all AWS instances are pointing to the same set of ntp.org servers.
   - Clocks are standardized to the UTC time zone
2. All frontend functionality (e.g. user dashboards and portals) is separated from backend (e.g. database and app servers) systems by being deployed on separate servers or containers.
3. All software and systems are required to complete full-scale testing before being promoted to production.
4. All code changes are reviewed to assure software code quality, while in development, to proactively detect potential security issues using pull-requests and static code analysis tools. More details can be found in the *Software Release / Code Promotion* section.

17.2.2 Configuration Monitoring and Auditing

All infrastructure and system configurations, including all software-defined sources, are centrally aggregated to a configuration management database (CMDB) – AWS CloudTrail.

Configuration auditing rules are created according to established baseline, approved configuration standards and control policies. Deviations, misconfigurations, or configuration drifts are detected by these rules and alerted to the security team.

17.2.3 Production Systems Provisioning

1. Before provisioning any systems, a request must be created and approved in the Rally Infrastructure (IN) project.
   - Rally access requires authenticated users.
   - Security grants access to the Rally IN project following the procedures covered in the Access Establishment and Modification section.
2. The security team must approve the provisioning request before any new system can be provisioned, unless a pre-approved automation process is followed.
3. Once provisioning has been approved, the implementer must configure the new system according to the standard baseline chosen for the system's role.
4. If the system will be used to store sensitive information, the implementer must ensure the volume containing this sensitive data is encrypted.
5. Sensitive data in motion must always be encrypted.
6. A security analysis is conducted once the system has been provisioned. This can be achieved either via automated configuration/ vulnerability scans or manual inspection by the security team. Verifications include, but is not limited to:
   - Removal of default users used during provisioning.
   - Network configuration for system.
   - Data volume encryption settings.
   - Intrusion detection and virus scanning software installed.
7. The new system is fully promoted into production upon successful verification against corresponding APS standards and change request approvals.

17.2.4 User Endpoint Security Controls and Configuration

1. Employee laptops, including Windows, Mac, and Linux systems, are configured either
   - Manually by IT or the device owner; or
   - Automatically using a configuration management tool or equivalent scripts.

2. The following security controls are applied at the minimum:
   - Disk encryption
   - Unique user accounts and strong passwords
   - Approved NTP servers
   - Approved security agents including Anti-Virus software
   - Locking after 10 mins of inactivity
   - Auto-update of security patches
3. The security configurations on all end-user systems are inspected by Security through either a manual periodic review or an automated compliance auditing tool.

17.2.5 Anti-Virus policy

- For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.
- A licensed anti-virus software package must be utilized for all computer and system components (any network component, server or application included in or connected to the cardholder data environment) within the cardholder environment and for all computers not directly associated with the cardholder environment.
- The licensed anti-virus software utilized must be the most current version available.
- All computers and system components within the cardholder environment must have standard, supported anti-virus software installed.
- The anti-virus software must be active, must be scheduled to perform virus checks at regular intervals and must have its virus definition and all other associated software files kept current.
- The anti-virus software must be enabled for automatic updates and periodic scans.
- All computers not directly associated with the cardholder environment must have standard, supported anti-virus software installed.
- The anti-virus software for all computers not directly associated with the cardholder environment must also be active, scheduled to perform virus checks at regular intervals and must have its virus definitions and all other associated software files kept current.
- No user shall disable or tamper with the configuration of anti-virus software installed on any computer or device.

17.2.6 Server Hardening Guidelines and Processes

1. **Linux System Hardening:** Linux systems have their baseline security configuration applied via automation tools. These tools cover:
   - Ensuring that the machine is up-to-date with security patches and is configured to apply patches in accordance with our policies.
   - Stopping and disabling any unnecessary OS services.
   - Apply applicable CIS benchmarks or DISA STIGs to OS and applications.
   - Configuring 15-minute session inactivity timeouts for SSH sessions.
   - Installing and configuring the virus scanner.
   - Installing and configuring the NTP daemon, including ensuring that modifying system time cannot be performed by unprivileged users.
   - Configuring disk volumes for providers that do not have native support for encrypted data volumes, including ensuring that encryption keys are protected from unauthorized access.
   - Configuring authentication to the centralized Directory Services servers, if used.
   - Configuring audit logging as described in the Auditing Policy section.

2. **Windows System Hardening:** Windows systems have their baseline security configuration applied via the combination of Group Policy settings and/or automation scripts. These baseline settings cover:

- Joining the Windows Domain Controller and applying the Active Directory Group Policy configuration (for AD-managed systems only).
- Ensuring that the machine is up-to-date with security patches and is configured to apply patches in accordance with our policies.
- Apply applicable DISA STIGs to OS and applications.
- Stopping and disabling any unnecessary OS services.
- Configuring session inactivity timeouts.
- Installing and configuring security protection agents such as anti-virus scanner.
- Configuring transport encryption according to the requirements described in the Mobile Device Security and Disposable Media Management section.
- Configuring the system clock to point to approved NTP servers and ensuring that modifying system time cannot be performed by unprivileged users.
- Configuring audit logging as described in the Auditing Policy section.

3. Any additional configuration changes applied to hardened Windows systems must be clearly documented by the implementer and reviewed by the Security team.

17.2.7 Configuration and Provisioning of Management Systems

1. Provisioning management systems such as configuration management servers, remote access infrastructure, directory services, or monitoring systems follows the same procedure as provisioning a production system.
2. Critical infrastructure roles applied to new systems must be clearly documented by the implementer in the change request.

17.2.8 Configuration and Management of Network Controls

All network devices and controls on a sensitive network are configured such that:

- Vendor provided default configurations are modified securely, including
- default encryption keys,
- default SNMP community strings, if applicable,
- default passwords/passphrases, and
- other security-related vendor defaults, if applicable.
- In addition to standard time-based rotation, encryption keys and passwords are changed any time anyone with knowledge of the keys or passwords leaves the company or assumes a position not authorized for such access.
- Traffic filtering (e.g. firewall rules) and inspection (e.g. Network IDS/IPS or AWS VPC flow logs) are enabled.
- An up-to-date network diagram is maintained.

In AWS, network controls are implemented using Virtual Private Clouds (VPCs) and Security Groups. The configurations are managed as code and stored in approved repos. All changes to the configuration follow the defined code review, change management and production deployment approval process.

17.2.9 Provisioning AWS Accounts

AWS Account Structure / Organization

APS maintains a single Organization in AWS, maintained in a top-level AWS account (master). Sub-accounts are connected that each hosts separate workloads and resources in its own sandboxed environment. The master account itself handles aggregated billing for all connected sub-accounts but does not host any workload, service or resource, with the exception of Route53, ECR (for approved containers), and CloudTrail log aggregation hosting. DNS records for subdomains are maintained in the corresponding sub-accounts.

Access to each account is funneled through our designated SSO provider, which establishes a trust relationship to a set of predefined roles in the master account. Once authenticated, a user then leverages AWS IAM Assume Role capability to switch to a sub-account to access services and resources.

The account and network structure looks like the following:

```
SSO/IdP ── APS-master
            │  └── billing and root DNS records
            │  └── master container repository (for approved containers)
            │  └── CloudTrail aggregation (write-only S3 bucket)
            │
            ├── APS-dev
            │    └── VPC
            │        └── Subnets
            │             └── Security-Groups
            │                  └── EC2 instances
            │                       └── Docker containers
            │
            ├── APS-prod-us1
            │    └── VPC
            │         └── Subnets
            │              └── Security-Groups
            │                   └── EC2 instances
            │                        └── Docker containers
            │
            ├── APS-security (for audit trail and compliance aggregation)
            │  └── Guard Duty
            │  └── Security Hub
            │  └── Config
            │
            ...
```

Infrastructure-as-Code

APS AWS environments and infrastructure are managed as code. Provisioning is accomplished using a set of automation scripts and CloudFormation code. Each new environment is created as a sub-account connected to `APS-master`. The creation and provisioning of a new account follows the instructions documented in the Bootstrap a new AWS environment page of the development wiki.

17.2.10 Patch Management Procedures

Local Systems

APS uses automated tooling to ensure systems are up-to-date with the latest security patches.

- On local Linux and Windows systems, the unattended-upgrades tool is used to apply security patches in phases.
- High Risk security patches are automatically applied as they are released
- Monthly system patching for regular applications are applied as needed.
- Snapshotting of a system will take place before an update is applied.
- Once the update is deemed stable the snapshot will be removed.
- In case of failure of the update the snapshot will be rolled back.
- If the staging systems function properly after the two-week testing period, the security team will promote that snapshot into the mirror used by all production systems. These patches will be applied to all production systems during the next nightly patch run.
- The patching process may be expedited by the Security team
- On Windows systems, the baseline Group Policy setting configures Windows Update to implement the patching policy.

Cloud Resources

APS follows a “cattle-vs-pets” methodology to keep the resources in the cloud environments immutable and up-to-date with security patches.

- AWS Elastic Container Service (ECS) is used to dynamically manage container resources based on demand.
- Engineering team builds security-approved AMI from the latest AWS optimized Amazon Machine Image (AMI) to include required security agent.
- The security agents installed on the security-approved AMIs continuously scan for and report new vulnerabilities.
- The custom AMIs are automatically rebuilt from the latest AWS AMIs weekly to include the latest security patches.

User Endpoints

APS requires auto-update for security patches to be enabled for all user endpoints, including laptops and workstations.

- The auto-update configuration and update status on all end-user systems are inspected by Security through either manual periodic audits or automated compliance auditing agents installed on the endpoints.

17.2.11 Production Deploy / Code Promotion Processes

In order to promote changes into Production, a valid and approved Change Request (CR) is required. It can be created in the Change Management System/Portal which implements the APS Change Management workflow, using the Infrastructure (IN) Rally project to manage changes and approvals.

- At least two approvals are required for each IN ticket. By default, the approvers are
- Security Lead and
- Engineering Lead.
- Additional approver(s) may be added depending on the impacted component(s). For example,
- the IT Manager is added as an approver for IT/network changes; and
- the DevOps Lead is added as an approver for changes to `aws-APS-infra` account in AWS.
- Each IN ticket requires the following information at a minimum:
- Summary of the change
- Component(s) impacted
- Justification
- Rollback plan
- Additional details are required for a code deploy, including:
- Build job name
- Build ID and/or number
- Deploy action (e.g. plan, apply)
- Deploy branch (e.g. master)
- Target environment (e.g. `aws-APS-infra`, `aws-APS-prod-us`, `datacenter-hq`)
- Links to pull requests and/or Rally issues

17.2.12 Emergency Change

In the event of an emergency, the person or team on call is notified. This may include a combination or Development, IT, and Security.

If an emergency change must be made, such as patching of a zero-day security vulnerability or recovering from a system downtime, and that the standard change management process cannot be followed due to time constraint or personnel availability or other unforeseen issues, the change can be made by:

- **Notification:** The Engineering Lead, Security Lead, and/or IT Lead must be notified by email, Slack, or phone call prior to the change . Depending on the nature of the emergency, the leads may choose to inform members of the executive team.
- **Access and Execution:** Manually access of the production system or manual deploy of software, using one of the following access mechanisms as defined in Access Control policy and procedures:

a. Support/Troubleshooting access

b. Root account or root user access

c. Local system access (for on-premise environment)

- **Post-emergency Documentation:** An Infrastructure (IN) ticket should be created within 24 hours following the emergency change. The ticket should contains all details related to the change, including:
- Reason for emergency change
- Method of emergency access used
- Steps and details of the change that was made
- Sign-off/approvals must be obtained per the type of change as defined by the standard CM process
- **Prevention and Improvement:** The change must be fully reviewed by Security and Engineering together with the person/team responsible for the change. Any process improvement and/or preventative measures should be documented and an implementation plan should be developed.

18. Threat Detection and Prevention

`Last Reviewed: 2025-02-17:19:44:43-UTC`

In order to preserve the integrity of data that APS stores, processes, or transmits for Customers, APS implements strong intrusion detection tools and policies to proactively track and retroactively investigate unauthorized access. This include threat detection and prevention at both the network and host level, as well as threat intelligence monitoring.

18.1 Policy Statements

APS policy requires that:

(a) All critical systems, assets and environments must implement realtime threat detection or prevention.

18.2 Controls and Procedures

18.2.1 System Malware Protection

1. All end-user workstations and production systems must have antivirus running. The default anti-malware solution used is Jamf Protect. The anti-malware solution will include protection against malicious mobile code.
- Next generation endpoint protection agent may be used as an equivalent solution.
- linux hosts are installed with the AIDE intrusion detection system, per the Amazon Linux 2 CIS Benchmark section 1.3.1
- Hosts are scanned continuously for malicious binaries in critical system paths. Additionally, if supported, the agent is set to to scan system every 2 hours and at reboot to assure no malware is present.
- The malware signature database is kept up to date, changes are pushed continuously.
- Logs of virus scans and alerts are maintained according to the requirements outlined in System Auditing.
2. Detected malware is evaluated and removed following the established incident response process.
3. All systems are to only be used for APS business needs.

18.2.2 Firewall Protection

Firewall protection is implemented at the following layers

- **Network** - including Network ACL and Security Groups in AWS as well as on- premise firewalls between the office networks and the Internet.
- **Host** - local firewalls are enabled on the user endpoints as well as servers (compute and database instances in AWS are protected by security groups)
- **Application** - web application firewall (WAF) and content distribution are configured at the application layer to protect against common web application attacks such as cross site scripting, injection and denial-of-service attacks.

18.2.3 Network Intrusion Detection

Intrusion Detection for On-Premise Internal Networks

- APS leverages pfsense for network security of its on-premise environments.
- pfsense features stateful firewall inspection and intrusion detection/prevention (IDS/IPS) of applicable incoming and outgoing network traffic. Attacks and suspicious network activities are blocked automatically.
- APS IT manager is responsible for configuring the firewall and IDS/IPS rules and reviewing the configuration as least quarterly.

Intrusion Detection in AWS Cloud Environments

APS implemented a real-time threat detection solution by monitoring AWS Cloudtrail events and/or VPC flow logs.

- Cloudtrail events are monitored by **AWS GuardDuty**
- VPC flow logs are sent to and analyzed by **AWS GuardDuty**.

Additional monitoring is provided by our infrastructure service provider AWS.

18.2.4 Host Intrusion Detection

Host based intrusion detection is supported via one of the following:

- On Windows and macOS systems: **AWS Inspector** agents for malware detection and behavior-based endpoint threat detection.
- On Linux servers: **AWS Inspector** agents for activity monitoring, vulnerability scanning, and threat detection. This includes all virtual instances running in the cloud environment.

18.2.5 Web Application Protection

APS leverages AWS Services to protect web applications against common attacks such as SQL injection, cross-site scripting, and denial-of-service (DoS/DDoS) attacks. The services used include AWS Shield, WAF, Cloudfront, and/or API Gateway.

18.2.6 Centralized Security Information and Event Management

Security events and alerts are aggregated to and correlated by one or both of the following solutions:

- AWS SecurityHub
- Internally developed security automation tooling

18.2.7 Threat Intelligence Monitoring

RH-ISAC

APS is an active member of the Retail and Hospitality Information Sharing and Analysis Center (RH-ISAC).

APS Security team is subscribed to receive threat alerts from RH-ISAC.

Intelligence Feeds

Additional intelligence feeds are received automatically through some of the 3rd party security solutions that have been implemented on the networks and/or endpoints. The data gathered through these external intel feeds is automatically used by the security solutions to analyze events and generate alerts.

Regulatory Requirements Updates

The Security Officer actively monitors the regulatory compliance landscape for updates to regulations such as HIPAA, PCI and GDPR.

19. Vulnerability Management

`Last Reviewed: 2025-02-17:19:44:43-UTC`

19.1 Policy Statements

APS policy requires that:

(a) All product systems must be scanned for vulnerability on the defined, predetermined schedule and with each major change, as applicable.

(b) All vulnerability findings must be reported and tracked to resolution. Records of findings must be retained for a defined, predetermined timeframe.

19.2 Controls and Procedures

19.2.1 Vulnerability Scanning and Infrastructure Security Testing

The scanning and identification of system vulnerabilities is performed by

1. Automated security agent installed on all Linux servers.
- This includes physical and virtual servers hosted on premise as well as EC2 instances in AWS.
- The agent automatically reports to a centralized management server/dashboard with details of the server instance and any vulnerability finding.
- This assessment is performed on an ongoing basis.

1. Penetration testing is performed regularly as part of the APS vulnerability management policy.
- External penetration testing is performed at least annually by either a certified penetration tester on APS security team or an independent third party.

1. APS developed an internal vulnerability management tool/database used to track all system entities and associated vulnerabilities.
2. Findings from a vulnerability scan or penetration testing are analyzed by the security team, together with IT and Engineering as needed, and reported following the process as defined in the next section. A written report may be generated in addition to creating the findings in Rally.
3. All security testing reports and findings records are retained for 7 years.

19.2.2 Security Findings Reporting, Tracking and Remediation

We follow a simple vulnerability tracking process using Rally. The records of findings are retained for seven years.

Reporting a finding

- Upon identification of a vulnerability (including vulnerability in software, system, or process), a Rally Issue of (issueType = **Finding**) is created on the SECURITY Project.

- Populate the following custom fields as part of the Rally issue when applicable:

- **Source of Finding** (dropdown list)
- **In Production** (yes/no/na selection)
- **Application/Repo Name** (text/tag)
- **Version Number** (text/tag)

- The **Summary** of the Finding should be in this format: "{[sev]} {short description}" (e.g. "[High] Outdated package on ECS AMI image").
- The **Description** of the Finding should include further details, without any confidential information, and a link to the source.
- The **Priority** of the Finding should match its severity level.

Priority/Severity Ratings and Service Level Agreements

In an effort to quickly remediate security vulnerabilities the following timelines have been put in place to drive resolution.

Sev Rating	Priority Level	SLA	Definition	Examples
P0	Highest	3 days	Vulnerabilities that cause a privilege escalation on the platform from unprivileged to admin, allows remote code execution, financial theft, unauthorized access to/extraction of sensitive data, etc.	Vulnerabilities that result in Remote Code Execution such as Vertical Authentication bypass, SSRF, XXE, SQL Injection, User authentication bypass
P1	High	7 days	Vulnerabilities that affect the security of the platform including the processes it supports.	Lateral authentication bypass, Stored XSS, some CSRF depending on impact.
P2	Medium	30 days	Vulnerabilities that affect multiple users, and require little or no user interaction to trigger.	Reflective XSS, Direct object reference, URL Redirect, some CSRF depending on impact.
P3	Low	Best Effort	Issues that affect singular users and require interaction or significant prerequisites (MitM) to trigger.	Common flaws, Debug information, Mixed Content.

In the case a sev rating / priority level is updated after a vulnerability finding was originally created, the SLA is updated as follow:

- **severity upgrade:** reset SLA from time of escalation
- **severity downgrade:** SLA time remains the same from time of creation/identification of finding

Resolving a finding

- The Finding should be assigned to the owner responsible for the system or software package.
- All findings should be addressed according to the established SLA.
- No software should be deployed to production with unresolved HIGH or MEDIUM findings, unless an Exception is in place (see below).

- A finding may be resolved by

a. providing a valid fix/mitigation

b. determining as a false positive

c. documenting an approved exception

Closing a finding

- The assignee should provide a valid resolution (see above) and add a comment to the finding.
- The finding should be re-assigned to the Reporter or a member of the security team for validation.
- Upon validation, the finding can be marked as Done (closed) by the Reporter.
- **Before the finding can be marked as closed by the reporter, the fix must be deployed to dev and have a targeted release date for deploying to production noted on the ticket.**

Exceptions

- An Exception may be requested when a viable or direct fix to a vulnerability is not available. For example, a version of the package that contains the fix is not supported on the particular operating system in use.
- An alternative solution (a.k.a. compensating control) must be in place to address the original vulnerability such that the risk is mitigated. The compensating control may be technical or a process or a combination of both.
- An Exception must be opened in the form of a Rally issue (issueType = **Exception**) on the SECURITY project.
- The Exception Rally issue must reference the original Finding by adding an Issue Link to the Finding Rally issue.
- Each Exception must be reviewed and approved by the Security team and the impacted asset owner.
- All Exceptions are reviewed every six months to re-assess its validity.

20. Mobile Device Security and Storage Media Management

`Last Reviewed: 2025-02-17:19:44:43-UTC`

APS recognizes that media containing sensitive data may be reused when appropriate steps are taken to ensure that all stored sensitive data has been effectively rendered inaccessible. Destruction/disposal of sensitive data shall be carried out in accordance with federal and state law. The schedule for destruction/disposal shall be suspended for sensitive data involved in any open investigation, audit, or litigation.

APS utilizes virtual storage repositories to store production data. Volumes and repositories utilized by APS and APS Customers are encrypted. APS does not use, own, or manage any mobile devices, removable storage media, or backup tapes that have access to sensitive data.

20.1 Policy Statements

APS policy requires that:

(a) All media, including mobile and removable media, storing APS company data must be encrypted.

(b) Critical data as defined in APS data classification model §data-management may not be stored on mobile devices or removable media such as USB flash drives.

(c) All destruction/disposal of sensitive data storage media will be done in accordance with federal and state laws and regulations and pursuant to the APS's written retention policy/schedule.

- Records that have satisfied the period of retention will be destroyed/disposed of in an appropriate manner.
- Records involved in any open investigation, audit or litigation should not be destroyed/disposed of.

(d) All sensitive data must rendered inaccessible in a forensically sound manner prior to media reuse or disposal.

(e) Mobile devices, including laptops, smart phones and tables, used in support of critical business operations shall be fully managed and/or audited by APS IT and Security.

20.2 Controls and Procedures

20.2.1 Media Disposal Process

IT and Security is responsible to ensure media containing critical / sensitive data is disposed securely in the following manner:

- The methods of destruction, disposal, and reuse are reassessed periodically, based on current technology, accepted practices, and availability of timely and cost-effective destruction, disposal, and reuse technologies and services. This may include
- Secure wipe;
- Physical destruction;
- Destruction of encryption keys (if the data on the media is encrypted using a strong algorithm such as AES-256).
- If the records have been requested in the course of a judicial or administrative hearing, a qualified protective order will be obtained to ensure that the records are returned to the organization or properly destroyed/disposed of by the requesting party.
- All APS Subcontractors provide that, upon termination of the contract, they will return or destroy/dispose of all company information. In cases where the return or destruction/disposal is not feasible, the contract limits the use and disclosure of the information to the purposes that prevent its return or destruction/disposal.
- In the cases of a APS Customer terminating a contract with APS and no longer utilize APS Services, data will be returned or disposed per contract agreement or APS Platform use terms and conditions. In all cases it is solely the responsibility of the APS Customer to maintain the safeguards required of laws and regulations once the data is transmitted out of APS environments.

20.2.2 Use of USB Flash Drive and External Storage Device

Per APS corporate policy, confidential and critical data may not be stored on external devices such as USB flash drives. For definition of confidential and critical data, see APS Data Classification and Handling Policy.

Usage of USB flash drives for temporary transfer of confidential and critical data may be allowed on a case by case basis, when the following process is followed:

- Data is only allowed on encrypted flash devices approved by APS Security and the IT Manager (currently **manual process**).
- The process starts with the submission of a ticket in Rally. The ticket must be approved by IT and Security.
- Upon completion of data transfer all sensitive data on the device must be completely removed.
- The device is to be returned to the IT Manager to double check that the data has been removed.
- The IT Manager will check the drive back in.

20.2.3 Support and Management of BYOD Devices

APS provides company-issued laptops and workstations to all employees.

Mobile devices (including personal smart devices) may be used for business purpose under the following conditions and management:

- All employee mobile devices accessing or containing company data are inventoried and managed by IT using **Jamf**. The inventory will maintain current information on the owner of the device, its approved usages, installed applications, system status (operating system version and patches), and its state (e.g. in-use, lost, decommissioned).
- Mobile device management software is deployed to ensure the proper protection and configuration of mobile devices, including:
- Encryption must be enabled for device storage
- Device password must be enabled and meet security policy requirements
- Device must be locked after 10 minutes of inactivity
- Operating systems and patches are up to date
- All applications downloaded on employee mobile devices used for business purposes must be installed through a pre-approved app store or application list.
- Circumvention of built-in device security controls such as jailbreaking is strictly prohibited and enforced by detective or preventative software.
- Anti-malware software is installed and active on mobile devices. Alternatively, a sandbox environment is created on BYOD devices using the **Jamf** MDM solution to allow only white-listed application and data in a contained workspace.
- Any confidential or sensitive data is only allowed to be accessed via and stored inside the sandbox environment on mobile devices.
- Employees acknowledge that their mobile devices may be remotely controlled, locked or erased via the MDM software.
- Eligibility and usage of BYOD devices is subject to manager and/or IT/Security approval.

21. Business Continuity and Disaster Recovery

`Last Reviewed: 2025-02-17:19:44:43-UTC`

The APS Contingency Plan establishes procedures to recover APS following a disruption resulting from a disaster. This Disaster Recovery Policy is maintained by the APS Security Officer and Cloud Engineer.

NIST: This APS Contingency Plan is created under the legislative requirements set forth in the Federal Information Security Management Act (FISMA) of 2002 and the guidelines established by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, titled “Contingency Planning Guide for Information Technology Systems” dated June 2002.

21.1 Policy Statements

APS policy requires that:

(a) A plan and process for business continuity and disaster recovery (BCDR), including the backup and recovery of systems and data, must be defined and documented.

(b) BCDR shall be simulated and tested at least once a year. Metrics shall be measured and identified recovery enhancements shall be filed to improve the BCDR process.

(c) Security controls and requirements must be maintained during all BCDR activities.

21.2 Controls and Procedures

21.2.1 BCDR Objectives and Roles

Objectives

The following objectives have been established for this plan:

1. Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
   - *Notification/Activation phase* to detect and assess damage and to activate the plan;
   - *Recovery phase* to restore temporary IT operations and recover damage done to the original system;
   - *Reconstitution phase* to restore IT system processing capabilities to normal operations.
2. Identify the activities, resources, and procedures needed to carry out APS processing requirements during prolonged interruptions to normal operations.
3. Identify and define the impact of interruptions to APS systems.
4. Assign responsibilities to designated personnel and provide guidance for recovering APS during prolonged periods of interruption to normal operations.
5. Ensure coordination with other APS staff who will participate in the contingency planning strategies.
6. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

Example of the types of disasters that would initiate this plan are natural disaster, political disturbances, man made disaster, external human threats, and internal malicious activities.

APS defined two categories of systems from a disaster recovery perspective.

1. *Critical Systems*. These systems host production application servers/services and database servers/services or are required for functioning of systems that host production applications and data. These systems, if unavailable, affect the integrity of data and must be restored, or have a process begun to restore them, immediately upon becoming unavailable.
2. *Non-critical Systems*. These are all systems not considered critical by definition above. These systems, while they may affect the performance and overall security of critical systems, do not prevent Critical systems from functioning and being accessed appropriately. These systems are restored at a lower priority than critical systems.

Line of Succession

The following order of succession to ensure that decision-making authority for the APS Contingency Plan is uninterrupted.

The Chief Executive Officer (CEO) is responsible for ensuring the safety of personnel and the execution of procedures documented within this APS Contingency Plan. The Head of Engineering is responsible for the recovery of APS technical environments. If the Head of Engineering is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the CEO shall function as that authority or choose an alternative delegate. To provide contact initiation should the contingency plan need to be initiated, please use the contact list below.

- Tim Kieschnick, Head of Engineering: tim.kieschnick@aboveproperty.com
- Aaron Shepherd, CEO: aaron.shepherd@aboveproperty.com

Response Teams and Responsibilities

The following teams have been developed and trained to respond to a contingency event affecting APS infrastructure and systems.

1. **IT** is responsible for recovery of the APS hosted environment, network devices, and all servers. The team includes personnel responsible for the daily IT operations and maintenance. The team leader is the IT Manager who reports to the CEO.
2. **HR & Facilities** is responsible for ensuring the physical safety of all APS personnel and environmental safety at each APS physical location. The team members also include site leads at each APS work site. The team leader is the Facilities Manager who reports to the CEO.
3. **DevOps** is responsible for assuring all applications, web services, platform and their supporting infrastructure in the Cloud. The team is also responsible for testing re-deployments and assessing damage to the environment. The team leader is the Head of Engineering.
4. **Security** is responsible for assessing and responding to all cybersecurity related incidents according to APS Incident Response policy and procedures. The security team shall assist the above teams in recovery as needed in non-cybersecurity events. The team leader is the Security Officer.

Members of above teams must maintain local copies of the contact information of the BCDR succession team. Additionally, the team leads must maintain a local copy of this policy in the event Internet access is not available during a disaster scenario.

All executive leadership shall be informed of any and all contingency events. Current members of APS leadership team include the Security Officer, CTO, CIO, COO, CEO.

21.2.2 General Disaster Recovery Procedures

Notification and Activation Phase

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to APS. Based on the assessment of the Event, sometimes according to the APS Incident Response Policy, the Contingency Plan may be activated by either the CEO or Head of Engineering. The Contingency Plan may also be activated by the Security Officer in the event of a cyber disaster.

The notification sequence is listed below:

- The first responder is to notify the CEO. All known information must be relayed to the CEO.
- The CEO is to contact the Response Teams and inform them of the event. The CEO or delegate is responsible to begin assessment procedures.
- The CEO is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the CEO is to following the steps below.
- Damage Assessment Procedures:
- The CEO is to logically assess damage, gain insight into whether the infrastructure is salvageable, and begin to formulate a plan for recovery.
- Alternate Assessment Procedures:
- Upon notification, the CEO is to follow the procedures for damage assessment with the Response Teams.
- The APS Contingency Plan is to be activated if one or more of the following criteria are met:
- APS will be unavailable for more than 48 hours.
- On-premise hosting facility or cloud infrastructure service is damaged and will be unavailable for more than 24 hours.
- Other criteria, as appropriate and as defined by APS.
- If the plan is to be activated, the CEO is to notify and inform team members of the details of the event and if relocation is required.
- Upon notification from the CEO, group leaders and managers are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.
- The Head of Engineering is to notify the hosting facility partners that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site.
- The Head of Engineering is to notify remaining personnel and executive leadership on the general status of the incident.
- Notification can be message, email, or phone.

Recovery Phase

This section provides procedures for recovering APS infrastructure and operations at an alternate site, whereas other efforts are directed to repair damage to the original system and capabilities.

Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

Recovery Goal: The goal is to rebuild APS infrastructure to a production state.

The tasks outlines below are not sequential and some can be run in parallel.

1. Contact Partners and Customers affected to begin initial communication - DevOps
2. Assess damage to the environment - DevOps
3. Create a new production environment using new environment bootstrap automation - DevOps
4. Ensure secure access to the new environment - Security
5. Begin code deployment and data replication using pre-established automation - DevOps
6. Test new environment and applications using pre-written tests - DevOps
7. Test logging, security, and alerting functionality - DevOps and Security
8. Assure systems and applications are appropriately patched and up to date - DevOps
9. Update DNS and other necessary records to point to new environment - DevOps
10. Update Partners and Customers affected through established channels - DevOps

Reconstitution Phase

This section discusses activities necessary for restoring full APS operations at the original or new site. The goal is to restore full operations within 24 hours of a disaster or outage. If necessary, when the hosted data center at the original or new site has been restored, APS operations at the alternate site may be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the computer center.

1. Original or New Site Restoration

- Repeat steps 5-9 in the Recovery Phase at the original or new site / environment.
- Restoration of Original site is unnecessary for cloud environments, except when required for forensic purpose.

2. Plan Deactivation

- If the APS environment is moved back to the original site from the alternative site, all hardware used at the alternate site should be handled and disposed of according to the APS Media Disposal Policy.

21.2.3 Testing and Maintenance

The CEO and/or Head of Engineering shall establish criteria for validation/testing of a Contingency Plan, an annual test schedule, and ensure implementation of the test. This process will also serve as training for personnel involved in the plan's execution. At a minimum the Contingency Plan shall be tested annually (within 365 days). The types of validation/testing exercises include tabletop and technical testing. Contingency Plans for all application systems must be tested at a minimum using the tabletop testing process. However, if the application system Contingency Plan is included in the technical testing of their respective support systems that technical test will satisfy the annual requirement.

Tabletop Testing

Tabletop Testing is conducted in accordance with the CMS Risk Management Handbook, Volume 2. The primary objective of the tabletop test is to ensure designated personnel are knowledgeable and capable of performing the notification/activation requirements and procedures as outlined in the CP, in a timely manner. The exercises include, but are not limited to:

- Testing to validate the ability to respond to a crisis in a Coordinated, timely, and effective manner, by simulating the occurrence of a specific crisis.

Simulation and/or Technical Testing

The primary objective of the technical test is to ensure the communication processes and data storage and recovery processes can function at an alternate site to perform the functions and capabilities of the system within the designated requirements. Technical testing shall include, but is not limited to:

- Process from backup system at the alternate site;
- Restore system using backups; and
- Switch compute and storage resources to alternate processing site.

21.2.4 Work Site Recovery

In the event a APS facility is not functioning due to a disaster, employees will work from home or locate to a secondary site with Internet access, until the physical recovery of the facility impacted is complete. The recovery shall be performed by the facility management firm under contract with APS, and coordinated by the Facility Manager and/or the Site Lead.

APS's software development organization has the ability to work from any location with Internet access and does not require an office provided Internet connection.

21.2.5 Production Environments and Data Recovery

Production data is to be synchronized across multiple S3 buckets in AWS.

APS assumes that in the worst-case scenario, that one of the production environments suffers a complete data loss, the account will be reconstructed from code

Recovery of production Environments and data should follow the procedures listed above and in Data Management - Backup and Recovery

22. Incident Response

`Last Reviewed: 2025-02-17:19:44:43-UTC`

APS implements an information security incident response process to consistently detect, respond, and report incidents, minimize loss and destruction, mitigate the weaknesses that were exploited, and restore information system functionality and business continuity as soon as possible.

The incident response process addresses:

- Continuous monitoring of threats through intrusion detection systems (IDS) and other monitoring applications;
- Establishment of an information security incident response team;
- Establishment of procedures to respond to media inquiries;
- Establishment of clear procedures for identifying, responding, assessing, analyzing, and follow-up of information security incidents;
- Workforce training, education, and awareness on information security incidents and required responses; and
- Facilitation of clear communication of information security incidents with internal, as well as external, stakeholders

22.1 Policy Statements

APS policy requires that:

(a) All computing environments and systems must be monitored in accordance to the policies and procedures specified in the following APS policies and procedures:

- Auditing
- System Access
- End-user Computing and Acceptable Use

(b) All alerts must be reviewed to identify security incidents.

(c) Incident response procedures are invoked upon discovery of a valid security incident.

(d) Incident response team and management must comply with any additional requests by law enforcement in the event of criminal investigation or national security, including but not limited to warranted data requests, subpoenas, and breach notifications.

22.2 Controls and Procedures

22.2.1 Security Incident Response Team (SIRT)

The Security Incident Response Team (SIRT) is responsible for:

- Review, analyze and log of all received reports and track their statuses.
- Performing investigations, creating and executing action plans, post-incident activities.
- Collaboration with law enforcement agencies.

Current members of the APS SIRT:

- Security Officer
- Security Engineers
- Head of Engineering
- DevOps and Production Support Team

22.2.2 Incident Response Plan

The APS incident response plan follows the process recommended by SANS, an industry leader in security. Process flows are a direct representation of the SANS process.

APS's incident response classifies security-related events into the following categories:

- **Events** - Any observable computer security-related occurrence in a system or network with a negative consequence. Examples:
- Hardware component failing causing service outages.
- Software error causing service outages.
- General network or system instability.
- **Precursors** - A sign that an incident may occur in the future. Examples:
- Monitoring system showing unusual behavior.
- Audit log alerts indicated several failed login attempts.
- Suspicious emails targeting specific APS staff members with administrative access to production systems.
- Alerts raised from a security control source based on its monitoring policy, such as
- Microsoft 365 (user authentication activities)
- Threat Stack (AWS Cloudtrail events or system agent activities)
- AWS Config & Monitoring (cloud services configuration or access alerts)
- AWS CloudWatch alerts
- **Indications** - A sign that an incident may have occurred or may be occurring at the present time. Examples:
- Alerts for modified system files or unusual system accesses.
- Antivirus alerts for infected files or devices.
- Excessive network traffic directed at unexpected geographic locations.
- **Incidents** - A confirmed attack / indicator of compromise or a validated violation of computer security policies or acceptable use policies, often resulting in data breaches. Examples:
- Unauthorized disclosure of sensitive data.
- Unauthorized change or destruction of sensitive data.
- A data breach accomplished by an internal or external entity.
- A Denial-of-Service (DoS) attack causing a critical service to become unreachable.

APS employees must report any unauthorized or suspicious activity seen on production systems or associated with related communication systems (such as email or Slack). In practice this means keeping an eye out for security events, and letting the Security team know about any observed precursors or indications as soon as they are discovered.

> **Attention**
>
> Incidents of a severity/impact rating higher than **MINOR** shall trigger the following response process, or as defined more specifically in the **Incident Categories and Playbooks** section.

I - Identification and Triage

1. Immediately upon observation APS members report suspected and known Events, Precursors, Indications, and Incidents in one of the following ways:

a. Direct report to management, the Security Officer, or other;

b. Email;

c. Phone call;

d. Submit an incident report online via APS Internal ServiceDesk;

e. Secure chat; or

f. Anonymously through workforce members desired channels.

2. The individual receiving the report facilitates the collection of additional information about the incident, as needed, and notifies the Security Officer (if not already done).

3. The Security Officer determines if the issue is an Event, Precursor, Indication, or Incident.

4. If the issue is an event, indication, or precursor the Security Officer forwards it to the appropriate resource for resolution.

a. Non-Technical Event (minor infringement): the Security Officer of designee creates an appropriate issue in Rally and further investigates the incident as needed.

b. Technical Event: Assign the issue to an technical resource for resolution. This resource may also be a contractor or outsourced technical resource, in the event of a lack of resource or expertise in the area.

5. If the issue is a security incident the Security Officer activates the Security Incident Response Team (SIRT) and notifies senior leadership by email.

a. If a non-technical security incident is discovered the SIRT completes the investigation, implements preventative measures, and resolves the security incident.

b. Once the investigation is completed, progress to Phase V, Follow-up.

c. If the issue is a technical security incident, commence to Phase II: Containment.

d. The Containment, Eradication, and Recovery Phases are highly technical. It is important to have them completed by a highly qualified technical security resource with oversight by the SIRT team.

e. Each individual on the SIRT and the technical security resource document all measures taken during each phase, including the start and end times of all efforts.

f. The lead member of the SIRT team facilitates initiation of an Incident ticket in Rally Security Project and documents all findings and details in the ticket.

- The intent of the Incident ticket is to provide a summary of all events, efforts, and conclusions of each Phase of this policy and procedures.
- Each Incident ticket should contain sufficient details following the SANS Security Incident Forms templates, as appropriate.

6. The Security Officer, or APS representative appointed notifies any affected Customers and Partners. If no Customers and Partners are affected, notification is at the discretion of the Security and Privacy Officer.

7. In the case of a threat identified, the Security Officer is to form a team to investigate and involve necessary resources, both internal to APS and potentially external.

II - Containment (Technical)

In this Phase, APS's engineers and security team attempts to contain the security incident. It is extremely important to take detailed notes during the security incident response process. This provides that the evidence gathered during the security incident can be used successfully during prosecution, if appropriate.

1. Review any information that has been collected by the Security team or any other individual investigating the security incident.
2. Secure the blast radius (i.e. a physical or logical network perimeter or access zone).
3. Perform the following forensic analysis preparation, as needed:

a. Securely connect to the affected system over a trusted connection.

b. Retrieve any volatile data from the affected system.

c. Determine the relative integrity and the appropriateness of backing the system up.

d. As necessary, take a snapshot of the disk image for further forensic; and if appropriate, back up the system.

e. Change the password(s) to the affected system(s).

f. Determine whether it is safe to continue operations with the affect system(s).

g. If it is safe, allow the system to continue to function; and move to Phase V, Post Incident Analysis and Follow-up.

h. If it is NOT safe to allow the system to continue operations, discontinue the system(s) operation and move to Phase III, Eradication.

i. The individual completing this phase provides written communication to the SIRT.

4. Complete any documentation relative to the security incident containment on the Incident ticket, using SANS IH Containment Form as a template.
5. Continuously apprise Senior Management of progress.
6. Continue to notify affected Customers and Partners with relevant updates as needed.

III - Eradication (Technical)

The Eradication Phase represents the SIRT's effort to remove the cause, and the resulting security exposures, that are now on the affected system(s).

1. Determine symptoms and cause related to the affected system(s).
2. Strengthen the defenses surrounding the affected system(s), where possible (a risk assessment may be needed and can be determined by the Security Officer). This may include the following:

a. An increase in network perimeter defenses.

b. An increase in system monitoring defenses.

c. Remediation ("fixing") any security issues within the affected system, such as removing unused services/general host hardening techniques.

3. Conduct a detailed vulnerability assessment to verify all the holes/gaps that can be exploited have been addressed.

a. If additional issues or symptoms are identified, take appropriate preventative measures to eliminate or minimize potential future compromises.

4. Update the Incident ticket with Eradication details, using SANS IH Eradication Form as a template.
5. Update the documentation with the information learned from the vulnerability assessment, including the cause, symptoms, and the method used to fix the problem with the affected system(s).
6. Apprise Senior Management of the progress.
7. Continue to notify affected Customers and Partners with relevant updates as needed.
8. Move to Phase IV, Recovery.

IV - Recovery (Technical)

The Recovery Phase represents the SIRT's effort to restore the affected system(s) back to operation after the resulting security exposures, if any, have been corrected.

1. The technical team determines if the affected system(s) have been changed in any way.

a. If they have, the technical team restores the system to its proper, intended functioning ("last known good").

b. Once restored, the team validates that the system functions the way it was intended/had functioned in the past. This may require the involvement of the business unit that owns the affected system(s).

c. If operation of the system(s) had been interrupted (i.e., the system(s) had been taken offline or dropped from the network while triaged), restart the restored and validated system(s) and monitor for behavior.

d. If the system had not been changed in any way, but was taken offline (i.e., operations had been interrupted), restart the system and monitor for proper behavior.

e. Update the documentation with the detail that was determined during this phase.

f. Apprise Senior Management of progress.

g. Continue to notify affected Customers and Partners with relevant updates as needed.

h. Move to Phase V, Follow-up.

V - Post-Incident Analysis (Technical and Non-Technical)

The Follow-up phase represents the review of the security incident to look for "lessons learned" and to determine whether the process that was taken could have been improved in any way. It is recommended all security incidents be reviewed shortly after resolution to determine where response could be improved. Timeframes may extend to one to two weeks post-incident.

1. Responders to the security incident (SIRT Team and technical security resource) meet to review the documentation collected during the security incident.

2. A "lessons learned" section is written and attached to Incident ticket.

a. Evaluate the cost and impact of the security incident to APS using the documents provided by the SIRT and the technical security resource.

b. Determine what could be improved. This may include:

- Systems and processes adjustments
- Awareness training and documentation
- Implementation of additional controls

c. Communicate these findings to Senior Management for approval and for implementation of any recommendations made post-review of the security incident.

d. Carry out recommendations approved by Senior Management; sufficient budget, time and resources should be committed to this activity.

3. Ensure all incident related information is recorded and retained as described in APS Auditing requirements and Data Retention standards.

4. Close the security incident.

Periodic Evaluation

It is important to note that the processes surrounding security incident response should be periodically reviewed and evaluated for effectiveness. This also involves appropriate training of resources expected to respond to security incidents, as well as the training of the general population regarding the APS's expectation for them, relative to security responsibilities. The incident response plan is tested annually.

22.2.3 Incident Categories and Playbooks

- The IRT reviews and analyzes on the security events on as part of its daily operations.

- Based on the initial analysis, an event may be dismissed due to false positives, normal business operations, exceptions that are already in place, permitted per policy, or duplicates. An audit trail will be kept for event dismissal.
- A valid security event may be upgrade to a security incident. Upon which, an incident classification and severity is assigned as specified below.
- Record of the decision must be stored with details on date(s), name(s) of the person(s) conducted assessment.
- A containment, eradication and recovery procedure is triggered based on the Category classification of the incident.
- In addition to the general incident management procedures previously described, one or more of the following playbooks are consulted based on the classification of a particular incident.

Classification

- **Category 1** – General Incidents, including physical security incidents
- **Category 2** – Attacks on internal corporate infrastructure, including network, hardware, software
- **Category 3** – Malware
- **Category 4** – Attacks on external facing assets, such as website, web applications, web services. Including denial of service attacks.
- **Category 5** – Human targets, social engineering, phishing, etc.
- **Category 6** – Breach/leakage of critical or confidential data

Severity Levels:

- **Critical** – incident that involves immediate and significant interruption to business operations and/or breach of critical or confidential data
- **Major** – incident that involves immediate interruption to business operations but will not likely result in immediate data breach
- **Minor** – all other confirmed incidents

Response Procedures: Cat 1 – General Incident

- Prioritize handling the incident based on functional impact, informational effort, recoverability efforts and other relevant factors
- Report the incident to the appropriate internal personnel and external organizations
- Acquire, preserve, secure, and document evidence
- Contain the incident
- Eradicate the incident
- Identify and mitigate all factors that enabled the incident to occur
- Remove any results of malicious activity
- Recover from the incident
- Restore affected systems and business functions
- Implement additional preventive measures

Response Procedures: Cat 2 – Internal Infrastructure Incident Response

Depending on the type of event, use the following incident response playbooks:

- Unauthorized Access
- Root Access
- Elevation of Privilege

Response Procedures: Cat 3 – Malware outbreak

Follow this incident response playbook:

- Malware

Response Procedures: Cat 4 – External web attacks and DoS/DDoS attacks

- Mobilize the Engineering team to secure systems and ensure Business Continuity
- Conduct a thorough investigation of the incident
- Manage public relationships
- Address legal and regulatory requirements
- Trigger BCDR if necessary

Response Procedures: Cat 5 – Social Engineering

Follow the Phishing incident response playbook

Response Procedures: Cat 6 – Data Leakage

Data Theft incident response playbook outlines the response instructions

Response Procedures: Special Cases

At least the following two special cases are considered when responding to an incident:

Criminal Activities:

In the event of an attack that involves suspected criminal activities, the IRT and management team will inform law enforcement.

Insider Threat:

Members of the cross-discipline insider threat incident handling team include:

- Security,
- CEO, and
- Head of Engineering as appropriate.

22.2.4 Emergency Operations Mode

If an incident constitutes an emergency – for example, a detected cyberattack that impacts production systems – APS plans to operate in a “read-only” mode, to continue to provide customers access to their data. All write access is temporarily blocked and data upload is paused until the emergency is resolved. This is accomplished by updating the access policy in production AWS environments.

In emergency operations mode, temporary access may be granted to security and/or engineering team to access the production environments to perform forensics, root cause analysis, eradication/remediation, or other necessary activities for incident recovery.

22.2.5 Tabletop Exercise

At least once per year, APS security and engineering teams jointly performs a Red Team exercise and/or a simulated “drill” of an emergency cyberattack that results in one or more **CRITICAL** incidents. Depending on the type of exercise, the duration may range from 2-4 hours (simulated “drill”) to a couple of weeks (full Red Teaming exercise).

The exercise will follow a cyberattack playbook. It may be conducted with all internal resources or with the help of an external security consulting firm. The goal of the exercise is to ensure all parties involved receive proper training to handle an actual

incident and to test out the documented procedures in order to identify gaps ahead of a real event. Senior leadership team may be invited to participate in the “drill” depending on the nature of the exercise or receive a readout of the outcome.

22.2.6 Incident Tracking and Records

A record is created for each reported incident in Jira. Each incident record contains details about the incident capturing the incident attributes and progression, including the following as applicable:

- Summary
- Description
- Impact
- Priority / Urgency
- Categorization
- Analysis Notes and Comments
- Cause / Determination
- Outcome / Resolution
- Lessons Learned

If a more detailed post-mortem is applicable, the Security and/or DevOps team will create the write-up and link it in the incident record.

23. Breach Investigation and Notification

`Last Reviewed: 2025-02-17:19:44:43-UTC`

In the case of a breach, APS shall notify all affected Customers. It is the responsibility of the Customers to notify affected individuals.

23.1 Policy Statements

APS policy requires that:

(a) Breach notification procedures are invoked upon confirmation of security breach that results in unauthorized disclosure of unprotected/unencrypted sensitive data.

(b) Individuals impacted by a confirmed data breach must be notified within a predefined, required timeframe of discovery of such breach.

23.2 Controls and Procedures

23.2.1 Breach Investigation Process

1. Discovery of Breach: A data breach shall be treated as “discovered” as of the first day on which such breach is known to the organization, or, by exercising reasonable diligence would have been known to APS (includes breaches by the organization’s Customers, Partners, or subcontractors). APS shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or Partner of the organization. Following the discovery of a potential breach, the organization shall begin an investigation (see organizational policies for security incident response and/or risk management incident response) immediately, conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each Customer affected by the breach. APS shall also begin the process of determining what external notifications are required or should be made (e.g., law enforcement officials)
2. Breach Investigation: The APS Security Officer shall name an individual to act as the investigator of the breach (e.g., security officer, risk manager, etc.). The investigator shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in the organization as appropriate (e.g., administration, security incident response team, human resources, risk management, public relations, legal counsel, etc.) The investigator shall be the key facilitator for all breach notification processes to the appropriate entities (e.g., law enforcement officials). All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of seven years. A breach log is kept and maintained by the Security Officer.
3. Risk Assessment: A risk assessment is performed in accordance to applicable laws and regulations.
4. Timeliness of Notification: Upon discovery of a breach, notice shall be made to the affected APS Customers, usually within 24-48 hours but no later than 10 calendar days after the discovery of the breach. It is the responsibility of the organization to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.
5. Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states to the organization that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the organization shall:

- If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the timer period specified by the official; or
- If the statement is made orally, document the statement, including the identify of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

6. Content of the Notice: The notice shall be written in plain language and must contain the following information:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved), if known;
- Any steps the Customer should take to protect Customer data from potential harm resulting from the breach.
- A brief description of what APS is doing to investigate the breach, to mitigate harm to individuals and Customers, and to protect against further breaches.
- Contact procedures for individuals to ask questions or learn additional information, which may include a toll-free telephone number, an e-mail address, a web site, or postal address.

7. Methods of Notification: APS Customers will be notified via email and phone within the timeframe for reporting breaches, as outlined above.
8. Maintenance of Breach Information/Log: As described above and in addition to the reports created for each incident, APS shall maintain a process to record or log all breaches of unsecured sensitive data regardless of the number of records and Customers affected. The following information should be collected/logged for each breach (see sample Breach Notification Log):

- A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of records and Customers affected, if known.
- A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.), if known.
- A description of the action taken with regard to notification of patients regarding the breach.
- Resolution steps taken to mitigate the breach and prevent future occurrences.

9. Workforce Training: APS shall train all members of its workforce on the policies and procedures with respect to sensitive data as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within the organization.
10. Complaints: APS must provide a process for individuals to make complaints concerning the organization’s patient privacy policies and procedures or its compliance with such policies and procedures.
11. Sanctions: The organization shall have in place and apply appropriate sanctions against members of its workforce, Customers, and Partners who fail to comply with privacy policies and procedures.
12. Retaliation/Waiver: APS may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. The organization may not require individuals to waive their privacy rights under as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

23.2.2 APS Platform Customer Responsibilities

The following requirements and guidelines shall be provided to and agreed upon by a client organization using APS platform to host sensitive data.

The agreement may be in the form of a contract or acceptance of terms and conditions.

1. The APS Customer that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured sensitive data shall, without unreasonable delay and in no case later than 72 hours after discovery of a breach, notify APS of such breach. The Customer shall provide APS with the following information:

- A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of records and Customers affected, if known.
- Resolution steps taken to mitigate the breach and prevent future occurrences.

2. Depending on the nature of the breach, an investigation may be conducted by APS or the Customer or jointly to determine the cause of breach.
3. Notice to Media: Unless APS is directly at fault for the cause of breach, APS Customers are responsible for providing notice to prominent media outlets at the Customer's discretion.
4. Notice to Authorities: Unless APS is directly at fault for the cause of breach, APS Customers are responsible for providing notice to the appropriate authorities at the Customer's discretion.

23.2.3 Sample Letter to Customers in Case of Breach

[Date]

[Name] [Name of Customer] [Address 1] [Address 2] [City, State Zip Code]

Dear [Name of Customer]:

I am writing to you from Above Property LLC., with important information about a recent breach that affects your account with us. We became aware of this breach on [Insert Date] which occurred on or about [Insert Date]. The breach occurred as follows:

Describe event and include the following information:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
- A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved), if known.
- Any steps the Customer should take to protect themselves from potential harm resulting from the breach.
- A brief description of what APS is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
- Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, web site, or postal address.

Other Optional Considerations:

- Recommendations to assist customer in remedying the breach.

We will assist you in remedying the situation.

Sincerely,

Pete Ehlke
Security Officer
Above Property LLC.
pete.ehlke@aboveproperty.com

23.2.4 List of Contacts for Authorities

Federal Trade Commission

- Phone: 1-877-382-4357
- Website: https://ftccomplaintassistant.gov

Privacy Shield

- Website: https://www.privacyshield.gov/assistance

GDPR Lead Supervisory Authority (UK) - ICO

- Website:
- https://ico.org.uk/make-a-complaint/
- https://ico.org.uk/global/contact-us/

GDPR Lead Supervisory Authority (Ireland) - DPC

- Website: https://www.dataprotection.ie/en/contact/how-contact-us

Naples Police Department

- Phone: 239-213-4844
- Address: 355 Riverside Circle Naples, FL 34102

Federal Bureau of Investigation Naples Office

- Phone: (239) 262-7941
- Address: 3001 Tamiami Trail N Naples, FL 34103

24. Third Party Security, Vendor Risk Management and Systems/Services Acquisition

`Last Reviewed: 2025-02-17:19:44:43-UTC`

APS makes every effort to assure all third party organizations are compliant and do not compromise the integrity, security, and privacy of APS or APS Customer data. Third Parties include Vendors, Customers, Partners, Subcontractors, and Contracted Developers.

24.1 Policy Statements

APS policy requires that:

(a) A list of approved vendors/partners must be maintained and reviewed annually.

(b) Approval from management, procurement and security must be in place prior to onboarding any new vendor or contractor. Additionally, all changes to existing contract agreements must be reviewed and approved prior to implementation.

(c) For any technology solution that needs to be integrated with APS production environment or operations, a Vendor Technology Review must be performed by the security team to understand and approve the risk. Periodic compliance assessment and SLA review may be required.

(d) APS Customers or Partners should not be allowed access outside of their own environment, meaning they cannot access, modify, or delete any data belonging to other 3rd parties.

(e) Additional vendor agreements are obtained as required by applicable regulatory compliance requirements.

- A GDPR Data Processing Agreement/Addendum (DPA) is defined and executed for each APS vendor/contractor that processes personal data of EU users.

24.2 Controls and Procedures

24.2.1 Vendor Technology Risk Review

APS security policy requires a risk review of vendor technology, prior to any technology being integrated to APS operations and/or infrastructure. Employees are required to engage security team to conduct such review. The request may be submitted by email directly to the security team, or by opening a Rally ticket through the APS internal service desk.

Security team is responsible to conduct the reviews via interviews and reviews of documentation, to ensure the vendor complies with regulatory requirements and follows security best practices to minimize risk to an acceptable level.

A vendor technology risk (VTR) assessment is conducted using Google VSAQ, in the following steps:

1. Reviewer sends questionnaire link(s) to vendor contact.
2. Vendor completes the questionnaire(s).
3. Vendor saves/exports answers to the assessment questionnaire(s).
4. Vendor contact sends the answers file back to reviewer.
5. Reviewer opens the same questionnaire(s) and loads the answers received from the vendor to complete the assessment.
6. Reviewer follows up with vendor contact as needed.
7. Reviewer facilities discussion with business owner to determine if the risk is acceptable. Vendor remediation may be required depending on the results.

A list of approved vendors / contractors is maintained by the Security and Operations teams.

24.2.2 Vendor Contractual Agreements

GDPR. If the vendor processes data for customers from in the European Economic Area, United Kingdom or Switzerland (the “Designated Countries”), the vendor must be GDPR compliant, and a Data Processing Agreement (DPA) is required.

SLA for Service Providers. For network and infrastructure service providers that support production and/or critical operations at APS, a Service Level Agreement (SLA) is defined and included in the service contract.

As appropriate, the executed agreement(s) are linked or attached to the vendor on the approved vendors list.

24.2.3 Monitoring Vendor Risks

Vendor contracts are reviewed either annually or according to the signed contract duration.

Based on the risk level and the sensitivity/criticality of data the vendor has access to, the vendor review may include an updated risk analysis performed by the security team in addition to legal and business review of contract terms.

If the vendor is a service provider, the DevOps team monitors the service status of the provider according to its SLA. This is done by either manually reviewing the posted service status on the vendor’s status pages at least quarterly, or by setting up alarms for service interruption using automation.

24.2.4 Software and Systems Acquisition Process

APS Security maintains a list of pre-approved business software and a list of approved vendors / contractors.

If additional commercial software, hardware system, or cloud services is needed, a request should be submitted through APS internal service desk. This will trigger the approval by manager/security and procurement process.

As applicable, APS security team may conduct a risk analysis on the software or system to ensure it complies with APS security, compliance and legal requirements and does not interfere with the security controls. If a risk is identified, additional controls should be identified and implemented (or planned) prior to acquisition. An alternative product may be considered as a result of the risk analysis.

25. Privacy and Consent

`Last Reviewed: 2025-02-17:19:44:43-UTC`

APS is committed to protecting the privacy of our customers.

25.1 Policy Statements

APS policy requires that:

(a) Privacy policy shall be made available to inform Customers how APS collects, uses, secures and shares customer information.

(b) Valid consent must be obtained for data collected from a Customer and the purposes data is used for must be provided. Customer must be provided an option to opt-in or opt-out.

25.2 Controls and Procedures

25.2.1 Privacy Policy

Current Privacy Policy is published at https://compliance.aboveproperty.com/privacy-policy/

25.2.2 Notice of Privacy Practice

Current Notice of Privacy Practice (NPP) is published at https://compliance.aboveproperty.com/privacy-policy/

25.2.3 Platform Use Terms and Consent

The Terms of Use and Consent for APS platform and applications are hosted online or within the application itself.

26. Use of Generative AI

26.1 Cybersecurity Policy for the use of Generative AI

26.1.1 Effective Date: March 1 2024

26.1.2 1.0 Purpose

The purpose of this policy is to establish guidelines and best practices for the responsible and secure use of generative artificial intelligence (AI) within our organization. Generative AI refers to technology that can generate human-like text, images, or other media content using AI algorithms.

26.1.3 2.0 Scope

This policy applies to all employees, contractors, and third-party individuals who have access to generative AI technologies or are involved in using generative AI tools or platforms on behalf of our organization.

26.1.4 3.0 Acceptable Use

General Guidelines

DO:

- Understand that GenAI tools may be useful but are not a substitute for human judgment and creativity.
- Understand that many GenAI tools are prone to “hallucinations,” false answers or information, or information that is stale, and therefore responses must always be carefully verified by a human.
- Treat every bit of information you provide to an GenAI tool as if it will go viral on the Internet, attributed to you or the Company, regardless of the settings you have selected within the tool (or the assurances made by its creators).
- Inform your supervisor when you have used a GenAI tool to help perform a task.
- Verify that any response from an GenAI tool that you intend to rely on or use is accurate, appropriate, not biased, not a violation of any other individual or entity’s intellectual property or privacy, and consistent with Company policies and applicable laws. Since general purpose GenAI tools are often trained on data whose provenance you cannot verify, this process should be extensive.

DO NOT:

- Do not use GenAI tools to make or help you make employment decisions about applicants or employees, including recruitment, hiring, retention, promotions, transfers, performance monitoring, discipline, demotion, or terminations.
- Do not upload or input any confidential, proprietary, or sensitive Company information into any GenAI tool. Examples include passwords and other credentials, protected health information, personnel material, information from documents marked Confidential, Sensitive, or Proprietary, or any other non-public Company information that might be of use to competitors or harmful to the Company if disclosed. Doing so may breach your or the Company’s obligations to keep certain information confidential and secure, risks widespread disclosure, and may cause the Company’s rights to that information to be challenged.
- Do not upload or input any personal information (names, addresses, likenesses, etc.) about any person into any GenAI tool.
- ***Do not upload or input any information of any kind about any customer or any customer’s customers/guests into any GenAI tool for any reason.***
- Do not represent work generated by a GenAI tool as being your own original work.
- Do not integrate any GenAI tool with internal Company software without first receiving specific written permission from your supervisor and the Engineering and Security Departments.
- Do not use GenAI tools other than those on the approved list from the Engineering and Security Departments. Malicious chatbots can be designed to steal or convince you to divulge information.

3.1. Authorized Use

Generative AI tools and platforms may only be used for business purposes approved by the organization. Such purposes may include content generation for marketing, product development, research, or other legitimate activities.

3.2. Compliance with Laws and Regulations

All users of generative AI must comply with applicable laws, regulations, and ethical guidelines governing intellectual property, privacy, data protection, and other relevant areas.

3.3. Intellectual Property Rights

Users must respect and protect intellectual property rights, both internally and externally. Unauthorized use of copyrighted material or creation of content that infringes on the intellectual property of others is strictly prohibited.

3.4. Responsible AI Usage

Users are responsible for ensuring that the generated content produced using generative AI aligns with the organization's values, ethics, and quality standards. Generated content must not be use if it is misleading, harmful, offensive, or discriminatory.

26.1.5 4.0 Access and Security

4.1. Authorized Access

Access to generative AI tools, platforms, or related systems should be restricted to authorized personnel only. Users must not share their access credentials or allow unauthorized individuals to use the generative AI tools on their behalf.

4.2. Secure Configuration

Generative AI tools and platforms must be configured securely, following industry best practices and vendor recommendations. This includes ensuring the latest updates, patches, and security fixes are applied in a timely manner.

4.3. User Authentication

Strong authentication mechanisms, such as multi-factor authentication (MFA), should be implemented for accessing generative AI tools and platforms. Passwords used for access should be unique, complex, and changed regularly.

4.4. Data Protection

Users must handle any personal, sensitive, or confidential data generated or used by generative AI tools in accordance with the organization's data protection policies and applicable laws. Encryption and secure transmission should be employed whenever necessary. Inputting sensitive, or confidential organization data into an online AI prompt is prohibited. A DLP (Data Loss Protection) solution should be implemented and used to stop data leaks from AI.

26.1.6 5.0 Monitoring and Incident Response

5.1. Logging and Auditing

Appropriate logging and auditing mechanisms should be implemented to capture activities related to generative AI usage. These logs should be regularly reviewed to detect and respond to any suspicious or unauthorized activities.

5.2. Incident Reporting Any suspected or confirmed security incidents related to generative AI usage should be reported promptly to the organization's designated cybersecurity team or incident response personnel.

5.3. Vulnerability Management Regular vulnerability assessments and security testing should be conducted on generative AI tools and platforms to identify and address any security weaknesses or vulnerabilities.

26.1.7 6.0 Training and Awareness

6.1. Education and Training

Employees and relevant personnel should receive training on the responsible and secure use of generative AI. This training should cover topics such as ethical considerations, potential risks, security best practices, and compliance requirements.

6.2. Awareness Campaigns

Regular awareness campaigns and communications should be conducted to reinforce the importance of cybersecurity, responsible AI usage, and adherence to this policy.

7.0 Non-Compliance

Non-Compliance with this policy may result in disciplinary action, up to and including termination of employment or contract, and legal consequences if applicable laws are violated.

26.1.8 8.0 Policy Review

This policy will be reviewed periodically and updated as necessary to address emerging risks, technological advancements, regulatory changes, and other conditions as necessary.

27. Appendix A. Employee Handbook

27.1 Employee Handbook and Policy Quick Reference

`Last Reviewed: 2025-02-17:19:44:43-UTC`

This is an abridged version of APS's security policy that all workforce members are required to be familiar with and comply with.

- You are required to follow detailed procedures defined in certain policies related to your job role.

Security is everyone's responsibility. If this is not your first job, don't do anything that might get you in trouble at your previous workplace. When in doubt, stop and ask.

Acknowledgement

As a APS employee, I acknowledge that

- I have reviewed and will comply with company security policies and procedures, acceptable use, and sanction policies.
- I accept that my work devices, including approved BYOD devices, and activities on such devices are subject to security monitoring.
- I will protect my work devices at remote locations and will not leave devices unattended.
- I will ensure my laptops and workstations are securely configured with whole disk encryption, endpoint security agent, malware protection, local firewall, password protected screensaver, and latest security patches.
- I will follow documented policies and procedures to protect sensitive and confidential data.
- I understand that customer data and sensitive data may only be stored in approved production environments.
- I understand company and regulatory requirements to protect critical data and will NOT
- store critical data such as customer data and passwords on online file shares (such as Google Drive, SharePoint, Dropbox), in logs and source codes;
- send critical data such as customer data and passwords by email, chat, or similar public communication channels;
- post critical data such as customer data and passwords in blogs, support tickets or other public forums; and
- I understand that use of paper records and fax transmission for sensitive customer data is not allowed.
- I will keep my passwords confidential and will NOT share my individual user passwords with other users.
- I will NOT use shared/generic, guest/anonymous, emergency or temporary accounts without explicit approval.
- I will regularly back up business data on my user devices to approved data storage media/repositories such as the company SharePoint site.
- I will report any incident and suspicious activity to Security and/or my manager.

27.1.1 Training

You will be prompted as part of onboarding, and periodically going forward, to complete the following security training:

- **General security policy and procedures** training, including
- Roles, Responsibilities and Training
- HR and Personnel Security
- Data Classification and Handling
- **Ongoing security awareness** training (a yearly series, currently provided by GLS On Demand)
- **Role-based security** training
- all members of the **Development/Engineering** team must carefully review the following policies and procedures
- Product Security and Secure Software Development
- Data Management
- Data Protection
- Configuration and Change Management
- all members of the **Administrative**, **Marketing** and **Procurement** teams must review the following policies and procedures
- Third Party Security, Vendor Risk Management and Systems/Services Acquisition
- all members of the **Administrative** and **Senior Leadership/Executive** teams must review the following policies and procedures
- Business Continuity and Disaster Recovery
- Compliance Audits and External Communications
- Risk Management
- all members of the **HR** and **Facilities** teams must review the following policies and procedures
- HR and Personnel Security
- Facility Access and Physical Security
- all team members responsible for **Product Management** and **Business Development** must review the following policies and procedures
- Privacy and Consent
- all members of the **Security**, **Compliance** and **IT** teams must review all policies and procedures in its entirety

27.1.2 Acceptable use policy for end-user computing

APS policy requires that:

(a) Per APS security architecture, all workforce members are primarily considered as remote users and therefore must follow all system access controls and procedures for remote access.

(b) Use of APS computing systems is subject to monitoring by APS IT and/or Security team.

(c) Employees may not leave computing devices (including laptops and smart devices) used for business purpose, including company-provided and BYOD devices, unattended in public.

(d) Device encryption must be enabled for all mobile devices accessing company data, such as whole-disk encryption for all laptops.

(e) Use only legal, approved software with a valid license. Do not use personal software for business purposes and vice versa.

(f) Encrypt all email messages containing sensitive or confidential data.

(g) Employees may not post any sensitive or confidential data in public forums or chat rooms. If a posting is needed to obtain technical support, data must be sanitized to remove any sensitive or confidential information prior to posting.

(h) Anti-malware or equivalent protection and monitoring must be installed and enabled on all endpoint systems that are commonly affected by malware, including workstations, laptops and servers.

(i) All data storage devices and media must be managed according to the APS Data Classification specifications and Data Handling procedures.

(j) Mobile devices are not allowed to connect directly to APS production environments.

27.1.3 Your responsibilities for computing devices

APS provides company-issued laptops and workstations to all employees. APS currently does not require or support employees bringing their own computing devices.

The laptops and/or workstations assigned to you are yours to configure and manage according to company security policy and standards. You are responsible to

- configure the system to meeting the configuration and management requirements, including password policy, screen protection timeout, host firewall, etc.;
- ensure the required anti-malware protection and security monitoring agent is installed and running; and
- install the latest security patches timely or enable auto-update.

IT and Security provides automated scripts for end-user system configurations and/or technical assistance as needed.

You are also responsible for maintaining a backup copy of the business files local on your laptop/workstation to the appropriate location on APS file sharing / team site (e.g. SharePoint). Examples of business files include, but are not limited to:

- Documents (e.g. product specs, business plans)
- Presentations
- Reports and spreadsheets
- Design files/images/diagrams
- Meeting notes/recordings
- Important records (e.g. approval notes)

Important

DO NOT backup critical data such as customer data or PII to file sharing sites. If you have such critical data locally on your device, contact IT and Security for the appropriate data management and protection solution.

Unless the local workstation/device has access to **Critical** data, backups of user workstations/devices are self managed by the device owner. Backups may be stored on an external hard drive or using a cloud service such as iCloud if and only if the data is both encrypted and password protected (passwords must meet APS requirements).

You are responsible to ship a replaced device back to IT within ten (10) days of receiving the replacement computing device (e.g.: laptop, cell phone, etc.).

There is no provision for employees to purchase computing devices from APS.

27.1.4 Getting help

Support for most of our business applications are self-service, such as password reset via Microsoft 365.

If needed, users may use our internal service desk to request IT and Security support. Common requests include:

- Password reset and access requests
- Request new software and hardware
- Technical support
- Recommend changes to policies and processes

27.1.5 How to report an incident or suspicious activity

You are responsible to report all suspicious activities and security-related incidents immediately to the Information Security team, by one of the following channels:

- (preferred) DM the Security Officer on APS's slack workspace. For urgent issues requiring immediate attention, open an incident for the Security team on PagerDuty
- "Report a security incident" by creating an issue on Rally and/or via the internal help desk
- If access to Rally is not available, employees may send an email to security@aboveproperty.com
- For non-sensitive, non-confidential security issues and concerns, employees may post questions on APS's #security Slack channel.
- Additionally, employees may report the incident to their direct manager.

28. Appendix B. Approved Software

28.1 Approved Software

`Last Reviewed: 2025-02-17:19:44:43-UTC`

Software approved for use at APS includes, but is not limited to:

- Adobe suite
- Atlassian suite
- Jetbrains suite
- Google Workspaces suite
- Code editors (IntelliJ, PyCharm, WebStorm, VS Code, etc)
- 1Password / BitWarden (The use of LastPass is strongly discouraged due to its poor security record)
- Docker (Due to licensing considerations, Docker Desktop requires explicit approval from the Head of Engineering. APS strongly encourages the use of finch in lieu of Docker Desktop.)
- Node/npm/yarn
- Java (OpenJDK or Amazon Corretto distributions. Due to licensing restrictions, the use of Oracle Java is expressly prohibited.)
- Python 3.7 and later
- Git
- Office 365
- Microsoft 365 (and any apps/services managed by Microsoft 365)
- Postman
- Slack
- Microsoft Teams
- Zoom

Reputable and well documented open source / free software may be used for development purposes at the discretion of the Engineering team. Cb Defense agents must be active to monitor the behavior of all application processes. Additional periodic audit may be conducted to review the usage of open source tools. Examples of such software include, but are not limited to:

- Chrome and various browser extensions
- Firefox and various browser extensions
- Homebrew
- GraphQL/GraphiQL
- Keybase
- Skitch
- Spectacle
- Terraform
- etc.

Software not in the list above may be installed if it is necessary for a business purpose, legal, with a valid license, and approved on a case-by-case basis by your manager or the Security Officer.

29. Appendix C. Approved Vendors

29.1 Approved Vendors

`Last Reviewed: 2025-02-17:19:44:43-UTC`

For confidentiality reasons, the list of approved vendors is maintained internally by Above Property LLC. and is available to customers and business partners by request under NDA.

30. Appendix D. Key Definitions

30.1 Key Definitions

`Last Reviewed: 2025-02-17:19:44:43-UTC`

- *Application*: An application hosted by APS, either maintained and created by APS, or maintained and created by a Customer or Partner.
- *Application Level*: Controls and security associated with an Application. In the case of PaaS Customers, APS does not have access to and cannot assure compliance with security standards and policies at the Application Level.
- *Audit*: Internal process of reviewing information system access and activity (e.g., log-ins, file accesses, and security incidents). An audit may be done as a periodic event, as a result of a patient complaint, or suspicion of employee wrongdoing.
- *Audit Controls*: Technical mechanisms that track and record computer/system activities.
- *Audit Logs*: Encrypted records of activity maintained by the system which provide: 1) date and time of activity; 2) origin of activity (app); 3) identification of user doing activity; and 4) data accessed as part of activity.
- *Access*: Means the ability or the means necessary to read, write, modify, or communicate data/ information or otherwise use any system resource.
- *BaaS*: Backend-as-a-Service. A set of APIs, and associated SDKs, for rapid mobile and web application development. APIs offer the ability to create users, do authentication, store data, and store files.
- *Backup*: The process of making an electronic copy of data stored in a computer system. This can either be complete, meaning all data and programs, or incremental, including just the data that changed from the previous backup.
- *Backup Service*: A logging service for unifying system and application logs, encrypting them, and providing a dashboard for them. Offered with all APS Add-ons and as an option for PaaS Customers.
- *Breach*: A data breach is the intentional or unintentional release of secure or sensitive information to an untrusted environment or individual. A data breach often involves an incident where information is stolen or taken from a system without the knowledge or authorization of the system’s owner.
- *De-identification*: The process of removing identifiable information so that data is rendered to not be personally identifiable .
- *Disaster Recovery*: The ability to recover a system and data after being made unavailable.
- *Disaster Recovery Service*: A disaster recovery service for disaster recovery in the case of system unavailability. This includes both the technical and the non-technical (process) required to effectively stand up an application after an outage. Offered with all APS Add-ons and as an option for PaaS Customers.
- *Disclosure*: Disclosure means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.
- *Customers*: Contractually bound users of APS Platform and/or services.
- *Environment*: The overall technical environment, including all servers, network devices, and applications.
- *Event*: An event is defined as an occurrence that does not constitute a serious adverse effect on APS, its operations, or its Customers, though it may be less than optimal. Examples of events include, but are not limited to:
- A hard drive malfunction that requires replacement;
- Systems become unavailable due to power outage that is non-hostile in nature, with redundancy to assure ongoing availability of data;
- Accidental lockout of an account due to incorrectly entering a password multiple times.
- *Hardware (or hard drive)*: Any computing device able to create and store sensitive data .
- *IaaS*: Infrastructure-as-a-Service.
- *Individually Identifiable Health Information*: That information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

- *Indication*: A sign that an Incident may have occurred or may be occurring at the present time. Examples of indications include:
- The network intrusion detection sensor alerts when a known exploit occurs against an FTP server. Intrusion detection is generally reactive, looking only for footprints of known attacks. It is important to note that many IDS “hits” are also false positives and are neither an event nor an incident;
- The antivirus software alerts when it detects that a host is infected with a worm;
- Users complain of slow access to hosts on the Internet;
- The system administrator sees a filename with unusual characteristics;
- Automated alerts of activity from log monitors like OSSEC;
- An alert from OSSEC about file system integrity issues.
- *Intrusion Detection System (IDS)*: A software tool use to automatically detect and notify in the event of possible unauthorized network and/or system access.
- *IDS Service*: An Intrusion Detection Service for providing IDS notification to customers in the case of suspicious activity. Offered with all APS Add-ons and as an option for PaaS Customers.
- *Law Enforcement Official*: Any officer or employee of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.
- *Logging Service*: A logging service for unifying system and application logs, encrypting them, and providing a dashboard for them. Offered with all APS Add-ons and as an option for PaaS Customers.
- *Messaging*: API-based services to deliver and receive SMS messages.
- *Minimum Necessary Information*: Protected health information that is the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The “minimum necessary” standard applies to all protected health information in any form.
- *Off-Site*: For the purpose of storage of Backup media, off-site is defined as any location separate from the building in which the backup was created. It must be physically separate from the creating site.
- *Organization*: For the purposes of this policy, the term “organization” shall mean APS.
- *PaaS*: Platform-as-a-Service.
- *Partner*: Contractual bound 3rd party vendor with integration with the APS Platform. May offer Add-on services.
- *PMP or Platform*: APS Precision Medicine Platform and its overall technical environment.
- *Precursor*: A sign that an Incident may occur in the future. Examples of precursors include:
- Suspicious network and host-based IDS events/attacks;
- Alerts as a result of detecting malicious code at the network and host levels;
- Alerts from file integrity checking software;
- Audit log alerts.
- *Restricted Area*: Those areas of the building(s) where protected health information and/or sensitive organizational information is stored, utilized, or accessible at any time.
- *Risk*: The likelihood that a threat will exploit a vulnerability, and the impact of that event on the confidentiality, availability, and integrity of sensitive data, other confidential or proprietary electronic information, and other system assets.
- *Risk Assessment*:

  Referred to as Data Protection Imapct Analysis (DPIA) in GDPR

- Identifies the risks to information system security and determines the probability of occurrence and the resulting impact for each threat/vulnerability pair identified given the security controls in place;
- Prioritizes risks; and
- Results in recommended possible actions/controls that could reduce or offset the determined risk.
- *Risk Management*: Within this policy, it refers to two major process components: risk assessment and risk mitigation.

- *Risk Management Team*: Individuals who are knowledgeable about the Organization's Privacy, Security and Compliance policies, procedures, training program, computer system set up, and technical security controls, and who are responsible for the risk management process and procedures outlined below.
- *Risk Mitigation*: A process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk assessment process to satisfactory levels within an organization given its mission and available resources.
- *Role*: The category or class of person or persons doing a type of job, defined by a set of similar or identical responsibilities.
- *SaaS*: Software-as-a-Service.
- *Sanitization*: Removal or the act of overwriting data to a point of preventing the recovery of the data on the device or media that is being sanitized. Sanitization is typically done before re-issuing a device or media, donating equipment that contained sensitive information or returning leased equipment to the lending company.
- *Security Incident* (or just Incident): A security incident is an occurrence that exercises a significant adverse effect on people, process, technology, or data. Security incidents include, but are not limited to:
- A system or network breach accomplished by an internal or external entity; this breach can be inadvertent or malicious;
- Unauthorized disclosure;
- Unauthorized change or destruction of sensitive data (i.e. deletion or alterations not following APS's procedures);
- Denial of service not attributable to identifiable physical, environmental, human or technology causes;
- Disaster or enacted threat to business continuity;
- Information Security Incident: A violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices. Examples of information security incidents may include, but are not limited to, the following:
- Denial of Service: An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources;
- Malicious Code: A virus, worm, Trojan horse, or other code-based malicious entity that infects a host;
- Unauthorized Access/System Hijacking: A person gains logical or physical access without permission to a network, system, application, data, or other resource. Hijacking occurs when an attacker takes control of network devices or workstations;
- Inappropriate Usage: A person violates acceptable computing use policies;
- Other examples of observable information security incidents may include, but are not limited to:
- Use of another person's individual password and/or account to login to a system;
- Failure to protect passwords and/or access codes (e.g., posting passwords on equipment);
- Installation of unauthorized software;
- Terminated workforce member accessing applications, systems, or network.
- *Threat*: The potential for a particular threat-source to successfully exercise a particular vulnerability. Threats are commonly categorized as:
- Environmental - external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, etc.
- Human - hackers, data entry, workforce/ex-workforce members, impersonation, insertion of malicious code, theft, viruses, SPAM, vandalism, etc.
- Natural - fires, floods, electrical storms, tornados, etc.
- Technological - server failure, software failure, ancillary equipment failure, etc. and environmental threats, such as power outages, hazardous material spills.
- Other - explosions, medical emergencies, misuse or resources, etc.
- *Threat Action*: The method by which an attack might be carried out (e.g., hacking, system intrusion, etc.).
- *Threat Source*: Any circumstance or event with the potential to cause harm (intentional or unintentional) to an IT system. Common threat sources can be natural, human or environmental which can impact the organization's ability to protect sensitive data.
- *Trigger Event*: Activities that may be indicative of a security breach that require further investigation.

- *Unrestricted Area*: Those areas of the building(s) where protected health information and/or sensitive organizational information is not stored or is not utilized or is not accessible there on a regular basis.
- *Vendor*: External individuals or organizations marketing or selling products or services, or providing services to APS.
- *Vulnerability*: A weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a threat and lead to a compromise in the integrity of that system, i.e., resulting in a security breach or violation of policy.
- *Workforce*: Means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.
- *Workstation*: An electronic computing device, such as a laptop or desktop computer, or any other device that performs similar functions, used to create, receive, maintain, or transmit sensitive data. Workstation devices may include, but are not limited to: laptop or desktop computers, smart phones, tablet PCs, and other handheld devices. For the purposes of this policy, “workstation” also includes the combination of hardware, operating system, application software, and network connection.

31. Appendix E. Privacy Policy

31.1 Privacy and Cookie Policy

31.1.1 Effective: 1 March 2024.

31.1.2 General Terms

Above Property LLC. (APS) declares to abide by the European General Data Protection Regulation 2016/679 of 27 April 2016 with this Privacy Policy.

31.1.3 Data that we collect about you

Personal data means any information that can identify a natural person or any information that can link to an identifiable natural person. Personal data does not include information that is anonymized and where no natural person can be identified.

31.1.4 Personal data that we collect about you:

Above Property LLC. (APS) is an information technology provider for the hotel and hospitality industry. When you make a hotel reservation at one of our customer hotels, we collect Personal Information (your name, address, email address, and payment data) necessary to complete the reservation. Some of our hotel customers may require us, as a data processor, to verify your age and/or birthday in order to reserve rooms at their hotels. We will only ask for information from you that is necessary to complete a hotel reservation.

31.1.5 How we collect data about you

Above Property LLC. (APS) obtains personal data about you when you use that data to make a hotel reservation at any of our customers' hotels.

31.1.6 Purposes of processing your data

Above Property LLC. (APS) is an information technology provider for the hotel and hospitality industry. When you make a hotel reservation at one of our customer hotels, we may collect Personal Information (your name, address, email address and payment data- collectively, "information") about you in connection with your (or your organization's) use of our Services that link to this Privacy Policy. We will only ask for information from you (such as your name, address, email, and payment data) that is necessary to complete a hotel reservation.

31.1.7 Data Retention

We keep your reservation information, like your name, email address, and home address, for as long as our customer hotel (the data controller) instructs us to. We also keep information about you and your use of the Services for as long as necessary for our legitimate business interests, for legal reasons, and/or to prevent harm.

31.1.8 Transfer of data

We may share your information with our business units, affiliates, subsidiaries, business partners, service providers and/or your representatives, in order to provide or improve our Services to you. We do not share information with third parties so that they can independently market their own products or services to you unless we have explicitly given you the option to opt-in or opt-out of such disclosures. We will never sell your Personal Information to any third party without your express written consent.

We may share your data with the following categories of third parties:

- Employees of Above Property LLC. (APS)
- Contractors in order to provide services
- Employees and Contractors at the hotel where you made your reservation
- Payment processors in order to process online payments, bank transfers and merchant banks
- Professional advisors such as accountants, auditors
- Legal authorities and law enforcement such as the police, tax authorities

We do not allow our service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

We guarantee a similar level of protection by imposing contractual obligations to our subcontractors that are similar to this Privacy Policy.

We share data with the following specific third parties:

- Google Analytics: we use Google Analytics to anonymously gather statistics about Website users in order to maintain and improve the user experience and Website. Google Analytics is a third-party service provided by Google and this Privacy Policy does not cover the processing performed by Google. For more information about how Google collects and processes your data, please refer to their privacy policy.
- FreedomPay: some of our hotel customers use FreedomPay as their credit card processor, and we may use FreedomPay to make your credit card transactions more secure. FredomPay requires that certain reservation details, such as Guest Name and Dates of Stay, accompany payment information so the hotel is able to associate a credit card with a specific reservation. FreedomPay is a third-party service and this Privacy Policy does not cover the processing performed by FreedomPay. For more information about how FreedomPay collects and processes your data, please refer to their privacy policy.
- Shift4: some of our hotel customers use Shift4 as their credit card processor, and we may use Shift4 to make your credit card transactions more secure. Shift4 requires that certain reservation details, such as Guest Name and Dates of Stay, accompany payment information so the hotel is able to associate a credit card with a specific reservation. Shift4 is a third-party service and this Privacy Policy does not cover the processing performed by Shift4. For more information about how Shift4 collects and processes your data, please refer to their privacy policy.
- Stripe: some of our hotel customers use Stripe as their credit card processor, and we may use Stripe to make your credit card transactions more secure. Stripe requires that certain reservation details, such as Guest Name and Dates of Stay, accompany payment information so the hotel is able to associate a credit card with a specific reservation. Stripe is a third-party service and this Privacy Policy does not cover the processing performed by Stripe. For more information about how Stripe collects and processes your data, please refer to their privacy policy.

31.1.9 Third party external links

We may include links to third party websites, applications, or plug-ins. By clicking on those links you may allow third parties to collect or share data about you. We do not control these third party websites and this Privacy Policy does not cover the processing performed by them. We suggest you check the third party websites for more information about how they handle personal data.

31.1.10 Security measures

We have implemented appropriate technical and organizational measures, procedures and safeguards to prevent the destruction, loss, adjustment, accidental notification to a third party, removal and unauthorized access of personal data.

We maintain physical, electronic, and procedural safeguards to protect your information related to your hotel reservations. These include but are not limited to:

- Server encryptions
- SSL Certificates
- Physically secured servers
- Antivirus and Firewall
- Regular backups
- Encrypted passwords

We only allow access to your personal data to those employees, contractors and other third parties who have a business need to know. They only process your personal data on our instructions and are subject to a duty of confidentiality.

31.1.11 Cookies

A cookie is a small text file that is sent from the server of Above Property LLC. (APS) and is stored on your computer's hard drive. This allows us to remember your preferences when visiting our Website. The information stored through these cookies can only be read by Above Property LLC. (APS) and only for the duration of your visit to the Website.

Our Website uses cookies and similar technologies to identify you from other users of our Website. This allows us to offer you a better experience when you visit our Website and to optimize our Website in the meantime.

When you use the Website, your device or browser may be sent cookies from third parties, for example when using embedded content and social network links. It's important for you to know that we have no access to or control over cookies used by these companies or third-party websites. We suggest you check the third party websites for more information about their cookies and how to manage them.

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly.

31.1.12 Your GDPR rights (For EU Individuals)

Under the General Data Protection Regulation, data subjects within the European Economic Area are entitled to the following rights:

- Right of access – you have the right to be informed on how we use your personal data and you have the right to request access to the personal data that we have collected about you;
- Right of rectification – you have the right to correct inaccurate information that we may have about you;
- Right to object – you have the right to object to us processing your personal data;
- Right to restrict processing – you have the right to request us to suspend processing under certain circumstances;
- Right to data portability – you have the right to obtain a copy of your personal data in an easily readable format in order to transfer to another service;
- Right to erasure – otherwise known as the 'right to be forgotten' meaning that you have the right to request that we delete all the personal data that we have on you (with certain legal exceptions);
- Right to withdraw consent – where the processing is based on consent, you have the right to at all times, withdraw your consent.

31.1.13 If you wish to exercise any of your rights under the General Data Protection Regulation:

You can contact Above Property LLC. (APS) directly regarding matters pertaining to GDPR:

Above Property LLC
3555 Kraft Road, Suite 400
Naples, Fl 34105
U.S.A.

Telephone: +1 239 263 7406
Email: privacy@aboveproperty.com

We are committed to providing you with a response to your request within 30 days. However, if there are delays in providing you with your request, we will notify you of the delay, the reason for the delay and extend our response time.

31.1.14 Right to make a complaint

You have the right to make a complaint at any time with:

Data Protection Authority
Rue de la Presse 35, 1000 Brussels
Tel : +32 2 274 48 00
Fax : +32 2 274 48 35
contact@apd-gba.be

31.1.15 International transfers

APS is a U.S.-based company that offers our Services to U.S. and international customers. As a result, information that we collect, including personal information, may be transferred to our data centers or service providers in the U.S. By providing your personal information to us, you are consenting to the transfer of your personal information to the U.S. and to our (and our services providers') use and disclosure of your personal information in accordance with this Privacy Policy.

Due to the global nature of our operations, these transfers will involve transferring your data outside the European Economic Area to the United States. We ensure that there is an adequate level of protection for personal data in the receiving entity.

31.1.16 The Data Privacy Framework for EU, UK and Swiss Individual's Data Transfer to the United States

Above Property LLC. (APS) complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Above Property LLC. (APS) has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Above Property LLC. (APS) has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit:

https://www.dataprivacyframework.gov

Pursuant to the Data Privacy Framework the following notifications apply to EU, UK and Swiss personal data that is transferred into the United States:

The Federal Trade Commission has jurisdiction over Above Property LLC. (APS)'s compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF). EU, UK and Swiss individuals have the right to access their personal data. Individuals wishing to exercise this right may do so by contacting us as specified in the GDPR section of this document.

Above Property LLC. (APS) is liable for the onward transfer of EU, UK and Swiss data to third parties acting as our agents unless we can prove we were not a party giving rise to the damages.

We do not permit the use of EU, UK and/or Swiss data for reasons that are materially different from those for which the data was originally provided. If this practice should change in the future, we will update this policy and provide individuals with opt-out or opt-in (as applicable) choice prior to the release of their information.

We may be required to disclose EU, UK and/or Swiss personal data in response to lawful requests by public authorities including to meet national security and law enforcement requirements.

In compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), Above Property LLC. (APS) commits to resolve complaints about our collection or use of your personal information transferred to the U.S. pursuant to the EU-U.S. DPF, the UK extension to the EU-U.S. DPF, and the Swiss-U.S. DPF. EU, UK, and Swiss individuals with inquiries or complaints should first contact Above Property LLC. (APS). You can contact us at:

Above Property LLC
3555 Kraft Road, Suite 400
Naples, Fl 34105
U.S.A.

Telephone: +1 239 263 7406
Email: privacy@aboveproperty.com

Above Property LLC. (APS) has further committed to refer unresolved DPF Principles-related complaints to a U.S.-based independent dispute resolution mechanism, JAMS. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit https://www.jamsadr.com/DPF-Dispute-Resolution for more information and to file a complaint. This service is provided free of charge to you.

If your DPF complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See https://www.dataprivacyframework.gov/program-articles/How-to-Submit-a-Request-Relating-to-U-S-National-Security-Access-to-Data

31.1.17 Changes to this Privacy Policy

We may update this Privacy Policy from time to time to incorporate new rules or guidance issued under the General Data Protection Regulation, Data Privacy Framework, the UK Extension to the EU-U.S. DPF, the Swiss-U.S. Data Privacy Framework and local privacy and data protection legislation. A notice will be posted on the Website for 60 days whenever this Privacy Policy is changed in a material way.

32. Appendix F. Cookie Policy

32.1 COOKIE POLICY

We at APS (Above Property LLC. and our subsidiaries and affiliates) are committed to protecting your privacy. We and our partners use cookies and similar technologies on our services, including our websites and mobile applications (the “Services”). This Cookie Policy explains these technologies, why we use them, and the choices you have.

By visiting or using our Services, you are consenting to us gathering and processing information (as defined in our Privacy Policy) about you in accordance with this Cookie Policy.

32.2 TECHNOLOGIES WE USE

Like many Internet-enabled services, we use technologies that place small files/code on your device or browser for the purposes identified in our Privacy Policy, primarily to remember things about you so that we can provide you with a better experience.

Cookies. A cookie is a small data file stored on your browser or device. They may be served by the entity that operates the website you are visiting (“first-party cookies”) or by other companies (“third-party cookies”).

- For example, we partner with third-party analytics providers, like Google, which set cookies when you visit our websites. This helps us understand how you are using our Services so that we can improve them.

Pixels (Clear Gifs/Web Beacons/Web Bugs/Embedded Pixels). These are small images on a web page or in an email. They collect information about your browser or device and can set cookies.

Local Storage. Local storage allows data to be stored locally on your browser or device and includes HTML5 local storage and browser cache.

Software development kits (“SDKs”). SDKs are blocks of code provided by our partners that may be installed in our mobile applications. SDKs help us understand how you interact with our mobile applications and collect certain information about the device and network you use to access the application.

32.3 OUR USE OF THESE TECHNOLOGIES

Below are the ways that we and our partners use these technologies on our Services.

CATEGORY OF USE	PURPOSE OF USE
Preferences	To help us remember your settings and preferences so that we can provide you with a more personalized experience.
Authentication and Security	To log you into the Services; enable us to show you your account data; and help us keep your data and the Services safe and secure.
Service Features and Performance	To provide you with functionality and optimize the performance of the Services. For example, to allow you to share information from APS mobile apps with friends within your social networks/ circles.
Analytics and Research	To help us understand how you are using the Services so that we can make them better, faster, and safer.

32.4 YOUR CHOICES

You have a number of options to control or limit how we and our partners use cookies and similar technologies, including for advertising. Please note that APS websites and our Services do not respond to Do Not Track signals because we do not track our users over time and across third-party websites to provide targeted advertising.

You can set your device or browser to accept or reject most cookies, or to notify you in most situations that a cookie is offered so that you can decide whether to accept it. However, if you block cookies, certain features on our Services may not function. Additionally, even if you block or delete Cookies, not all tracking will necessarily stop.

- To prevent your data from being used by Google Analytics, you can install Google’s opt-out browser add-on.
- For information on how our advertising partners allow you to opt out of receiving ads based on your web browsing history, please visit http://optout.aboutads.info/.

32.5 CONTACT US

If you have questions about our use of cookies and similar technologies, please contact us at security@aboveproperty.com.

Security Officer
Above Property LLC.
3555 Kraft Road, Suite 400 Naples Fl 34105 USA

33. Appendix G. GDPR Data Processing Agreement

33.1 GDPR Data Processing Agreement/Addendum (“DPA”)

33.2 Data Protection Addendum

This Data Protection Addendum (this “Addendum”) is made and entered into as of the date appearing on the signature page hereto (the “Effective Date”) by and between Above Property LLC. (“Company”) and the Supplier named on the signature page hereto, and upon execution shall be incorporated by reference into each agreement for services (“Services Agreement”) pursuant to which Supplier may Process (as defined below) Personal Data (as defined below) for, from, or on behalf of Company.

33.2.1 A. Personal Data Protection

For the purposes of this Addendum, the terms “Controller”, “Data Subjects”, “Personal Data”, “Personal Data Breach”, “Processor” and “Process” shall have the meaning as defined in the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (“GDPR”) or any successor European Union data protection framework.

The parties agree that to the extent Supplier, in the context of performing the agreed services, processes any Personal Data of Company, Supplier shall be the Processor and Company shall be the Controller of such Personal Data. Notwithstanding any obligations of Company as Controller under applicable data protection law, Supplier undertakes the following as Processor:

(a) to process any Personal Data only on behalf and in accordance with Company’s documented instructions and not for any purposes other than those described in this Addendum, unless (i) Company has given its express prior consent or (ii) Supplier is strictly required to do so under applicable European Data Protection Law (as defined below); in such a case, Supplier shall inform Company of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. The subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and the categories of Data Subjects are further specified in Exhibit 1 to this Addendum.

(b) to comply with (i) the GDPR and any applicable European data protection laws and regulations (collectively “European Data Protection Law”), and (ii), in case Supplier is certified under the EU-U.S. and/or Swiss-U.S. Privacy Shield Framework, or any successor program recognized under European Data Protection Law to provide for an adequate level of data protection, the principles of such applicable Privacy Shield Framework or successor program, and (iii) all other applicable data protection and privacy laws and regulations ((i) to (iii) collectively “Data Protection Laws”).

(c) to implement appropriate technical and organizational measures in such a manner that the Processing, including by any Sub-Processors (as defined below), will meet the requirements under Data Protection Laws and ensure the protection of the rights of the Data Subjects, and to regularly test, assess and evaluate the effectiveness of and, as necessary, improve and update these measures. The measures shall ensure a level of data security appropriate to the risks for the rights and freedoms of the Data Subjects. In particular, Supplier shall protect the personal data against accidental or unlawful destruction, loss or alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise Processed.

(d) to keep Personal Data strictly confidential and to ensure, and be able to demonstrate on request, that (i) only those persons have access to the Personal Data who are authorized by Supplier and have a strict need to know the data for the purposes under this Addendum, and (ii) all persons with access to Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(e) to disclose Personal Data to third parties, including affiliated companies, and/or to engage another Processor for the Processing of Personal Data (“Sub-Processor”) only with Company’s express prior consent. Where Supplier is authorized to engage another Sub-Processor for carrying out Processing activities on behalf of Company, Supplier shall enter into a written contract with the Sub-Processor which (i) imposes on the Sub-Processor the same data protection obligations as set forth in this Agreement, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements under Data Protection Laws, and (ii) grants Company the right to directly audit the Sub-Processor as set forth under Section A(j). Supplier shall promptly send a copy of any sub-processor agreement it concludes under this Section A(e) to Company. Supplier shall select the Sub-Processor diligently, taking into account the technical and organizational measures it has implemented, and ensure, by carrying out audits before and regularly

after the commencement of the data processing by such Sub-Processor, that it maintains appropriate technical and organizational measures to safeguard an adequate level of data protection within the meaning of European Data Protection Law. Supplier shall remain fully liable to Company for the performance of this Agreement and be responsible and liable for any act or omission of the Sub-Processor with respect to its data protection obligations.

(f) to assist Company, including by appropriate technical and organizational measures, insofar as this is possible and taking into the nature of the processing, in fulfilling its obligations in relation to requests from Data Subjects for exercising their Data Subject's rights under Data Protection Laws, including, but not limited to, the Data Subject's right of access, right to rectification and erasure, right to restriction of processing, right to data portability and right to object, as provided for under the GDPR.

(g) to assist Company, taking into account the nature of the processing and information available to Supplier, in ensuring compliance with the obligations under applicable Data Protection Laws, including, in particular, by providing all information and assistance to enable Company (i) to comply with applicable data security obligations, (ii) to carry out a data protection impact assessment or prior consultation with the supervisory authority, as required under European Data Protection Law, and (iii) to respond promptly and properly to any enquiries concerning the Processing of Personal Data and cooperate in good faith with the supervisory authorities, the Data Subjects or any third party within a reasonable time. Supplier shall not communicate with any supervisory authority, Data Subject or any third party in connection with the Processing of Company's Personal Data without prior approval from Company, except as expressly permitted in this Section A.

(h) to notify Company, without undue delay, in writing or via e-mail (i) of any intended change of the locations currently set out in Exhibit 1 to this Addendum for the Processing of Personal Data, (ii) in case of a dispute, claim or request brought by a Data Subject directly against Supplier, (iii) in the event of any measure, request or other communication by a supervisory authority, including about any legally binding request for access or disclosure of Personal Data by a public authority (unless otherwise legally prohibited, in which case the Supplier will use its best efforts to obtain the right to waive this prohibition), and provide reasonable assistance if Company wishes to contest the request, and (iv) of any suspected or actual Personal Data Breach, any breach of applicable Data Protection Laws or of this Addendum. Supplier shall promptly remedy any breach and cooperate with Company in the investigation and remedy of such breaches and provide all reasonable assistance and information to enable Company to comply with, or, as applicable, to avoid, any data breach notification obligations vis-à-vis supervisory authorities and/or Data Subjects. Supplier shall further immediately inform Company if, in its opinion, an instruction infringes Data Protection Laws and/or Supplier becomes aware of the existence of any local laws that would have a substantial adverse effect on the guarantees and undertakings provided for under this Addendum.

(i) at the choice of Company, to return to Company (in a standard format facilitating portability) and/or to securely delete/destroy all Personal Data, including all existing copies thereof, in accordance with Company's instructions, within thirty (30) days upon Company's request or after the end of the provision of the services relating to Processing, and to certify to Company in writing that it has done so. Supplier shall not be obliged to delete/destroy all copies of the Personal Data where a longer storage by Supplier is required under European Data Protection Law, in which case Supplier shall inform Company accordingly, including about the legal grounds for, and the term of, any further storage;

(j) to make available to Company all information necessary to demonstrate compliance with the obligations under Data Protection Laws applicable to Company and to allow for and contribute to audits, including on-site inspections, conducted by Company or another auditor mandated by Company. (k) to enter into any further agreements that may be required under Data Protection Laws relating to Personal Data, and to provide all other assistance and support to Company.

33.2.2 B. Changes to this Addendum

The parties agree that, to the extent required under applicable Data Protection Laws, such as due to legislative changes, court decisions, and/or to reflect measures or guidance from the competent supervisory authorities or the European Commission, including, without limitation, the adoption of standards for contracts with processors according to Art. 28(7) or (8) GDPR or the invalidation, amendment, replacement or repeal of a decision adopted by the EU Commission in relation to international data transfers on the basis of Art. 45(3) or Art. 46(2) GDPR or on the basis of Article 25(6) or 26(4) of EU Directive 95/46/EC, such as, in particular, with respect to the EU Standard Contractual Clauses or similar transfer mechanisms, Company may request reasonable changes or additions to this Addendum to reflect applicable requirements.

33.2.3 C. Third party beneficiary clause

The parties agree that affiliates of the Company shall be entitled under and can enforce the terms of this Addendum against Supplier as third-party beneficiaries.

33.2.4 D. Termination

In the event of Supplier's violation of any obligation under Data Protection Laws or this Addendum, Company, without prejudice to any other rights which it may have, shall be entitled to terminate any Services Agreement forthwith. Any terms of this Addendum that by their nature extend beyond the termination of the Services Agreement, including without limitation this Addendum, Section A(i), shall remain in effect.

33.2.5 E. Precedence

In the event of a conflict between this Addendum and other provisions of the Services Agreement, this Addendum shall prevail.

[Signature page follows.]

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed as of _____, ___, 20___ by their respective officers thereunto duly authorized.

COMPANY:
Above Property LLC.

By:
Name:
Title:

SUPPLIER:

_____

By:
Name:
Title:

33.3 Exhibit 1 to Data Protection Addendum

Description of Processing

33.3.1 A. Subject-matter, nature and purpose of the Processing

Supplier provides certain services to Company, including *[insert general description of services relating to processing of personal data]*, as further specified in the Services Agreement. In the context of performing the obligations under the Services Agreement, Supplier may Process certain of Company's Personal Data as necessary for the purposes of *[insert purposes of Processing]*, as further specified in the Services Agreement. Such processing may include:
[insert description of relevant data processing activities/operations].

33.3.2 B. Duration of the Processing

[insert duration of data processing, e.g.: "The agreed Processing of Personal Data shall commence upon the effective date of the Services Agreement and be carried out for the term of the Services Agreement. The services relating to Processing of Personal Data shall automatically end in case the Services Agreement is effectively terminated or expires, in which case the Personal Data shall be handled in accordance with Section A(i). To the extent the Processing of Personal Data by Supplier is necessary for the winding-up of the Services Agreement, e.g. with respect to returning the Personal Data, the provisions of Section A shall continue to apply until the completion of the winding-up."]

33.3.3 C. Categories of Data Subjects

The Processing will concern the following categories of Data Subjects:
[insert categories of data subjects concerned, e.g.: a. Company employees and job candidates b. Managers, employees, agents or other contact persons at business partners c. Company customers that are natural persons d. Patients, research subjects or other customers of Company's clients]

33.3.4 D. Types of Personal Data

The Processing will concern the following types of Personal Data *[insert types of Personal Data concerned, e.g.:]*

- **a) Company employees and job candidates:**
  name, contact details (address, phone number and direct line, e-mail address), birth date/ country, gender, education (e.g., highest education level, country, degree, certificates), job information about current and previous employment (position, kind of work, work location, salary, replacement, company, location, department, position, function, grade, supervisor, employee class, grade and labor start/ entry date, labor agreement, business title, full or part-time, shifts, working hours), professional skills, CV and resume, training, compensation and remuneration (e.g., compensation rate, salary, target bonus, incentives, benefits), individual development plan, performance goals and assessment, position in company, bank account number and corporate credit card number, national ID and social security number, information about an immigration background.
- **b) Managers, employees, agents or other contact persons at business partners:**
  contact details (name, address, phone number and direct line, e-mail address).
- **c) Company customers that are natural persons:**
  name, contact details (address, phone number and direct line, e-mail address), information regarding purchases of such customers, bank account details, credit information, information about such customers' interest in Company products.
- **d) Patients, research subjects or other customers of Company's clients:**
  [insert the type of data in this category that your service providers might handle]

The Processing will concern the following special categories of data[^1]:
[…]

The Processing will include Personal Data relating criminal convictions and offenses relating to:
[…]

[^1]: *"Special categories of data" means any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.*

34. Appendix H. NIST Controls mapping

34.1 NIST Mappings to APS Policies and Controls

`Last Reviewed: 2025-02-17:19:44:43-UTC`

Below is a list of NIST SP 800-53 Controls Families and the mappings to APS policies and controls in place.

ID	NIST SP 800-53 Control Family	APS Policies and Controls
AC	Access Control	Access
AT	Awareness and Training	Roles and Responsibilities
AU	Audit and Accountability	Roles and Responsibilities; Compliance Audits
CA	Security Assessment and Authorization	Risk Management; Access
CM	Configuration Management	Configuration and Change Management
CP	Contingency Planning	Business Continuity and Disaster Recovery
IA	Identification and Authentication	Access
IR	Incident Response	Incident Response; Breach Notification
MA	Maintenance	Configuration and Change Management
PE	Physical and Environmental Protection	Facility and Physical Security
PL	Planning	Security Program Overview; Security Architecture & Operating Model
PS	Personnel Security	HR & Personnel Security
RA	Risk Assessment	Risk Management
SA	System and Services Acquisition	Third Party Security, Vendor Risk Management and Systems/Services Acquisition
SC	System and Communications Protection	Data Management; Data Protection; and Threat Detection & Prevention
SI	System and Information Integrity	Data Management; Data Protection; Product Security & Secure Software Development; Vulnerability Management;and System Audits, Monitoring & Assessments
PM	Program Management	Security Program Overview; Roles and Responsibilities; and Policy Management

35. Appendix I. PCI DSS Controls Mapping

35.1 PCI DSS 3 Requirements Mapped to APS Policies and Controls

`Last Reviewed: 2025-02-17:19:44:43-UTC`

Below is a list of PCI DSS 3.x Requirements and the mappings to APS policies and controls in place.

ID	PCI DSS 3 Requirement	APS Policies and Controls
1	Configure and use firewalls to protect cardholder data	HR and Personnel; Access; Data Protection; SDLC; Configuration & Change Management; Threat Detection and Prevention; Mobile Device Security and Media Management; Model
2	Do not use the vendor's default settings for system passwords and other security parameters	Model; Roles & Responsibilities; Risk Management; Asset Inventory Management; Data Management; Data Protection; Configuration and Change Management; Mobile Device Security and Media Management
3	Protect stored cardholder data	Data Management; Data Protection; Mobile Device Security and Management
4	Encrypt cardholder data when transmitting over open, public networks	HR and Personnel Security; Data Protection; Secure Software Development and Product Security
5	Protect all systems against malware and update anti-virus software regularly	System Audits, Monitoring and Assessments; HR and Personnel Security; Access; Configuration and Change Management; Threat Detection and Prevention; Mobile Device Security and Management
6	Develop secure systems and applications	Model; Roles, Responsibilities and Training; Risk Management and Risk Assessment Process; System Audits, Monitoring and Assessments; Secure Software Development and Product Security; Configuration and Change Management; Threat Detection and Prevention; Vulnerability Management; Mobile Device Security and Media Management
7	Restrict access to cardholder data based on business requirements	Access; Data Management
8	Identify and authenticate access to system components	Roles, Responsibilities and Training; System Audits, Monitoring and Assessment; Access
9	Restrict physical access to cardholder data	"Facility Access and Physical Security"; Asset Inventory Management; Mobile Device Security and Media Management
10	Track and monitor all access to network resources and cardholder data	Roles, Responsibilities and Training; System Audits, Monitoring and Assessments; Configuration and Change Management
11	Test security systems and processes regularly	Roles, Responsibilities and Training; System Audits, Monitoring and Assessments; Access; Secure Software Development and Product Security; Threat Detection and Prevention; Vulnerability Management
12	Create a policy that addresses information security for all staff	Roles, Responsibilities and Training; Policy Management; Risk Management and Risk Assessment Process; HR and Personnel Security; Secure Software Development and Product Security; Incident Response; Breach Investigation and Notification; Third Party Security and Vendor Risk Management

35.2

36. PCI DSS Program Charter

`Last Reviewed: 2025-02-17:19:44:43-UTC`

36.1 Background

APS accepts credit cards as a form of payment for services related to the hotel and hospitality industry, specifically to guarantee hotel room reservations on behalf of our hotel customers. APS is contractually responsible with our acquiring banks for the security of customer cardholder data; the security requirements are defined by the Payment Card Industry Data Security Standard (PCI DSS).

36.2 Business Need

Achieving point-in-time compliance can be a difficult task in itself, but sustaining compliance has proven to be more difficult. Achieving and maintaining PCI compliance is mission critical at APS. Maintaining compliance is accomplished through collaboration from critical stakeholders including information security, technical operations teams, and business operations. Without clear and effective communication, compliance cannot be achieved.

Business operations support is crucial in achieving and maintaining compliance with the PCI DSS; PCI compliance is more than an IT Operations and Security initiative that requires input from the entire organization. The following are core reasons the company and business operations need to address PCI DSS compliance:

1. It shows customers that the company takes the security of their private data and information seriously and adequately protect it with the guidelines set down by the major card brands Visa, MasterCard, American Express, and Discover.
2. The business will enhance its reputation with both customers and banking partners and facilitate a trust relationship.
3. Implementing PCI DSS security compliance program will demonstrate a commitment to enhancing the purchasing experience for the consumer.

36.3 Program Goals and Objectives

The primary goal of the PCI Program is to achieve and maintain PCI Compliance while reducing risks associated with the transmission, processing, and storage of cardholder data. This will be accomplished by:

- Educating personnel on credit card security and best practices
- Maintaining a library of actionable policies, standards, and procedures
- Securing technologies handling cardholder data with industry best practices in accordance with the PCI DSS

The secondary goal of the PCI Program is to establish business as usual (BAU) processes to facilitate ongoing PCI compliance. This will be accomplished by:

- Defining critical roles and responsibilities
- Developing a Steering Committee
- Developing a process to identifying organizational changes that impact PCI compliance

36.4 Program Objectives Statements

The primary objectives of the PCI Program include:

- Develop a robust inventory of policies, standards, and procedures
- Establish repeatable, compliant processes and procedures
- Establish and deploy PCI-relevant security training materials
- Achieve and maintain a constant state of PCI Compliance (business as usual)
- Establish an inventory of critical roles and responsibilities
- Develop a centralized compliance validation process
- Develop a centralized reporting process
- Establish visibility and collaboration across the organization through a PCI Steering Committee
- Proactively identify and document key changes impacting PCI compliance

36.5 Success Factors

The following factors will determine if the program is succeeding; these are not the specific criteria that will be used to measure program success or failure, but rather are the benchmarks the program requires in order to be successful.

The continued success of the PCI Program is contingent upon the following activities being completed:

- Quarterly steering committee meetings, including reviews of:

a. Daily log reviews

b. Firewall rule-set reviews

c. Application of configuration standards to new systems

d. Security alert responses

e. Change management processes

- Annual PCI DSS compliance certification
- Annual security awareness training with quarterly knowledge review
- Annual review of policies and standards
- No cardholder data breaches in previous year

36.6 Risks

Risks may be related to the business, technology, or a combination thereof. These risks should be analyzed and validated periodically as the program moves forward.

PCI Program risks include but are not limited to:

- Mergers and acquisitions having an unforeseen impact to PCI compliance
- PCI DSS Requirements changes over time impacting PCI compliant status
- Evolving sophistication of criminals and techniques compromises security

36.7 Program Constraints

It is imperative to document assumptions and constraints, both real and perceived that may impact the PCI Program from achieving its goals. Constraints may be related to the business, technology, or a combination thereof. These assumptions and constraints should be analyzed and validated periodically as the program moves forward.

PCI Program constraints include:

- Maintaining a large scope across multiple operations (e.g., locations and entities)
- Enforcing configuration and hardening guidelines across the enterprise
- Effectively segmenting in-scope systems
- Migrating from “point in time” assessment mentality
- Raising employee security education and awareness
- Assigning and enforcing control ownership
- Limited resources dedicated to PCI Compliance
- PCI requirements evolve

36.8 Charter Change Procedures

The PCI Program Charter is a “living document” maintained by the Chief Security Officer. The CSO reviews the Program Charter on an annual basis and provides updates as required. Change Control procedures are adhered to during the update process and the Program Charter is under version control at all times. Updated versions are submitted to the Security Committee and subsequently provided to all stakeholders.

36.9 Charter Acceptance

All members of the Security Committee attest to the objectives and goals of the PCI Program Office and commit to serving in an advisory capacity to the governance teams, guiding and monitoring the PCI Program Office to ensure compliance with the Payment Card Industry Data Security Standard (PCI-DSS).

37. Appendix K. Current PCI DSS AOC

37.0.1 Current PCI DSS Certification document

`Last Reviewed: 2025-02-17:19:44:43-UTC`

For convenience and off line viewing, we provide a PDF of our most current PCI DSS AOC.

Current penetration test and vulnerability scan reports are available by request under appropriate NDA, as are infrastructure and data flow diagrams.

37.1

38. PCI DSS4 Notes

`Last Reviewed: 2025-02-17:19:44:43-UTC`

38.1 Background

APS will adhere to all requirements in the PCI DSS 4 standard, which is mandatory as of 2025. Certain requirements of DSS 4 do not apply in our implementation, and the standard requires documentation for such cases. This document serves as the repository for all such documentation.

38.2 Requirement 11.3.1.2

11.3.1.2 requires that Internal vulnerability scans are performed via authenticated scanning as follows:

- Systems that are unable to accept credentials for authenticated scanning are documented.
- Sufficient privileges are used for those systems that accept credentials for scanning.
- If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2.

APS in-scope systems (the “payment services gateway”) do include methods for user authentication. However, the payment services gateway does not itself require authentication of any kind. The payment services gateway acts solely as a pass-through proxy for transactions that contain PAN data; the only business function they are capable of is extraction of PAN data, forwarding it to 3rd parties for tokenization, reassembling the original transaction using the tokenized data, and then passing it on downstream to out of scope systems for business processing. Downstream, out of scope systems may require that authentication data be present, but the in scope systems do not in any way require or use authentication to perform the in scope tasks.

38.3 Requirements 12.8.4 and 12.8.5

38.3.1 Our capacity as a TPSP

APS must acknowledge in writing to our customers that we are responsible for the security of account data possessed, stored, processed or transmitted on behalf of the customer, and must also accept responsibility to the extent that we could impact the security of the customer’s Cardholder Data Environment (CDE).

APS must support our customers’ requests for information to meet PCI DSS compliance requirements by providing the following upon request:

- PCI DSS compliance status information for any service performed on behalf of the customers (Requirement 12.8.4).
- Information regarding which PCI DSS requirements are our responsibility which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5).
- Response template:

By providing services to the entity, APS acknowledges and agrees that it is responsible for maintaining the security of any account data it possesses, stores, processes, or transmits on behalf of the entity, or to the extent that it could impact the security of the entity’s Cardholder Data Environment (CDE) and customers cardholder data, in accordance with the Payment Card Industry Data Security Standard (PCI DSS) and any other applicable laws, regulations, or industry standards. APS further acknowledges and agrees to implement and maintain appropriate security measures and controls to safeguard such data, including but not limited to encryption, access controls, monitoring, and incident response. APS shall promptly notify the entity

of any actual or suspected security breach or unauthorized access to such data and shall cooperate with the entity in investigating and resolving such incidents. This provision shall survive the termination or expiration of any agreement or relationship between the parties.

38.4 Requirement 12.9.2

APS responds in a timely manner to customers and TPSP requests for documentation related to our compliance posture. Our AOC and security policies are always available on line at https://compliance.aboveproperty.com

39. Responsible Disclosure Guidelines

We at Above Property LLC. (APS) are committed to the security of your data. If you believe that you have discovered a security vulnerability in our software or web sites, we ask that you follow basic industry standard responsible disclosure practices. We may compensate you if you responsibly report a vulnerability that we were unaware of and that requires us to address via code changes or configuration updates.

Reports should include at minimum a screenshot or a video of a proof-of-concept exploit. Vulnerability reports that do not include clear evidence of a proof-of-concept exploit or a description of an exploit clear enough for us to reproduce will be ignored.

Please submit vulnerability reports to security@aboveproperty.com. Email us for a PGP key if you would like to encrypt your message.

39.1 Rules of Engagement

- No Denial of Service testing
- No Physical or Social Engineering
- No testing of Third-party Services
- No uploading of any vulnerability or client-related content to third-party utilities (e.g. Github, DropBox, YouTube)
- All attack payload data must use professional language
- If able to gain access to a system, accounts, users, or user data, stop at point of recognition and report. Do not dive deeper to determine how much more is accessible.
- Low Impact Vulnerabilities - Out of Scope
- We will respond to you within two business days, and ask that your disclosure remain confidential during reasonable periods required to address it. We will set reasonable expectations for our communication responses, and ask that you be responsive as well.

39.2 Scope

The following vulnerabilities are considered low impact and will be marked as Out of Scope if submitted:

- Descriptive error messages (e.g. Stack Traces, application or server errors).
- HTTP 404 codes/pages or other HTTP non-200 codes/pages.
- Banner disclosure on common/public services.
- Disclosure of known public files or directories, (e.g. robots.txt).
- Clickjacking and issues only exploitable through clickjacking.
- CSRF on forms that are available to anonymous users (e.g. the contact form).
- Logout Cross-Site Request Forgery (logout CSRF).
- Presence of application or web browser 'autocomplete' or 'save password' functionality.
- Lack of Secure and HTTPOnly cookie flags.
- Lack of Security Speedbump when leaving the site.
- Weak Captcha / Captcha Bypass
- Username enumeration via Login Page error message
- Username enumeration via Forgot Password error message
- Login or Forgot Password page brute force and account lockout not enforced.
- OPTIONS / TRACE HTTP method enabled
- SSL Attacks such as BEAST, BREACH, Renegotiation attack
- SSL Forward secrecy not enabled
- SSL Insecure cipher suites
- Lack of SSL or Mixed content
- The Anti-MIME-Sniffing header X-Content-Type-Options
- Missing HTTP security headers, specifically https://www.veracode.com/blog/2014/03/guidelines-for-setting-security-headers
- Google Maps API Keys
- Account/e-mail enumeration using brute-force attacks
- Valid user account/email enumeration not requiring brute-force will be considered
- Any low impact issues related to session management (i.e. concurrent sessions, session expiration, password reset/change log out, etc.)
- Bypassing content restrictions in uploading a file without proving the file was received
- Clickjacking/UI redressing
- Client-side application/browser autocomplete or saved password/credentials
- Descriptive or verbose error pages without proof of exploitability or obtaining sensitive information
- Directory structure enumeration (unless the fact reveals exceptionally useful information)
- Incomplete or missing SPF/DMARC/DKIM records
- Issues related to password/credential strength, length, lockouts, or lack of brute-force/rate limiting protections
- Account compromises (especially admin) as a result of these issues will likely be considered VALID
- Leaking Session Cookies, User Credentials, or other sensitive data will be reviewed on a case by case basis
- If leaking of sensitive data requires MiTM positioning to exploit, it will be considered out of scope
- Login/Logout/Unauthenticated/Low-impact CSRF
- CSRF Vulnerabilities may be acceptable if they are of higher impact. Examples of low impact CSRF include: Add/Delete from Cart, Add/remove wishlist/favorites, Nonsevere preference options, etc.
- Low impact Information disclosures (including Software version disclosure)
- Missing Cookie flags
- Missing/Enabled HTTP Headers/Methods which do not lead directly to a security vulnerability
- Reflected file download attacks (RFD)

- Self-exploitation (i.e. password reset links or cookie reuse)
- SSL/TLS best practices that do not contain a fully functional proof of concept
- URL/Open Redirection
- Use of a known-vulnerable library which leads to a low-impact vulnerability (i.e. jQuery outdated version leads to low impact XSS)
- Valid bugs or best practice issues that are not directly related to the security posture of the client
- Vulnerabilities affecting users of outdated browsers, plugins or platforms
- Vulnerabilities that allow for the injection of arbitrary text without allowing for hyperlinks, HTML, or JavaScript code to be injected
- Vulnerabilities that require the user/victim to perform extremely unlikely actions (i.e. Self-XSS) Self-XSS for a Persistent/Stored XSS will be considered.
- Any type of XSS that requires a victim to press an unlikely key combination is NOT in scope (i.e. alt+shift+x for payload execution)

Additional specific vulnerability types considered out of scope due to low impact:

- IIS Tilde File and Directory Disclosure
- SSH Username Enumeration
- Wordpress Username Enumeration
- SSL Weak Ciphers/ POODLE / Heartbleed
- CSV Injection
- PHP Info
- Server-Status if it does not reveal sensitive information
- Snoop Info Disclosures

40. Appendix N. Complete PDF of this site

40.0.1 Full PDF

`Last Reviewed: 2025-02-17:19:44:43-UTC`

For convenience and off line viewing, we provide a full PDF of this site.