IT-003

Metropolitan Washington Airports Authority

INFORMATION SECURITY

DISTRIBUTION: All Employees

OPI: IT
DATE: February, 2018

FOREWORD

The Metropolitan Washington Airports Authority depends on the secure use of information technology, and the effective management, operation and delivery of these services to meet the Airports Authority's mission. To ensure protection of our critical information technology resources and minimize the risk from threats, we are issuing this revised Directive with updated, more secure, policies and procedures. This Directive supersedes all previous versions of information technology policies.

These new security standards are stronger to keep pace with ever-increasing cybersecurity risks. Effectively implementing security within any organization is a team effort in which everyone has a vital role to play. Each employee shares in the responsibility for securing and protecting our facilities and information technology assets. Everyone must remain vigilant at all times to safeguard the Airports Authority's mission.

The Directive's Rules of Behavior define the minimum standards of security behavior required of all users, including password rules and personal use restrictions. It only takes one oversight or failure by a single person to place critical systems and information at risk. Consequently, users are the front line of our defense, and they are expected to know and comply with this Directive as well as all other applicable laws and regulations governing information technology security.

The Directive applies to the entire Airports Authority and all bodies that operate within its facilities. It also applies to all contractors, collaborators and third parties that connect to, operate with or exchange data with the Airports Authority's technology infrastructure. New mandatory training is being introduced to make sure everyone is familiar with these updated policies and procedures. The Directive will be available for reference on the Airports Authority intranet.

Thank you for your help with this crucial responsibility of keeping our critical information and systems secure.

John E. Potter
President and Chief Executive Officer

2/22/18
Date

Contents

Background

To remain consistent with the Metropolitan Washington Airports Authority corporate strategy, the shared technology approach to modernizing information technology across the Airports Authority began in 2013. As a part of aligning technology to corporate strategy, groups were consolidated, technology was insourced, a consolidated Data Center was implemented, a common communication network was initiated, and wireless communication and digital innovation platforms were introduced. This common corporate strategy consists of the standardization, consolidation and consistent method of approach to all technology hardware, software, network communication systems, wireless communication and digital innovation platforms, and associated support services across the Airports Authority.

This approach ensures sustainable excellence by creating a stable core system of operations and a modernized technology infrastructure that can support the implementation of next generation technologies in a timely, efficient manner. Moreover, this shared technology approach will enable the Airports Authority to reduce its technology footprint, ease interoperability between various systems, enhance cybersecurity, reduce operational costs and provide efficient operation.

Purpose

This Directive sets forth the Airports Authority policy, procedures, roles and responsibilities regarding Information Security implementation across all aspects of the enterprise. This Directive applies to both Information Technology and Operational Technology systems.

Distribution

This Directive is distributed to all employees and contractors at the Ronald Reagan Washington National Airport, the Washington Dulles International Airport, the Dulles Toll Road and the Rail Office.

Scope

This Directive applies to the entire Airports Authority and all operating bodies within its facilities. All departments, programs, and projects engaged in the evaluation, selection, acquisition, implementation, maintenance and/or operation of new, refresh and/or upgraded technology must follow and fully comply with this Directive. It also applies to all contractors, collaborators, and third parties with technologies engaged, connecting to, interoperating with, and/or exchanging data with the Airports Authority technology infrastructure.

For all aspects of Information Security applied within Airports Authority jurisdiction, this Directive holds the final deposition and supersedes others, if any. It applies to all past, developmental and future technology efforts. Any existing arrangement that does not comply with this Directive will have to plan necessary activities, timelines and waiver requests where applicable to successfully incorporate the security processes and requirements specified in this Directive. Ongoing implementations may have to adjust to successfully comply with this Directive.

Common Information Security Approach

The goal of this Directive is to create a consistent, documented, common security approach across the Airports Authority. Via this Directive, the Airports Authority formally has adopted the National Institute of Science and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity as its official security framework (The Framework). This Framework is a risk-based approach to cybersecurity and was developed with critical infrastructure in mind. The Framework incorporates best practices from both federal organizations (National Institute of Science and Technology (NIST) and private sector organizations (Center for Internet Security (CIS), Open Web Application Security Project (OWASP), Control Objectives for Information and Related Technologies (COBIT), International Standards Organization (ISO) and International Society of Automation (ISA). Information Security is an ever-evolving field with continuously changing standards. As a result, the standards will be updated as needed to support the Airports Authority's risk management and cybersecurity needs. In cases where a standard does not provide guidance, contact the Office of Technology's Information Security.

Roles and Responsibilities

Effectively implementing security within any organization is a team effort where everyone has a vital role to play. Clearly defining and explaining who has what strategic role, responsibilities and accountability in the organization is critical to success.
Everyone shares joint responsibility in securing and protecting our facilities and Information and Operational Technology (assets). Consequently, everyone must remain vigilant at all times to safeguard the secure delivery of the Airports Authority's mission. This section defines who is responsible for security activities in support of the Airports Authority's mission and what security activities must be completed to mitigate risk across the organization.

All Users
Users act as the front line of the Airports Authority's Information Security defenses. As such, users must recognize their responsibilities and remain constantly vigilant to protect the Airports Authority's networks and assets whenever possible. The Information Security Rules of Behavior specifies the security behavior (e.g., passwords, personal use rules, etc., expected of ALL users without exception).

Users are individuals who have been granted access to the Airports Authority's assets to perform assigned duties. Users may include, but are not limited to, employees, vendors, volunteers, or other affiliates of the Airports Authority. All users are responsible for protecting the Airports Authority's information from unauthorized disclosure, modification, deletion and usage. Users will comply with all requirements in the Rules of Behavior in this Directive, any other applicable laws, and regulations. Users will report sensitive security issues, misuse, and violations of this Directive to their supervisor or the Chief Information Security Officer (CISO) as quickly as possible.

The Rules of Behavior will be reviewed and accepted by all users employed by or conducting work on behalf of the Airports Authority before they are granted an account on the Airports Authority's network. Users are required to review and accept the Rules of Behavior on an annual basis to retain their Airports Authority network access.

Some Users, based on their position in the Airports Authority or their job function may have additional roles. These additional roles are defined below.

President and Chief Executive Officer (CEO)
The CEO bears ultimate accountability and responsibility for risks to the Airports Authority, including cybersecurity risks to informational and operational assets wherever those systems may reside. As such, the CEO is responsible for ensuring that all Airports Authority departments comply with this Directive.

Executives
Executives are responsible for the effective delivery of their respective portions of the overall Airports Authority mission. Executives who have managerial and financial accountability for the data within an information or operational system will work with the CISO to determine the sensitivity of the data to ensure appropriate security controls are implemented.

Executives will ensure that staff are assigned and participate in those security activities required to assure the security controls are working. These include but are not limited to periodically verifying User access to applications and participating in Business Impact Assessments and Disaster Recovery Exercises. Executives are also required to ensure their staffs comply with the Rules of Behavior.

All systems and applications used within the Airports Authority or external systems hosting Airports Authority data are required to be security certified prior to use and at least once annually thereafter until they are no longer in use. For systems that do not pass the security certification process, executives will be required to formally accept the security risks identified before these systems are authorized for use.

Chief Information Officer (CIO)
The Airports Authority's CIO is responsible for ensuring the successful operation, security and availability of the Airport Authority's network and all systems operating on it or connected to it.

For enterprise systems providing all mission/business services (authentication systems, email, etc.) the CIO retains responsibility and accountability for the data security of those systems. The CIO also will assume data security responsibility where managerial and financial accountability has not been explicitly defined.

Chief Information Security Officer (CISO)
The CISO is responsible for developing, implementing, and administering the Airports Authority's Information Security program, and reporting security risks, incidents, and vulnerabilities to the CIO and Executives.

The CISO is accountable for the development and implementation of the Directive for information systems security management activities, and has jurisdiction over security related events, functions, vulnerabilities and threats. The CISO may execute authority to remove any content or system from the Airports Authority's networks, Internet/Intranet sites, servers, or workstations. The CISO has authority to disable any account and/or confiscate equipment when inappropriate or malicious activity has been discovered during an investigation of a security incident.

The CISO is the internal and external point of contact for all information security matters, incidents and concerns. The CISO will support, review and approve updates to this Directive and other security guidance documents as needed.

Contracting Officer (CO)
Contracting officers (COs) play a critical role in supporting the security goals of the organization. Contracts in which Airports Authority owned information will be shared with, hosted or maintained by a contractor require security certification by the CISO. For those contracts, COs must ensure that appropriate contract language, approved by the CISO, is included in the solicitation documents.

Contracting Officer Technical Representative (COTR)
COTRs play an essential role in supporting the security goals of the organization by ensuring Airports Authority owned assets entrusted to contractors are protected in accordance with the information security terms of the contract.

COTRs must provide contractors with a copy of the Rules of Behavior prior to the contactor's access to the Airports Authority assets. COTRs must ensure contractor access is removed on the last day of their services. If the contract period of performance is greater than one year, the contractor access must be validated on an annual basis.

Technical Staff
Technical staff includes the Office of Technology or other personnel (contractors, vendors, etc.) who manage assets for the Airports Authority. Technical staffs are typically in control of the Airports Authority's assets and are the custodians or guardians. Technical staff plays a critical role in implementing the protection requirements defined by this Directive. They are responsible for maintaining the security measures defined in the standards. Technical staff members must be familiar with all standards of this Directive that are applicable to the system function(s) or role(s) they perform.

Information Security Group (ISG)
The Information Security group (ISG), under the direction of the CISO, is responsible for the information security-related affairs of the Airports Authority.

In order to manage systems and enforce security, the ISG will log, review, and otherwise utilize any information stored on or passing through Airports Authority assets and systems. This includes, but is not limited to electronic data that is created, hosted, managed, transmitted, received, or stored on assets owned, leased, administered, hosted by another entity, or otherwise under the custody and control of the Airports Authority.

The ISG will develop, promulgate and manage an organizational security architecture, with inputs from relevant groups. The ISG also ensures that controls among subsystems, including monitoring and communications, meet or exceed minimum standards.

The ISG will develop and provide security awareness training for all Airports Authority Users and contractors. Training will be required within 90 days of being provided authorized access to the information system. Training is required annually thereafter.

The ISG will facilitate information sharing of Airports Authority information with external partners. The ISG also will determine the types of automated mechanisms or processes needed to best facilitate this information sharing.

The ISG will determine which information systems require specialized access agreements based on sensitivity of the data in the system and overall potential risk to the organization. Where a specialized access agreement is required, the ISG will work with the relevant personnel to:

- Develop and document access agreements for organizational information systems
- Review and update as necessary the access agreements at least annually
- Ensure that individuals requiring access to organizational information sign appropriate access agreements prior to being granted access. Access agreements will be re-signed on at least an annual basis or after they have been updated.

Compliance and Violations

This Directive is the benchmark for information security safeguards. All Airports Authority assets whether managed internally or externally must comply with the requirements of this Directive. All activity from the Airports Authority assets is subject to monitoring by authorized staff to ensure system integrity and compliance with the Directive. Assets not in compliance with the Directive may be subject to being disabled or removed by the ISG, if determined to pose an unacceptable risk or threat to the Airports Authority.

Users must understand their roles and responsibilities regarding information security issues and protecting information as set forth in the Directive. Failure to comply with the Directive may result in disciplinary action as outlined in the *Airports Authority Conduct and Discipline Directive*, HR-003A.

Contractors and subcontractors who fail to comply with the requirements of this Directive may face termination of their access to Airports Authority assets, removal from the contract, termination of the Airports Authority-related consulting agreement, termination of other active Authority consulting agreements and/or potential disbarment from doing future business with the Airports Authority. Penalties will depend on the severity of the failure and its impact on the Airports Authority's assets.

Rules of Behavior

Acceptable Use

Users of Airports Authority assets are expected to abide by the content specified in these Rules of Behavior, regardless of whether a particular Airports Authority asset is located internally or externally, such as in a cloud infrastructure or similar off-site hosted system.

Assets and capabilities are provided to users for the facilitation of Airports Authority business and are explicitly owned by the Airports Authority. The Airports Authority owns all property rights for any content or other material created, received, transmitted, stored on, or deleted from any Airports Authority information system.

General

Users will respect the confidentiality and integrity of all Airports Authority assets, familiarize themselves with the Airports Authority Information System Security Directive, and report any security weaknesses or breaches immediately to the ISG.

Users will respect security controls for Airports Authority assets and not attempt to circumvent those controls. Users will not access or attempt to access any Airports Authority assets which they have not been granted authorization to access.

Users must treat passwords and other access credentials as private and highly confidential. Sharing of credentials is strictly prohibited. Users are required to change their passwords every ninety (90) days. Users will take reasonable steps to prevent the disclosure of their passwords, security tokens, or similar information to unauthorized users.

Users will refrain from activities that may intentionally or inadvertently disrupt, impair, or undermine the performance of Airports Authority assets. These activities include, but are not limited to, the following:

- Intentionally causing any type of damage to Airports Authority-owned assets.
- Intentionally downloading or introducing computer viruses, malware or malicious code to an Airports Authority asset.
- Using tools, devices or other actions that bypass security mechanisms.
- Downloading, installing, or running security utilities or tools (e.g., password cracking programs, network discovery, etc.) without prior written approval from the ISG.
- Sending chain letters, unsolicited mass emails, gambling site information or pornography.
- Divulging to unauthorized persons any details regarding Airports Authority assets or architecture unless previously authorized.

Restricted and confidential data must not be stored on any laptops, mobile devices, or removable media such as USB, CD, DVD, without prior approval. Restricted and confidential data stored on these devices must be encrypted.

Users will not use cloud or Internet-based hosting services to store or share Airports Authority data unless specifically approved and acquired through the information technology office. Users should take such steps to log off or terminate connections to Airports Authority assets at the end of every workday. At a minimum, Users must lock devices when they are left unattended.

Users of Airports Authority-approved mobile communications devices will ensure that precautions are taken to prevent theft or loss. Airports Authority mobile devices will be physically secured when left unattended. Users must immediately report any loss or theft of a mobile device containing any Airports Authority information. In the event of a lost or stolen device (Airports Authority- owned or personally-owned) that contains Airports Authority information, Users will immediately report the loss. The Airports Authority reserves the right to clear its information from the device by any available technical means.

It is highly recommended that users not download and store sensitive system data to their workstations. User and contractor endpoint devices and workstations are not backed up. In the event a user downloads Airports Authority data to their endpoint or workstation, they become responsible for protection of the data downloaded and Data Custodians for that information. Responsibilities related to this activity include ensuring that system data is not

shared with unauthorized individuals or sent via the network, such as by email to unauthorized individuals. Sensitive system data, if printed, must not be left accessible to unauthorized individuals and should be carried by the User or secured in a locked cabinet or drawer when not in use.

Users and contractors must never back up Airports Authority data to any portable devices without prior approval. Also, users and contractors must never back up Authority data to any cloud infrastructure without prior approval.

Ownership

Airports Authority assets are the property of the Airports Authority and intended for official Airports Authority business use only. The Airports Authority retains property rights to all information created, generated, replicated, processed, stored, transmitted, and received by users in the course of using its assets.

Privacy

Users of any Airports Authority assets will not have any expectation of privacy in any message, file, image, or data created, sent, retrieved, or received.

All user activity on any Airports Authority information system is subject to monitoring, logging, auditing, review, dissemination and archiving by the information technology office. Internet traffic over Airports Authority assets will be inspected for malicious code or inappropriate content prior to delivery to the user. Internet activity will be monitored for violations of acceptable use, as well as any other applicable laws, regulations, or Airports Authority policies and procedures.

User's personal information should not be stored on Airports Authority assets and is done at the user's risk. Such information also may be subject to disclosure or review by Airports Authority officials.

Use of Portable Devices

Removable media is one of the easiest ways to compromise systems. As such, security controls to reduce risks around the use of these devices is crucial to the success of information security.

The Airports Authority only allows registered and approved removable media, vetted by the ISG, to be connected to Airports Authority information systems. If a User believes there is a legitimate business need to utilize such removable media, the User must contact the Helpdesk to make the request.

Personnel with ISG-approved removable media are responsible for physically controlling and securely storing such approved media at all times, and protecting such approved information system media until the media is sanitized and/or destroyed using approved equipment, techniques, and procedures.

Users immediately must report to any loss or theft of any portable device containing any Airports Authority information.

Incidental Personal Use

Personal use is the utilization of Airports Authority assets for purposes not related to conducting the business of the Airports Authority. In general, incidental personal use of the Airports Authority's assets, such as Internet access and email, is permitted, unless it:

- Interferes with the productivity or work performance of the User or other users
- Adversely affects the efficient operation of any assets or the Airports Authority's effectiveness in conducting its business objectives and mission

Prohibited Use

Certain activities are prohibited when using Airports Authority assets. These prohibited activities include, but are not limited to:

- Accessing, downloading, transmitting, printing, or storing information with sexually explicit content.
- Downloading or transmitting fraudulent, threatening, obscene, pornographic, intimidating, defamatory, violent, harassing, or discriminatory messages or images.

- Accessing any gambling sites.
- Pursuing personal profit or gain or engaging in outside employment or personal business, unauthorized fundraising or political activities.
- Unauthorized downloading, printing, or transmitting of information protected by federal or state copyright laws.
- Misusing or misapplying Airports Authority information access privileges.
- Using software in violation of Airports Authority vendor licensing agreements.

Personal Devices

Personally-owned devices will not be connected to Airports Authority assets or used to store Airports Authority information without prior approval. A User must sign a Smartphone Waiver Form to be authorized to use his or her personally-owned mobile communications device(s) to access any Airports Authority asset.

Access privileges to Airports Authority assets through a personally-owned mobile device will be terminated upon the user's separation from the Airports Authority or for any other reason deemed necessary to protect the Airports Authority.

Any Airports Authority data stored on a user's personal device is the property of the Airports Authority.

Remote Access

Remote access to Airports Authority assets only will be permissible through Airports Authority-provided and supported remote access software or services. Remote access will be provided after a determination has been made that access is required to perform assigned duties, or the User is defined as essential personnel by the Airports Authority. Users with remote access will ensure they connect to the Airports Authority from legitimately secure networks, such as a personally-owned home network or other validated network, and that the device used maintains basic security controls (e.g. anti-virus software) to prevent unauthorized access to all Airports Authority assets. Remote copying, moving, or storing of sensitive data to local hard drives, or other electronic media without prior ISG approval is strictly prohibited.

Awareness Training

Users with access to the Airports Authority's information system must undergo Security Awareness training on an annual basis. New Users must complete the security awareness training within 90 days of being granted access to any Airports Authority's assets. Users will acknowledge in writing or electronically that they have read and understood this Directive.

Security Certification

Security certification is necessary to ensure safeguards are in place or risks fully understood prior to Airports Authority use. All connections to the Airports Authority networks or hosts must be certified by the Airports CISO in writing prior to authorization for use. This includes, but is not limited to, all hardware and applications, whether hosted on Airports Authority property or in the Cloud, or managed by Airports Authority staff or external contractors.

Two methods will be used to certify systems for Airports Authority use:

- The most current version of the Statement on Standards for Attestation Engagements (SSAE) or
- Certification by the Office of Technology's ISG against the Security Directive Standards

Statement on Standards for Attestation Engagements

This standard is issued by the American Institute of Certified Public Accounts and has two types of reports: Type I and Type II. A Type II report identifies the type of security controls in place by the entity, and it is the report required to be certified using SSAE.

The Type II report must be provided to the ISG for review before contracts are finalized. The CISO will provide a certification for the system if the report satisfies the objectives of this Directive and there are no deficiencies or risks to the Airports Authority. Type II reports are issued for a fixed time period. To be certified, they must be current

Certification by the Office of Technology's ISG.

Using the standards of this Directive, a security assessment will be conducted to determine the security posture of the system and risks to Airports Authority. Upon conclusion of the assessment, a certification for the system will be provided by the CISO if it meets the standards of this Directive.

Failure to certify

If an entity fails the certification process, the risks identified will be provided to the requestor for mitigation. If the risks cannot be mitigated and a decision to continue with the implementation and/or use of the system is made, then a System Security Risk Acceptance Form must be completed. The form must be signed by the executive responsible for the system. Additionally the system must be isolated from all other Airports Authority systems.

The Security Certification process can be reviewed in more detail by clicking here.

Security Standards

The following standards provide the security requirements to be implemented across the Airports Authority to achieve a common security framework. Details related to each standard can be found by clicking the links below:

- Asset Management
- Risk Management
- Supply Chain Risk Management
- Identity Management and Access Controls
- Data Security
- Awareness and Training
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology
- Event Management
- Security Continuous Monitoring
- Detection Processes
- Response Planning
- Recovery Planning