



WMATA Information Technology

WMATA IT Security Standards and Guidelines

Office of Chief Information Security Officer

**Standards Description Document
IT-MITS-STND-01**

Version 1.0

Revision History

Version	Date	Subject Matter Expert	Author/Editor	Description
0.1	05/19/2017	Tijan Drammeh	Tijan Drammeh	Initial draft
0.2	06/14/2017	Tijan Drammeh	Tijan Drammeh	Comments from MITS management and Al Short, Deputy CIO incorporated.
1.0	06/20/2017	Tijan Drammeh	Tijan Drammeh	Final copy – All additional notes finalized.

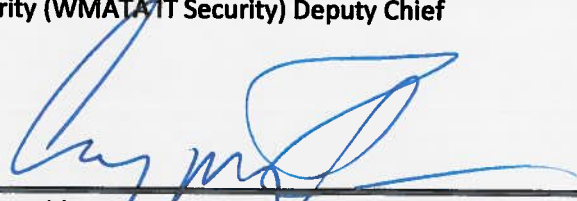
Standard and Guideline Document Authorization

The undersigned have reviewed this process definition document and hereby authorize its implementation as herein described.



7/14/2017

Tijan Drammeh, WMATA Information Technology Security (WMATA IT Security) Deputy Chief POC Date:



07/14/17

Corey Bobb, WMATA Information Technology Security (WMATA IT Security) Chief Owner Date:



14 July 2017

Al Short, WMATA Information Technology Deputy Chief Information Officer Approver Date:

Table of Contents

Revision History	i
Standard and Guideline Document Authorization	ii
1 Introduction	4
1.1 Scope.....	4
2 Information Security Standards	4
2.1 Risk Management.....	4
2.2 Information Security.....	4
2.3 Application Systems Implementation and Maintenance.....	8
2.4 Database Implementation and Support.....	9
2.5 Network Support and Management.....	11
2.6 Cloud Computing.....	14
2.7 Disaster Recovery Planning.....	15
2.8 Information Resource Strategy and Planning.....	16
2.9 Information Systems Operations.....	17
3 Guidelines and Tools	24
3.1 Guidelines.....	24
3.2 Tools.....	24
3.3 Training Requirements.....	24
4 References	25

1 Introduction

The Washington Metropolitan Area Transit Authority (WMATA) policies and procedures provide a framework that establishes data security, availability and integrity of the WMATA data and its operations. It is very important for all business units and IT to follow the WMATA policies and procedures as it ensures business operations on IT systems and also, guides on implementation of new projects and upgrades of existing solution.

1.1 Scope

The purpose of this document is to provide guidance to incoming or existing vendors on the procurement, upgrade and decommissioning of information technology systems, including hardware and software. Also, this document guides and lays out the framework existing and desired not only from the business owners but also, from vendors and contracting staff. All the proposed solutions and enhancements must follow the framework set by WMATA Information Technology office and any exceptions to this document must be presented to WMATA IT Security before procurement or designing solution.

This document can be used as guidance document along with request for proposal from business units.

2 Information Security Standards

The Washington Metropolitan Area Transit Authority (WMATA) Information technology standards are communicated via set of policies and procedures. These standards and guidelines are very important for WMATA and should be followed while doing any project or system upgrades which involve WMATA information systems.

2.1 Risk Management

Ensure that IT risk management is an integral part of the Authority's defined risk management process. WMATA IT Security should be involved in performing risk assessment on all the new proposed projects or existing information systems. WMATA IT Security department performs risk assessments on existing services and systems supporting the business goals as directed by the CIO. IT Risk management activities should include:

- i. Integrate risk identification, analysis, and mitigation activities into product development planning.
- ii. Define risk management processes at the beginning of project as initial step.
- iii. Raising awareness in the WMATA for the need of risk management.
- iv. Invoking the established Risk Management process to systematically assess risks.
- v. Minimize loss, disruption, damage and injury and reduce the cost of risk.
- vi. Inform policy and decision making by identifying, assessing and remediating impact to acceptable levels.

2.2 Information Security

2.2.1 User Access Management

- 2.2.1.1 Access to systems and network will require a valid user ID and password. All default and vendor-supplied user IDs and passwords will be disabled and removed. Minimum password length and security standards will be enforced by WMATA IT Security.

2.2.1.2 Two factor or additional authentication based upon risk assessment or sensitivity of system and/or data. Systems will be evaluated by OCISO and additional authentication guidance and requirement will be provided.

2.2.1.3 New devices will be identified and entered in system for records before going in production. Also, new devices will be hardened according to security posture defined by WMATA IT Security.

2.2.2 Access Control

2.2.2.1 Physical access to network servers, communication lines and other network hardware components will be controlled and restricted to those with a demonstrated need for access.

2.2.2.2 Access rights to information resources are granted to network administrators with elevated levels of access. These rights are granted for the purpose of providing support, troubleshooting and performing maintenance on WMATA equipment for customers. Data is not to be accessed, printed, modified or copied (except for routine backups) for any reason, unless prior written consent is given by the data owner.

2.2.2.3 Centrally controlled network servers should be used instead of sharing workstation resources to prevent access to sensitive data.

2.2.2.4 Remote access will be provided to individuals who demonstrate a clear business need for such access through an approved, standard methodology.

2.2.2.5 The use of remote control software is restricted to specific situations which must be justified and approved by the WMATA Chief Information Security Officer (CISO).

2.2.3 Payment Card Industry Data Security Standard (PCI DSS)

All the systems integrating with WMATA Credit card processing system or proposed to process credit/debit card payments must comply with PCI DSS latest standard posted on PCI council website.

2.2.4 IT Security Training

2.2.4.1 All users, managers and operators of WMATA information systems will receive and complete recurring IT Security Awareness training annually.

2.2.4.2 All users involved in development of software or custom development on an application should go through secure code development techniques training.

2.2.5 Vulnerability Management

All WMATA systems must follow vulnerability management process by OCISO. Vulnerability management overall supports the IT risk management program and security posture of IT environment. Systems supporting WMATA services and business process must have security implementation plan (SIP). Review cycle of SIP should be defined by OCISO. Review of SIP will be needed in case system goes through major upgrade. Compensatory controls should be placed to bring systems in compliance and a sign off will be required by the CIO and CISO for systems that do not meet WMATA defined standards and guidelines.

2.2.5.1 System Patching and Hardening

- i. All system devices belonging to, or managed by WMATA will be patched with vendor-provided operating system and application security patches.
- ii. All systems will be hardened utilizing industry best practices benchmarks. The Center for Internet Security (CIS) (<http://www.cisecurity.org>) will be the primary library of benchmarks for system hardening within WMATA. If a benchmark is not available for a particular system environment such as a Platform IT system, WMATA IT Security will collaborate with the system owner to select the most appropriate guidelines for their environment.
- iii. All systems will have the latest service packs and security patches installed per the approved maintenance cycle.
- iv. All systems will have the latest anti-virus software installed.
- v. New devices will be patched to the current patch level, as well as hardened to appropriate benchmarks prior to the device being connected to WMATA's network.
- vi. Patches will be applied:
 - a. By automated patch management software on workstations connected to the WMATA network; and
 - b. By automation and manually (where applicable) to all systems in accordance with an approved system maintenance plan.

2.2.5.2 Network Removal

Older devices with outdated operating systems or non-supported vendor operating systems that do not have the ability to use current operating system software will be removed from WMATA's network, unless the system owner requests and is granted an exception by WMATA CISO. Devices with non-supported vendor applications should be informed and reviewed by WMATA IT Security.

2.2.5.3 Monitoring

For security and network maintenance purposes, authorized individuals within WMATA may monitor equipment, systems and network traffic at any time. WMATA IT Security reserves the right to audit networks and systems to ensure compliance.

2.2.5.4 Sustainability and Supportability

Sustainability and supportability is a combination of preventative, corrective and reliability centered maintenance. Systems owners need to ensure that during program/project planning systems should have a sustainment and support plan in place that accounts for the total cost of ownership for vulnerability management in regards to:

- i. Labor and costs associated with vulnerability management are clear;
- ii. Maintenance windows are defined and repeatable; and
- iii. Vendor lifecycles are understood and sunset milestones are identified in order to plan for future technical refresh.

2.2.5.5 Also, system owners should ensure that vendor support plan includes timely delivery of system security and patch updates. Endpoint Monitoring

- i. Software to detect and clean viruses and malicious code will be installed on all WMATA stand-alone and networked information systems.

- ii. WMATA will use an IT Security approved product for protection from malicious code under the following minimum requirements:
 - a. The malicious code protection product will be configured for, and operated in real time to protect all servers and client computers;
 - b. The library definitions will be updated at least once per day; and
 - c. Scans will be done at a minimum of once per month on all user-controlled workstations and servers.
 - d. All media (disks, thumb drives, CDs, etc.) from an outside source or exchanged with another employee will be automatically scanned by WMATA systems for viruses and other malicious code when inserted before use.

2.2.6 Virus Protection

- 2.2.6.1 WMATA will subscribe to a virus notification service. Virus updates will be centralized and distributed at the discretion of WMATA IT Security, who will also alert users of risks, threats and required actions.
- 2.2.6.2 Virus protection must be installed at all entry points to WMATA networks, and scanners will be updated at a reasonable schedule. These scanners will scan incoming mail and files received from across a network. Additional virus checking will occur at various access points.
- 2.2.6.3 All software is to be installed in an isolated environment and tested for viruses prior to being placed in a networked environment. When certified to be virus free, it may be moved into the normal operating environment using the appropriate procedures.
- 2.2.6.4 Security team will maintain set of approved software.

2.2.7 System Audit Trail and Logging

- 2.2.7.1 All mission-critical servers (e.g., file, web, email, etc.) must be configured to securely and automatically log all significant security relevant events and sent to WMATA IT Security central logging system
- 2.2.7.2 Successful and unsuccessful login attempts by users will be captured and stored.
- 2.2.7.3 All logs must be secured so that they cannot be modified, and so that only authorized persons can read them.
- 2.2.7.4 Records reflecting security-relevant events must be periodically reviewed in a timely manner by computer operations staff, information security staff or systems administration staff. Alerts will be set on the central logging and file integrity system for various WMATA audits.
- 2.2.7.5 Records will be retained for the length of time as required for their applicable regulatory and statutory compliance. Records containing possible security and/or legal incident information will be retained longer at the discretion of WMATA IT Security or until such time as it is determined that WMATA will not pursue legal action or otherwise use the information.

2.2.8 Network and System Privacy and Monitoring

- 2.2.8.1 Unless contractual agreements dictate otherwise, all forms of communications sent over the WMATA WAN are the property of WMATA.

- 2.2.8.2 Information technology department reserves the right to examine all data stored in or transmitted by all computer systems owned and operated by WMATA.
- 2.2.8.3 Employees, contractors and vendors must have no expectation of privacy associated with the information they store in or send through WMATA information systems.
- 2.2.8.4 A successful system logon is an agreement to abide by all policies for system use.
- 2.2.8.5 No responsibility is assumed for the disclosure of information sent over WMATA WAN networks, and no assurances are made about the privacy of information handled by WMATA internal networks.
- 2.2.8.6 Nothing in this document will be construed to imply that WMATA policy does not support the controls dictated by agreements with third parties, such as organizations that have entrusted WMATA with confidential information.

2.3 Application Systems Implementation and Maintenance

All the development and configuration management should follow Software Development Life Cycle (SDLC) methodology. Incorporate information security throughout the software-development life cycle. Applications or systems which are subject to government regulations or industry standards must incorporate the security controls as listed in the regulations or industry security standards. Written software-development processes should exist and these processes must be based on industry standards, regulations and/or best practices.

Application systems should use WMATA central repository/tool for management of configuration and software development code libraries. Following areas should be addressed for application systems besides guidelines listed in this document:

2.3.1 Change management

All the changes to the application system should follow WMATA IT Change management process.

2.3.2 Segregation of environments and personnel

Development, test and production environments should be created for SDLC. Clear segregation of duties should be established between personnel for various phases of SDLC and enforce the separation with access controls. Production data should not be used for testing or development. Separate code libraries should be used for each environment via WMATA provided tools or industry standards tools. Any tool other than WMATA approved tool must be approved by OCISO.

2.3.3 Secure coding and review

Secure coding techniques should be used in the development of new systems or enhancement of the systems. OWASP top 10 and WMATA OCISO approved development processes should be used.

2.3.4 Patch management

Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Security patches should be installed within reasonable timeframe of release. Critical security patches should be installed within one month of release.

2.3.5 Application vulnerability management

Application vulnerability scans must be performed and all the vulnerabilities listed as high and medium must be remediated before implementing to the production environment.

2.4 Database Implementation and Support

All the databases should be located in an internal network zone as designated by WMATA IT Security. Use WMATA IT security configuration standards for all database components. WMATA IT Security follows industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: Center for Internet Security (CIS); International Organization for Standardization (ISO); SysAdmin Audit Network Security (SANS) Institute; National Institute of Standards Technology (NIST). All the guidelines listed in this document should be followed for data protection, availability and integrity.

2.4.1 Data Sensitivity

- 2.4.1.1 Sensitivity levels are assigned to data in WMATA's databases, applications and systems and stored in electronic media are based on the data's value to WMATA, its employees and customers. Threats to the data include anything that could affect the confidentiality, integrity and availability of the information. Sensitivity levels of confidential, internal use only and Public are defined, and data owners must assign all data under their control to one of these levels based on the data's value and its ability to provide services to its customers.
- 2.4.1.2 Collection and Storage of Personally Identifiable Information should only occur when it is essential to the functions and operations of WMATA. Storage of personally identifiable information should remain only in the information system's data base and not in ancillary storage areas (e.g., spreadsheets or other types of files).
- 2.4.1.3 Access to Personally Identifiable Information will be authorized by persons known as "data owners" or "authorizing agents" for a WMATA application system in support of necessary functions or operations.
 - i. Access to personally identifiable information is granted based on a "need-to-know" and/or "least-privilege" principle. Therefore, WMATA personnel shall only access information that they are specifically required to use in the performance of their duties.
 - ii. Access to sensitive information (both personally identifiable and confidential business information) will be revoked immediately on an employee's last day of employment or change in the employee role/responsibilities or upon the data owner/authorizing agent/Assistant General Manager's notification to WMATA IT Security of an employer-initiated termination of previously-granted access.
- 2.4.1.4 Transmission of Sensitive Information requires the sender to protect that information and inform the recipient(s) (including those involved in the delivery process) that the transmission contains sensitive information and must be protected.
 - i. Security of Paper Transmissions requires the sender to seal the envelope, mark the envelope as "CONFIDENTIAL" and take all necessary steps, as appropriate, to ensure delivery only to the correct party/parties to minimize the chance of unnecessary exposure.
 - ii. Security of Digital Transmissions requires the information be encrypted when being transmitted over public networks or carriers in digital form. WMATA IT

Security encryption standards should be used while transmitting sensitive information.

- iii. Security of Fax Transmissions requires the sender to ensure that the information is promptly retrieved and properly protected at both the sending and receiving locations, with appropriate telephone/email confirmation as appropriate.
- iv. Emailing of Sensitive Information is strongly discouraged..

2.4.1.5 Use and Storage of Sensitive Information

- i. The Assistant General Manager (AGM) of the department that is the owner or custodian of the data that may contain sensitive information maintains the responsibility for requesting that this data be scanned by WMATA IT Security for detection of sensitive information and compliance prior to internal or external posting.
- ii. Personally identifiable information and credit card information should be stored only where it is specifically required and in as few systems as possible. This data must be encrypted using WMATA IT Security-approved methods while in transit and at rest.
- iii. Systems on which sensitive information is stored must minimally comply with all basic computer security standards (e.g., patch management, anti-virus protection, password controls, etc.) Unencrypted sensitive information should be stored only on systems that are housed in secure and controlled environments. Where desktop systems access sensitive information, they must not be left logged in on an unattended basis or be available for casual perusal by unauthorized individuals.
- iv. Sensitive information stored on any system or media that is subject to loss or theft (including laptops, Universal Serial Bus (USB) drives, diskettes, CD/DVDs, personal computers and departmental servers) must be encrypted whenever not in use. Systems susceptible to theft should be physically secured.
- v. Whenever possible, sensitive data should be de-coupled from all personally identifiable information.
- vi. Paper documents and files containing sensitive information must be secured at all times. Such documents should not be left in open view on desks and when not in use must be stored in secured areas or locked files with access limited to authorized users.

2.4.1.6 Destruction of Sensitive Information

- i. Electronic and magnetic media (e.g., hard drives, diskettes, magnetic tapes and optical tapes) should be erased using secure deletion tools before transfer or disposal.
- ii. Media that are not or cannot be securely erased (e.g., USB drives, CDs, and DVDs) should be physically destroyed before disposal.
- iii. Paper documents and printouts containing sensitive information must be shredded before disposal.

2.4.1.7 Notice and Reporting of Security Breaches

In the event of a potential leak of sensitive information, WMATA IT Security should be notified immediately by the department/office that suspects a leak has occurred. In addition, the Office of the Inspector General and/other appropriate offices - including the Office of the Deputy General Manager, General Counsel, Department of System

Safety and Environmental Management, as well as the department where data originated from should also be notified.

2.5 Network Support and Management

2.5.1 WMATA Time Synchronization

Departments requiring the use of the centralized timing service will:

- 2.5.1.1 Request IT Network Communication Services (IT/NCS) approval on all end system timing device purchases to ensure compliance and conformity to the Time Synchronization System.
- 2.5.1.2 Work with IT/NCS for proper installation, configuration and activation of all end system timing devices.

2.5.2 Network Device Management

- 2.5.2.1 All devices (including routers, switches, appliances, servers and personal computers) must receive explicit connectivity approval from WMATA IT Security before being connected to the WMATA WAN.
- 2.5.2.2 WMATA IT Security must have root or admin-equivalent access to all devices on the network.
- 2.5.2.3 All network devices attached or to be attached to the WMATA WAN will be managed exclusively by NCS and IT Security. MOU must be in place before connecting the network devices to WMATA WAN

2.5.3 Addressing Requirements

- 2.5.3.1 All connected devices are limited to the use of WMATA IT Security-approved transmission protocols only.
- 2.5.3.2 All computers will be assigned IP addresses dynamically through a Dynamic Host Configuration Protocol (DHCP) server, and all other devices are assigned static IP addresses issued and maintained by WMATA IT Security.

2.5.4 Third Party and External Connectivity

- 2.5.4.1 All ingress connections into WMATA with non-WMATA networks must terminate at the Extranet for dedicated leased lines.
- 2.5.4.2 All external connectivity requests will be evaluated, implemented and managed by WMATA IT Security.
- 2.5.4.3 WMATA IT Security will validate all such connections on a quarterly basis.
- 2.5.4.4 Departments will notify WMATA IT Security of any established connections that are no longer needed as soon as possible.
- 2.5.4.5 All external parties must send logs to WMATA.

2.5.5 Network Patch Management

System administrators are required to promptly test, evaluate and apply (if testing is successful) all security patches and hot fixes to the operating system.

2.5.6 General Wireless Policies

2.5.6.1 Users of any WMATA wireless network are subject to the general requirements that:

- i. Only authorized WMATA users and devices are permitted to use WMATA's wireless technology resources.**
- ii. WMATA IT Security must approve all installations of wireless access points used within WMATA's facilities and enterprise-wide area network. Deployment and management of wireless access points at any WMATA facility is the responsibility of NCS.**
- iii. Wireless services, equipment and users must comply with general WMATA policies and configuration requirements.**
- iv. Users will not interfere with, or disrupt other authorized communications.**
- v. Users will not undertake the unauthorized interception of other traffic.**
- vi. Users will not create own personal hotspots on WMATA buildings and leased spaces. WMATA IT Security will intercept unauthorized signals and remove the unauthorized devices & submit to Chief of NCS.**
- vii. Users will not be connected to WMATA's internal network and any external wireless environment simultaneously on one device. In the event of interference between radio communication technology and a wireless access point, WMATA IT Security and NCS will coordinate WMATA's needs and will determine which system must be reconfigured or shut down to ensure safe and effective operations of WMATA.**
- viii. Users must be authenticated to gain access to any WMATA network.**
- ix. If a user becomes aware of a malicious act, they are to report it to WMATA IT Security and the WMATA Transit Police Department (MTPD) within one hour.**

2.5.6.2 The following requirements will be met in the deployment, configuration and administration of WLAN infrastructure connected to any internal WMATA network:

- i. Only approved wireless access points will be connected to an internal WMATA network. WMATA IT Security will implement wireless monitoring systems to identify and remove rogue access points.**
- ii. WLAN users with WMATA laptops and devices will authenticate to the WMATA WLAN via authentication certificates. Certificates must be installed on each device before the device is provisioned for use.**
- iii. Only WMATA-owned or leased equipment will be granted access to an internal WLAN. All WMATA devices that do NOT have an authentication certificate installed will only be permitted to access the WMATA guest network until a certificate is installed on the device.**
- iv. Vendors and contractors who wish to bring personal, non-WMATA issued devices to connect to the WLAN may do so, but they will ONLY be permitted access to the WMATA guest network.**
- v. All WLAN communications must utilize a secure encryption algorithm that provides an automated mechanism to change the encryption keys multiple times during the connected session and provides support for secure encryption protocols (i.e. the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher).**
- vi. Physical or logical separation between WLAN and wired LAN segments must exist.**

- vii. All WMATA WLAN access and traffic will be monitored for malicious activity, and associated event log files will be stored on a centralized storage device.
- viii. Configuration and security data associated with the WLAN must not be provided to unauthenticated devices (e.g., SSID broadcasting will be disabled).
- ix. WLAN clients will only permit infrastructure mode communication.

2.5.7 Wireless Registration and Appropriate Use

- 2.5.7.1 All wireless access points must be registered with IT. Any active, unregistered wireless access point discovered within WMATA's facilities will be considered an unauthorized device and will be removed from the network.
- 2.5.7.2 All requests for wireless access must be accompanied by a documented business case justification.
- 2.5.7.3 All policies that govern the wired environment apply to the wireless network environment.
- 2.5.7.4 Access IDs and passwords for the use of WMATA wireless communications in public areas will be coordinated through IT.

2.5.8 Wireless Interference and Coverage

- 2.5.8.1 WMATA approaches the shared use of wireless radio frequencies in much the same way that it manages the shared use of the wired network (enterprise-wide area network), in that:
 - i. IT will respond to reports of specific devices that are suspected of causing interference and disrupting WMATA's network and where interference between WMATA's network and other devices cannot be resolved.
 - ii. IT reserves the right to restrict the use of all wireless devices in WMATA-owned buildings and all adjacent outdoor spaces as necessary to support acceptable levels of service availability.
 - iii. In the event that a wireless device interferes with other equipment, NCS and IT Security will resolve the interference based on priority. The order of priority for resolving unregulated frequency spectrum use conflicts will be based on:
 - a. Safety and security;
 - b. Operational communications;
 - c. Administrative communications;
 - d. Public access communications; and
 - e. Personal communications, respectively.

2.5.9 Building Wireless Network Hotspots

- 2.5.9.1 When building a wireless network, which will only provide unauthenticated and/or authenticated access to the Internet, the following must be in place:
 - i. Logical or physical separation from the WMATA LAN when using WLAN hotspots.
 - ii. Packet filtering capabilities enabled to protect clients from malicious activity when using WLAN hotspots.
 - iii. Access and traffic monitoring for malicious activity and log files stored on a centralized storage device for all WLAN hotspots.

- iv. Permission Infrastructure mode communication only, where WMATA clients are concerned for WLAN clients.
- v. Frequent authentication password changes available via an accessible means.
- vi. Physical security of all the network and security devices.

2.5.10 WLAN Network Configuration:

2.5.10.1 The following network configuration will be used when bridging two wired LANs:

- i. All wireless bridge communications must utilize the strongest supported secure encryption algorithm.
- ii. Wireless bridging devices will not have a default gateway configured.
- iii. Wireless bridging devices will be physically or logically separated from other networks.
- iv. Wireless bridging devices will only permit traffic destined to traverse the bridge and should not directly communicate with any other network.
- v. Configuration and security data associated with the WLAN will not be provided to unauthenticated devices (e.g., SSID broadcasting will be disabled).
- vi. Wireless bridging devices will not be configured for any other service than bridging (e.g., a wireless access point).

2.6 Cloud Computing

Cloud computing has grown rapidly in WMATA. Business and IT groups should carefully plan the security and privacy aspects of cloud computing solutions before engaging them. In case WMATA business or IT or vendor proposes any of service models (Software as a service, Platform as a service, Infrastructure as a service) or deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud) as solution then they should ensure that WMATA security and privacy requirements are satisfied. All the projects regardless of service models or deployment models, business owners and IT groups should involve WMATA IT Security, Enterprise Architect (EA) and Network Communications and Services (NCS). Service agreements must comply with business requirements as well as WMATA security and privacy standards All agreements must be reviewed and signed off by the WMATA CIO and CISO.

Following areas should be addressed for cloud computing environment:

2.6.1 Governance, Risk and Compliance

Control and oversight of WMATA policies, procedures and standards (laws and regulations) for application development and information technology service acquisition, as well as design, implementation, test, use and monitoring of deployed or engaged services. Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time. Also, ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications. WMATA IT Security reserves the right to review and audit the implementation of security controls by vendors in these service arrangements. WMATA IT Security can initiate the review of security controls as per their discretion or major upgrade/integration with the system or policy change or as

directed by Security Assessment Plan under the IT risk management process.

2.6.2 Architecture

Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.

2.6.3 Identity and Access management

WMATA IT Security will ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.

2.6.4 Data Protection

WMATA has clear, exclusive ownership rights over data. At all times, WMATA should have ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data. WMATA IT Security will require secure data transfer and destruction procedures upon termination of relationship.

2.6.5 Software Segregation

WMATA IT Security will ensure virtualization and other logical segregation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization. WMATA IT Security will require auditability for the systems to demonstrate the segregation.

2.6.6 Availability

WMATA should have the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements. Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstated in a timely and organized manner.

2.6.7 Incident Response

WMATA should have the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization.

2.7 Disaster Recovery Planning

2.7.1.1 All the IT systems should have a written Disaster Recovery Plan (DRP). The plan should be submitted to IT/DCI (Data Center and Infrastructure).

2.7.1.2 All server files will be backed up through a combination of full and incremental backups. Backups will be sent routinely to an off-site storage depending upon the system.

2.7.1.3 Recovery operations will be documented, stored (both locally and in off-site storage) and executed at periodic intervals to assure the operational environment can be restored accurately and timely.

- 2.7.1.4 Key LAN/WAN components should use some form of duplication to minimize down time from various forms of unexpected outages.
- 2.7.1.5 Redundant WAN communication paths should be available for predetermined, critical systems and be a part of the overall system documentation.
- 2.7.1.6 Equipment replacement agreements should be in place to assure necessary hardware can be replaced with minimal disruption to the operating environment.
- 2.7.1.7 Explicit permission will be required from WMATA IT Security in case additional security requirements or resources are needed for new applications or devices.
- 2.7.1.8 New system will need truly redundant system before deployment.

2.8 Information Resource Strategy and Planning

- 2.8.1.1 Standard, pre-approved equipment and software are available through the WMATA central system. These should be used in most cases. Authorization to pre-approved and standard equipment doesn't need pre-authorization.
- 2.8.1.2 IT maintains a standard, pre-approved equipment, configurations and software list in the central system.
- 2.8.1.3 Employees requiring non-standard equipment or software must complete an online WMATA approved process to request administrative information technology equipment and software. The process/documentation must include a justification for the procurement, identify the budgeted funding source and, where applicable, provide the system configuration information.
- 2.8.1.4 The employee's supervisor or office director must approve the request; upon approval, IT is notified of the request.
- 2.8.1.5 Standard and non-standard items require IT review and approval for compliance from WMATA IT Security Office. Denials may include alternative recommendations.
- 2.8.1.6 The ordering office will contact IT to establish a schedule for the appropriate configuration and installation of the equipment or software. Licensed software may not be installed on WMATA equipment in violation of the licensing agreement.
- 2.8.1.7 All software must be approved by WMATA IT Security prior to installation and installed by IT authorized personnel.
- 2.8.1.8 Software may be loaded on any computer if it meets ALL of the following:
 - i. The software is from a recognized source (either as physical media or a reputable download site).
 - ii. The software is legally licensed or otherwise authorized for use.
 - iii. The software is an original copy (as distinct from a home-made copy).
 - iv. The software is being used for a reasonable legitimate business need as defined by the end user (e.g. not to help run an eBay business or sort home photos).
 - v. The software version is currently supported by the publisher and not more than one version behind the current version.
 - vi. The software is not a BETA version.

- vii. The software is widely used and not known to have serious vulnerabilities or legal liability issues.
- viii. Software that does not meet the criteria should be researched online or undergo testing and approval by IT Security staff prior to installation to ensure safety.

2.9 Information Systems Operations

2.9.1 Change Control (Application and Operating Systems)

- 2.9.1.1 Centrally managed application will be used to record all information technology changes.
- 2.9.1.2 All software changes will require written data owner/management approval prior to implementation.
- 2.9.1.3 Access to production application objects/elements/data will be restricted and controlled.
- 2.9.1.4 Segregation of duties will be maintained while moving changes to production.
- 2.9.1.5 Promotion of application changes from a test environment to a production environment requires formal change management procedures to be executed by non-programming personnel. These procedures should include appropriate backups of software and components prior to the promotion. Execution modules and source code will be managed in this process to ensure that the source code matches the code that will be executing in the production environment.
- 2.9.1.6 Written communication will be established for the changes impacting production environment and its users.

2.9.2 Personal Computers, Smartphones, and Tablets

- 2.9.2.1 All business units must register all WMATA desktops, smartphones and tablets with IT.
- 2.9.2.2 Each PC, smartphone, and tablet must be imaged with the standard and approved WMATA operating system (OS) image.
- 2.9.2.3 No PCs may be connected to WMATA WAN, and, at the same time, be connected to another wireless connection, hotspot or any other mechanism that could be used to create a connection between WMATA WAN and an external network.
- 2.9.2.4 Installation or use of remote access hardware/software (e.g. dial-up modem) without explicit permission from WMATA IT Security is strictly prohibited.
- 2.9.2.5 Each computer will be attached to the domain.

2.9.3 Appropriate Usage

- 2.9.3.1 The primary usage of WMATA-provided electronic access is for official WMATA business, which includes, but is not limited to:
 - i. Sending and/or receiving official WMATA correspondence to locations or addresses internal or external to WMATA; and

- ii. Mass mailings of official information throughout WMATA when the message is pertinent to the vast majority of the recipients, and with the required approval of an Office Director/General Superintendent has been obtained, including but not limited to:
 - a. Staff notices;
 - b. Service schedules;
 - c. Newsletters; and
 - d. Meeting announcements.

2.9.3.2 Neither employees nor contractors have an inherent right to WMATA electronic access, and such access is at the discretion of office directors/general superintendents. Additionally, information technology equipment availability and/or limitations may preclude an employee or contractor from having electronic access. Use of WMATA electronic access for non-WMATA purposes may be revoked or limited at any time by appropriate WMATA department heads/office directors.

2.9.4 Inappropriate Usage

2.9.4.1 Employees and contractors are expected to conduct themselves professionally in the workplace and to refrain from using WMATA electronic access for activities that are inappropriate. Misuse or inappropriate personal use of WMATA electronic access includes, but is not limited to:

- i. Using WMATA systems to gain unauthorized access to other systems.
- ii. The creation, copying, transmission or re-transmission of chain letters or other unauthorized mass mailings (regardless of the subject matter).
- iii. Mass mailings of personal information throughout WMATA (e.g., personal items for sale.)
- iv. Using WMATA electronic access for activities that are illegal, inappropriate or offensive to fellow employees, contractors or the public. Such activities include, but are not limited to hate speech or material that is prohibited by nondiscrimination laws that are applicable to WMATA.
- v. The creation, downloading, viewing, storing, copying or transmission of illicit and/or illegal materials. This includes materials related to sexually explicit, sexually oriented, illegal gambling, illegal weapons, terrorist activities and any other illegal activities or activities otherwise prohibited.
- vi. Engaging in any outside fund-raising activity, endorsing any product or service or engaging in any prohibited partisan political activity.
- vii. Releasing agency information to external news groups, bulletin boards or other public forums without WMATA consent. This includes, but is not limited to any use that could create the perception that the communication was made in one's official capacity as a WMATA employee or contractor (unless appropriate WMATA approval has been obtained), or uses contrary to WMATA's mission or positions.
- viii. Any use that could generate more than minimal additional expense to WMATA. Examples of minimal additional expenses include using a computer printer to print a few pages of material, infrequently sending personal email messages or limited use of the Internet for personal reasons. Such use should only incur a minimal additional expense to WMATA in areas such as:
 - a. Communications infrastructure costs (e.g., telephone charges, telecommunications traffic, etc.);

- b. Use of consumables in limited amounts (e.g., paper, ink, toner, etc.);
 - c. General wear and tear on equipment;
 - d. Data storage on storage devices; and/or
 - e. Transmission impacts with moderate email message sizes (such as emails with small attachments).
- 2.9.4.2 The unauthorized acquisition, use, reproduction, transmission or distribution of any controlled information (including computer software and data) that includes privacy information, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data or export-controlled software or data.
- 2.9.4.3 Maintaining or supporting a personal or private business, support of for-profit activities or other outside employment or business activity. Examples of this prohibition include employees and contractors using a WMATA computer and Internet connection to run a travel business or investment service, consulting for pay, sales or administration of business transactions, and sale of goods or services.
- 2.9.4.4 General interest information is to be placed on the WMATA Employee Bulletin Board, rather than sending an email message to large groups of employees. Predetermined posting areas are: lost/found items, death notices, for sale/rent, giveaways, retirements/farewells, special events and help/assistance requested.
- 2.9.4.5 The forwarding of WMATA business emails to an end user's own personal/private accounts (such as gmail.com, hotmail.com or other Internet based email services).
- 2.9.4.6 The use of an end-users own personal/private account (such as gmail.com, hotmail.com or other Internet based email services) to conduct WMATA business.

2.9.5 Acceptable Personal Use

- 2.9.5.1 Limited personal use is also authorized, and each director/general superintendent is responsible for establishing appropriate standards. Employees or contractors are allowed to use electronic access for non-WMATA purposes when such use involves minimal additional expense to WMATA, is performed on the employee's or contractor's non-work time, does not interfere with the mission or operations of a department or office, and does not violate any other security standard, law or regulation.
- 2.9.5.2 The following examples are specifically acceptable uses of the Internet by WMATA users:
- i. Accessing Internet content for professional development, to maintain currency of training or education, or to discuss issues related to the Internet user's WMATA activities;
 - ii. Use for advisory, standards, research, analysis and professional society activities related to the user's work tasks and duties;
 - iii. Using the Internet to read news stories or other information of personal interest, check financial information, review pay deposits, etc.

2.9.6 Examples of Unauthorized Personal Use

- 2.9.6.1 The following are specifically unacceptable uses of the Internet by WMATA users.

- i. Any purpose which violates a federal or state law, code, policy, standard or procedure.
- ii. Purposes that conflict with the mission, charter or work tasks of a WMATA department.
- iii. Private business, including commercial advertising.
- iv. Viewing, accessing, transmitting, distributing, making and or/ causing anyone to receive:
 - a. Sexually explicit and obscene material (including any and all forms of pornography, adult humor, profanity, dating services/personals);
 - b. Websites selling alcohol, tobacco, drugs, firearms and other weapons;
 - c. Websites advocating or involving terrorism, hacking, gambling, fraud or any other criminal conduct or enterprises;
 - d. Harassing material, including racial, religious, national origin, sexual or sexual-orientation harassment; and/or
 - e. Information that violates federal laws on discrimination.
- v. Interference with or disruption of the network and/or associated users, services or equipment.
- vi. Promoting or advertising religious or political positions, causes or organizations.

2.9.7 Privacy Expectations

- 2.9.7.1 WMATA employees and contractors do not have a right to, nor should they have an expectation of privacy while using any WMATA electronic access at any time, including accessing the Internet or using email. To the extent that employees and contractors wish that their private activities remain private, they should avoid using WMATA electronic access, even if that activity is otherwise authorized.
- 2.9.7.2 By using WMATA electronic access, WMATA employees and contractors consent to disclosing the contents of any files or information maintained or passed through WMATA electronic access.
- 2.9.7.3 Certain WMATA offices and departments have special privacy requirements that must be assured in order to send sensitive emails or store information on network drives. IT approval is required for the usage or establishment of secured, private areas on the network to accomplish this.
- 2.9.7.4 By using WMATA electronic access, employees and contractors consent to monitoring and recording of their access to, and use of electronic equipment that is covered with or without cause or prior notification. While some offices and departments may be using security measures that ensure confidentiality of information, the general understanding is that such use is not secure, is not private and is not anonymous.
- 2.9.7.5 System managers do occasionally employ monitoring tools to detect improper use. Electronic communications may be disclosed within WMATA to employees and contractors who have a need to know in the performance of their duties. IT will receive approval from relevant department heads prior to any interception or examination of their department's data.

2.9.8 Inappropriate Web Content and Filtering

- 2.9.8.1 The use of WMATA information technology systems to access inappropriate web content is strictly prohibited and will be blocked. Any user attempting to access such content will be subject to disciplinary action, up to and including termination of employment.
- 2.9.8.2 The use of web content filtering ensures that Internet users do not intentionally or inadvertently access Internet sites and Web pages that are non-business related and could otherwise violate relevant WMATA policies or regulations. WMATA exercises its' access control rights, in the best interest of all Internet users, by disallowing, segregating or rejecting certain Internet listings. The following web content categories will be blocked:
- i. Sexually explicit and obscene material (including any and all forms of pornography, adult humor, profanity, dating services/personals);
 - ii. Websites selling alcohol, tobacco, drugs, firearms and other weapons;
 - iii. Websites advocating or involving terrorism, hacking, gambling, fraud or any other criminal conduct or enterprises;
 - iv. Harassing material, including racial, religious, national origin, sexual or sexual-orientation harassment; and/or
 - v. Information that violates federal laws on discrimination.
- 2.9.8.3 If a website is believed to be miscategorized, end users may request a website review by contacting the IT Helpdesk. WMATA IT Security will review the request and unblock websites found to be miscategorized.
- 2.9.8.4 Employees may access blocked websites with the permission of their management, if it is appropriate and necessary for business purposes. The request will require a written request by the appropriate office director, general superintendent or AGM. WMATA IT Security will review all such requests and unblock as appropriate.
- 2.9.8.5 Any Internet sites or web pages deemed illegal by federal or applicable state laws are prohibited and will be blocked.

2.9.9 Web Content Filtering System Access and Management

- 2.9.9.1 The content filtering system will be managed by specific WMATA IT Security personnel assigned and designated to engineer and update the system as appropriate.
- 2.9.9.2 All reporting and data access will be approved by the AGM, IT and the Chief, IT Security.

2.9.10 Unique User ID (UID) Ownership and Accountability

- 2.9.10.1 All users are to be provided with a unique user ID (UID) and password prior to being permitted to use any hardware and/or software connected to the WMATA network.
- 2.9.10.2 The UID will be individually owned in order to maintain accountability.
- 2.9.10.3 A UID will be used by only a single individual, and that one individual is responsible for every action initiated by that account.

- 2.9.10.4 Root and master UIDs will be used for specific tasks that cannot be accommodated with the use of an individually owned one.
- 2.9.10.5 Service accounts should only be used for application internal communication and must not be used by system and data administrators to log to servers or applications.
- 2.9.10.6 System administrators are not permitted to use root accounts for normal operational tasks. Each system administrator should be assigned a unique account as stipulated above.
- 2.9.10.7 All user accounts will be certified every 12 months. All accounts that are not certified will be suspended. Accounts that are not certified within three months of suspension will be removed from the system of record.
- 2.9.10.8 All user accounts will be suspended immediately upon notification of the user's separation from WMATA.
- 2.9.10.9 Anyone transferring from one department to another will have any specialized access for the prior department removed. The management official of the new department must initiate a request for specialized access, if appropriate.

2.9.11 UID Authentication

- 2.9.11.1 A UID and password combination serves as the primary digital identity for each authorized system user.
- 2.9.11.2 The UID and password combination will not be shared under any circumstances.
- 2.9.11.3 The use of generic or shared UID and password combinations are not authorized but may be considered on a case-by-case basis.
- 2.9.11.4 Access to a system will be locked if more than five consecutive invalid passwords are keyed.

2.9.12 Password Standards

WMATA IT Security utilizes industry best practices benchmarks. IT Security will provide the current password standards used in initial project meetings or as needed by implementation team.

2.9.13 Service Account Password Standards

WMATA IT Security utilizes industry best practices benchmarks. IT Security will provide the current password standards used in initial project meetings or as needed by implementation team. Service account password standards are lot stricter than user account passwords.

2.9.14 Password Management and Compliance Standards

- 2.9.14.1 Audit information will be captured by the system to reflect password usage and management.
- 2.9.14.2 Passwords will be treated as highly sensitive data and must be protected by the use of encryption at all times.
- 2.9.14.3 All password systems will be configured by the appropriate system owner or administrator to implement the following security controls:

- i. **Password Management** - Each password system will be configured to automatically enforce minimum password standards, such as password length, composition and required password change interval. Users will automatically receive notification seven days in advance of their password expiration.
- ii. **Accountability** - Each password system will identify each instance of authorized access, because systems that process sensitive information must guarantee user accountability.
- iii. **Personal Identification** - Each password system will assure identification of each individual user.
- iv. **Password Integrity and Confidentiality** - Each password system will protect the password database at a level equal to the protection given sensitive information throughout WMATA.
- v. **Auditing** - Each system will be configured to record information about user accesses.
- vi. **Use of Passwords to Protect Data** - All stored passwords will be encrypted using an approved encryption method.

2.9.14.4 Passwords will not be stored, unencrypted:

- i. In readable form in batch files;
- ii. In automatic logon scripts;
- iii. In software macros;
- iv. In terminal function keys;
- v. In data communications software;
- vi. In web browsers;
- vii. On hard drives unencrypted; or
- viii. In other locations where unauthorized persons might discover them.

2.9.15 Remote Access Methods

- 2.9.15.1** Secure remote access to WMATA's network is vital to maintaining the integrity and availability of the network. Only the following remote access methods are permitted: IPSec VPN; or SSL VPN.
- 2.9.15.2** The Remote User must have the capability to connect to an Internet Service Provider (ISP) i.e., a Digital Subscriber Line (DSL) service, a cable modem provider, commercial dial-up service or any Local Area Network (LAN) with Internet access.
- 2.9.15.3** Remote connectivity to the WMATA WAN is permitted by either IPSec VPN or SSL VPN only.

2.9.16 Authorized Remote Users

- 2.9.16.1** Only those remote users who have a valid business justification for remote VPN access to WMATA resources will be granted access appropriate to that user's job function. Access is limited to specific business purposes in support of WMATA's mission.
- 2.9.16.2** Remote access will be restricted to the resources specified in submitted requests.

2.9.17 Anti-Virus Software Requirements for Remote Users

- 2.9.17.1** It is the direct responsibility of the user of the remote session to ensure WMATA-approved anti-virus software is installed on the remote PC.

2.9.17.2 Anti-virus software can be obtained at no charge from WMATA IT Security for approved WMATA employees and contractors. The user remains directly responsible for maintaining both anti-virus application upgrades and virus signature updates.

2.9.17.3 WMATA retains the right to inspect end user stations for up-to-date antivirus software and virus definitions before granting access via VPN. Should it be found that the user does not have the appropriate antivirus protection, their connection will be terminated, and no further VPN access will be granted until the end user station is confirmed as anti-virus compliant.

2.9.17.4 Users not in compliance with any part of the anti-virus requirement will be denied VPN access to WMATA resources.

2.9.18 Remote Session Audit and Monitoring

2.9.18.1 Each remote session will be monitored, and the date, time, duration and user ID will be audited.

2.9.18.2 In order to ensure equitable use of resources, session lengths will time out if the connection remains inactive for a predetermined amount of time (e.g., 30 minutes).

2.9.19 Reporting Violations

2.9.19.1 Employees or contractors observing violations, or receiving emails in violation of this section (2.10) should report the violation as follows:

- i. Matters of a suspected criminal nature (e.g., distribution of child pornography) will be reported to MTPD and/or OIG.
- ii. Materials that violate nondiscrimination laws applicable to WMATA, including but not limited to sexual harassment, shall be reported to CIVR.
- iii. Matters constituting non-criminal serious misuse (e.g., viewing or disseminating pornography and sexually-explicit material, use for non-WMATA profit-making activity) will be reported to OIG.

3 Guidelines and Tools

Guidelines and tools are available with IT offices on policies and procedures. Please reach out for specific guideline to IT Security office for further guidance:

3.1 Guidelines

All users of WMATA IT Systems must follow standard operating procedures issued by IT offices. Each policy or standard has its guidelines to assist business users, contractors and vendors.

3.2 Tools

Following tools are provided to IT personnel as self-service portals. These tools should be used to manage the vulnerabilities and security gaps in the systems.

3.2.1 Security Center – Self-service vulnerability management portal

3.2.2 IBM Endpoint – Patch management tool to apply patches to operating systems.

3.3 Training Requirements

All employees and contracting staff should be trained in their respective technical and soft skills according to their roles and responsibilities. All personnel are required to acknowledge at least annually that they have read and understood the security policy and procedures. All personnel should attend security awareness training upon hire and at least annually.

4 References

Related Policy or other supporting documents