Appendix 5

MARYLAND DEPARTMENT OF TRANSPORTATION

INFORMATION SECURITY PLAN

Revision Date: 05/05/2017

Table of Contents

This document contains sensitive information; its contents are not to be shared without the written permission of the Maryland Department of Transportation Chief Information Officer.

1.1 Objective of Security Planning

The objective of system security planning is to improve protection of information technology (IT) resources. Maryland Department of Transportation (MDOT) systems have some level of sensitivity and require protection as part of good management practice. This document discusses the protection of MDOT information technology (IT) resources. The content provides security guidance in the form of subject matter security policies grouped together to form a basis for a security plan. The completion of system security plans is a requirement of the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," and Public Law 100-235, "Computer Security Act of 1987."

The purpose of this security plan is to provide an overview of the security requirements for the MDOT tangible and intangible assets. This document provides security guidance for security controls that are in place or are planned in order to strengthen the MDOT overall security posture. This system security plan also delineates responsibilities and expected behavior of all individuals who access MDOT IT resources. The intent of this security plan is to provide a living document that should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for use by all MDOT Agencies and departments and reflects input from various MDOT managers with responsibilities for various IT resources. Additional contributors include MDOT information owners, system administrators, system operators, end-users, and the Security Working Group for the MDOT. Updated information may be included in the basic plan and the structure and format will continue to be organized according to MDOT agency requirements as defined by the MDOT Security Working Group (SWG) beginning in early 2000.

This security plan will protect MDOT IT resources, if all Transportation Business Units (TBUs) of the MDOT review and continue to contribute requirements to the Security Working Group where necessary changes are authorized. All security relevant enhancements must be documented and authorized by the MDOT Change Advisory Board (CAB)on a weekly basis. This risk management component of MDOT provides an important quality control by authorizing proposed change control and accepting all residual risks ensuring a balance among continuity of operations, costs, and viable security solutions.

> **The security-planning document is based on an assessment of management, operational and technical controls and the authorization of the CAB in response to recommendations from modal representatives and the Security Working Group. An annual review of the entire security plan must be done and documented and a periodic recurring review of the guidance provided within this security plan must be carried out in response to any significant change that impacts the three main security attributes, namely, confidentiality, integrity, and availability. This security plan better positions the MDOT in ongoing efforts to strengthen security posture, and meeting fiduciary responsibility of due care and due diligence. Thus, MDOT is**

taking a proactive approach to information assurance through layered security that calls upon talent, technology, and tools.

1.2 History of This Document

The Information Systems Security Plan document is the result of a collaborative effort between the MDOT modal representatives and the SWG and is based on the requirements of the MDOT TBUs as submitted to the SWG. Work continues in crafting content and enhancing structure and format that complements existing MDOT documentation. Adoption of this document is contingent upon acceptance by the MDOT Change Advisory Board.

1.3 Organization of This Document

Security Policy is the basis for much of the security guidance within an organization, therefore this document is organized in a linear format with the subject matter content reflecting various specific security policies contributed from MDOT representatives. The SWG considered the content and appropriateness before making further changes during review sessions held monthly and the policies will eventually be available on MDOT intranet web sites for easy access.

1.4 Seven Areas of Security Useful For Policy and Planning

1.4.1 Physical Security

Physical security measures focus on the physical protection of a system or facility and the controls in place, which restrict access to system resources through:

- Access control systems that range from simple key locks to cipher locks and sophisticated key/swipe card systems, and biometric fingerprint readers.
- Keys, combinations and keycards that require the same level of protection afforded the most sensitive information processed or handled within the facility.

1.4.2 Environmental Security

- Fire suppression systems (sprinklers, fire extinguishers).
- Heating and air conditioning systems.
- Emergency lighting and power distribution systems.
- Controlled environment (temperature, humidity, air filtration).
- Manual procedures and practices designed to protect delicate equipment from damage.
- Prohibition of eating and drinking around computer equipment.

- Prohibition of smoking around equipment to eliminate a common source of damage to hard drives and potential for fires.

- Institution of good housekeeping practices to control dust and dirt around computer equipment.

1.4.3 Personnel Security

Personnel security practices are those steps taken to:

- Ensure the integrity and reliability of prospective system users and all other persons with access to sensitive infrastructure and information.

- Ensure user awareness and understanding of their individual security responsibilities.

1.4.4 Hardware Security

- Ensure the protection of the hardware components of a system.

- Maintenance of accurate and up-to-date inventories of all equipment.

- Procedures (property passes) that ensure accountability for all equipment.

- Procedures for securing or logically disconnecting equipment when idle or unattended

1.4.5 Software And Data Security

Security practices in these two areas focus on the manual practices and procedures implemented to complement the automated security controls that:

- Protect operating system software, applications software and database files.

- Protect (configuration/change management) application and operating system software throughout the development and integration processes.

- Provide assurance of the integrity and accuracy of the software.

- Continue software and data security practices throughout the system life cycle.

- Address the effective implementation, integration and administration of the various security features contained in the operating system, application, and database software.

1.4.6 Security Administration

Security administration practices include those measures associated with the implementation and administration of the computer security program. These practices include:

- Develop and implement comprehensive and effective security plans.
- Develop and test contingency and disaster recovery plans.
- Document all aspects of the security program.
- Develop and provide security training to all employees at all levels.
- Maintain a high level of user security awareness.

1.4.7 Procedural Security

Procedural security measures include manual controls implemented to supplement automated protection provided by infrastructure components by:

- Documentation of those measures and controls as a foundation to support secure system operations.
- Creation of an enterprise level Security Policy document that is based on a security risk assessment baseline that provides guidance for the creation of subsequent security documentation and supporting procedures.
- Includes the definitions, roles and responsibilities of all system users.
- Specifies the system security architecture and implementation.
- Specifies types of user activities.
- Describes other sets of manual procedures designed to ensure the safe and secure operation of networks and mainframe systems.

Section 2: Introduction

2.1 Critical Business Function

Information and information systems are necessary for the performance of just about every essential activity. Serious security problems with this information or these information systems could result in lost customers, reduced revenues, identity theft, compromise of data, and/or degraded reputation. As a result, information security must be a critical part of an MDOT's business environment.

2.2 Information Security Policies

An Information Security Policy is an imperative element of a complete information security plan that touches every part of MDOT where data is created, modified, stored or processed. Internet security demands the presence of policies that dictate how security products and devices are used to protect MDOT assets. Information Security is not about tools, but about risk assessment, management, and everyone exercising best practices. Therefore, sound security policies and practices help shore up defenses and thwart inadvertent or hostile attacks on the MDOT network. Adequate Information Security Policies that secure MDOT services creates trustworthiness that customers both demand and deserve.

Section 3: Remote Data Access Policy

3.1 Purpose

The purpose of this policy is to support the appropriate strategies for, and acceptable use of, remote access to Maryland Department of Transportation (MDOT) networks and network services and MDOT data. Well designed and properly managed systems expedite business communications, reduce paperwork, and automate routine office tasks thereby increasing productivity and reducing costs. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT Chief Information Officer (CIO).

3.2 Scope

This policy applies to an individual, group of individuals, organizations, or companies who have been given authorization to access the Maryland Department of Transportation (MDOT) enterprise network/data remotely. This policy applies to all Transportation Business Units (TBUs), Agencies and/or Departments operating as part of the Maryland Department of Transportation. Amendments, changes and/or additions to this policy follow a structured review and approval process.

For the purpose of this policy, Remote Access is defined as accessing non-public MDOT or TBU networks, computers, or computer services and applications (such as Web sites and Web-based applications and corporate data from a location that does not provide a direct connection (wired or wireless) to the MDOT/TBU Enterprise (internal) network/data. If at any time the connection must go through a network not provided by MDOT, the connection is considered remote access.

Public access to services, data, and applications made available on the Internet is not within the scope of this policy.

3.3 Policy Statement

Remote access is made available for administrative, management, enforcement, procurement, support, and maintenance functions. MDOT computers and networks provide access to numerous computing resources, many of which contain confidential data or contain devices that support public safety. Remote access is a privilege and requires that individuals act responsibly. Users must respect the rights of other users as well as the integrity of the systems, related physical resources, relevant laws, regulations and contractual obligations. Users must also ensure the appropriate confidentiality of information retrieved and stored on remote devices.

.

3.4 Responsibilities

Each TBU is responsible for observing this policy or developing policy that is entirely consistent with this MDOT policy. The unique needs of each TBU's business and technical environments may include additional guidance as long as it is consistent with and meets the minimum requirements of State policies, standards and guidelines as well as regulatory mandates, such as Payment Card Industry (PCI), and the requirements of other agencies MDOT interfaces with, such as the U.S. Department of Justice, Federal Bureau of Investigation – "Criminal Justice Information System (CJIS) Security Policy".

Agency and TBU executive management will ensure that program unit management and unit supervisors implement policy. Individuals with supervisory responsibilities must ensure that their subordinates are aware of their responsibilities.

Remote Data Access Policy is developed by the MDOT sanctioned Security Working Group and submitted to Configuration Control Change Advisory Board (CAB) for interim approval. The MDOT CIO will present the proposed policy to the Information Technology Governance Board (ITGB) for review. The MDOT CIO will have final approval of the policy.

Approved Remote Data Access Policy is implemented under the direction of the MDOT Network Project Manager and the CAB and consists of tracking the approved Change Requests (CRs), ensuring that approved work is progressing on the CAB schedule.

The following sections define remote access responsibilities based on the role of the individual:

3.4.1 MDOT

MDOT will provide and centrally manage a Mobile Device Management Suite (MDM)[1]. This suite will enable technical controls to be managed on remote devices by MDOT. The MDM suite will force specific security functionality on remote devices such as password locks/timeouts, etc… At any time MDOT may find it necessary for security reasons to deregister a remote device, thereby cutting off access to the MDOT network. The above described functionality covers both personally owned and state owned equipment.

3.4.2 Remote Access User

Remote Access Users are defined as individual employees, contractors, or federal/state/local government employees who require remote access to MDOT networks and network services and corporate data. Remote Access Users are responsible for obtaining, completing, submitting, and observing requirements of the Remote Access Request Form.

[1] As of this update 01/09/14 An MDM suite has been purchased. TBU administrators have been trained and will be able to establish their policies for applications that would be available from mobile devices.

All Internet Remote Access Users are responsible for procuring, configuring, and installing a personal firewall, anti-virus protection software, and encryption software (as appropriate for sensitive data) on the device used to remotely connect to MDOT, if available. Remote Access Users are further responsible for keeping these protections up to date. Users are responsible for assuring that their operating system and application software is patched against known vulnerabilities. Remote Users accept that their personally owned or MDOT provided mobile device will be managed via the MDM system. MDOT will load MDM software which allows MDOT the ability to remote disconnect and even wipe the device of MDOT info that is segmented out separately from their own information if it is a personal device.

The Remote Access User is responsible for installing, configuring, and maintaining any additional software required for establishing remote access communications, such as Virtual Private Network (VPN) clients or Secure Socket Layer (SSL) clients. Remote Access Users are also responsible for any additional software required to access network services, such as Citrix or other required software on their personal device.

The Remote Access User is responsible for the safekeeping of any devices assigned to the user for two-factor authentication, (such as hardware tokens mini-token, smart cards, etc.) and must report lost or stolen devices immediately to their Remote Access Administrator or TBU Service Desk. The Remote Access User may incur the cost of replacement devices.

The Remote Access User is responsible for reporting Remote Access Client or Application Software problems to their TBU Service Desk. The Remote Access User is also responsible for notifying the Remote Access Administrator that the connection either does or does not work upon completion of installation.

The Remote Access User is responsible for all system hardware and software maintenance to their remote device. MDOT and MDTA are not responsible for the condition of the remote Access User's personal remote device.

The Remote Access User's supervisor is responsible for notifying the Remote Access Administrator if and when the Remote Access User leaves state service, or is no longer working on behalf of an MDOT TBU in the case of a contractor.

3.4.3 TBU Supervisor

The TBU Supervisor is responsible for reviewing the Remote Access Request Form from the User and ensuring the user has correctly completed and signed the user portion of the form.

The TBU Supervisor authorizes the request by signing the Remote Access Request Form and specifying the types of access the User is granted. The TBU Supervisor then forwards the form to the TBU IT Office.

The TBU Supervisors will use MDOT approved technologies such as MDM, virtualization and remote control, to keep confidential data off mobile devices.

3.4.4 TBU Remote Access Administrator

The TBU Remote Access Administrator is responsible for coordinating activities associated with the Remote Access Request Form. He/she ensures the information on the form is correct and signed by the User, and the User's supervisor.

The TBU Remote Access Administrator is responsible for creating a remote access account for the user.

The TBU Remote Access Administrator is responsible for providing the User with all the passwords, configuration information, installation software and manuals required to access resources on the MDOT network remotely.

The TBU Remote Access Administrator is responsible for providing any required training to the Remote Access User on the use of applications required for Remote Access to the MDOT network

Each TBU Remote Access Administrator shall maintain a file, electronic or paper, containing the signed copies of the Remote Access Forms.

The Remote Access Administrator is responsible for notifying the user's supervisor when the account is setup.

The Remote Access Administrator is responsible for notifying the Remote Access User's Supervisor of violations of this and any acceptable use policy.

3.4.5 Remote Access Request Process

Figure 1 presents a diagram of the remote access request process.

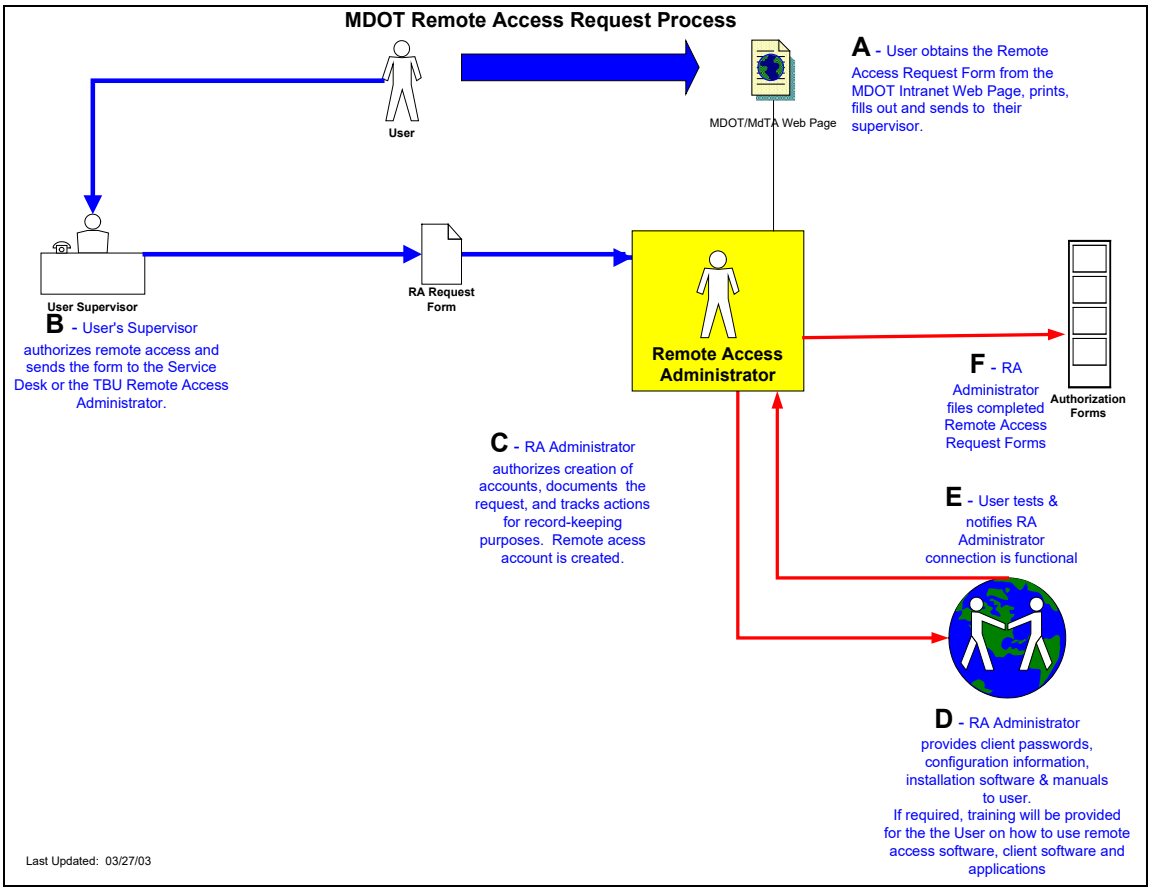

Figure 1 - Remote Access Request Process

3.5 Guidance

3.5.1 User or Individual Remote Access

An MDOT/TBU employee or individual contractor employee (User) requiring remote access to the MDOT/TBU network(s) and services initiates the Remote Access Request Process. The entity can obtain the Remote Access Request Form from the MDOT Intranet Web Page) or from the Remote Access Administrator. The User will print, complete and sign the User portion of the form and forward it to the User's Supervisor.

The User's Supervisor will review the User's request, authorize it and send the MDOT Remote Access Request Form to the TBU Service Desk or Remote Access Administrator.

The TBU Remote Access Administrator then reviews the request, ensures the Supervisor has correctly completed the Supervisor's section. The TBU Remote Access Administrator will ensure the request is documented and the actions are tracked in Maximo or another process for record-keeping purposes.

The TBU Remote Access Administrator then creates a remote access account for the user.

The TBU Remote Access Administrator maintains a file, electronic or paper, containing the completed MDOT Remote Access Request Form.

3.5.2 Third Party Remote Access

Request for remote access from organizations seeking a site-to-site connection over Internet-based Virtual Private Network (VPN) connections, or via direct telecommunication circuits will follow the guidance found in the "Third-party Access Policy".

3.5.3 Acceptable Use

Remote Access is provided for the purpose of conducting the business of and to support the mission of each department of MDOT. The following list, although not all-inclusive, provides some examples of acceptable use:

- Communication with Federal, State or Local Government personnel, vendors, and other private businesses;
- Communication and information exchange for professional development or to maintain knowledge or skills;
- Activities involving State-association, Government-advisory, or standards activities;
- Communications for administrative purposes.
- Activities involved in the remote administration, support, or maintenance of MDOT/TBU network, computers, applications, and computing services
- Remote access to authorized systems and or data via the Internet

3.5.4 Remote Host Requirements for PCI Data Security Standards

In accordance with Payment Card Industry Data Security Standards (PCI DSS)[2], any MDOT employee or contractor remotely accessing a device that is in-scope with cardholder data must use a State-issued laptop with the following configuration in effect:

[2] PCI DSS Requirements and Security Assessment Procedures v3., 1.4, 1.4a, 1.4b (https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf)

- Local firewall configured according to MDOT standards that cannot be changed by the laptop user.

- Local administrator account is not known or accessible by the laptop user.

- Local user account is for use by the laptop user and does not have access to change the firewall settings.

- Automatic updates setup for anti-virus, malware, and patches.

3.5.5 Restrictions

Remote Access may not be used for unlawful activities, commercial purposes not under the auspices of MDOT, personal financial gain, personal use inconsistent with guidelines contained in this policy, or uses that violate other State policies or guidelines. The latter include, but are not limited to, policies and guidelines regarding intellectual property, or regarding sexual or other forms of harassment. The following list, although not all-inclusive provides some examples of unacceptable use of Remote Access:

- Private or personal, for profit activities (e.g., consulting for pay, sale of goods, charity fundraising);

- Solicitation of non-State business, or any use for personal gain or profit;

- Engaging in any illegal or wrongful conduct, including communications which violate any laws or regulations, including copyrights, patent protections, license agreements, or other intellectual property rights of third parties;

- At no time should any MDOT employee, contractor, or federal/state/local government employee provide their login or email password to anyone, not even family members.

- MDOT employees, contractors or federal/state/local government employee with remote access privileges must ensure that their company-owned or personal computer or workstation, which is remotely connected to the MDOT corporate network, is not connected to any other network at the same time

- Accessing or transmitting threatening, obscene, defamatory, fraudulent or harassing messages, even as a prank;

- Use for any purpose that is against State or Public policy or contrary to the State's best interest;

- Intentionally seeking information about, obtaining copies of, or modifying files, other data, or passwords belonging to other users, unless explicitly authorized to do so by those users;

- Attempts to gain unauthorized access to any information facility, whether successful or not. This includes running programs that attempt to calculate or guess passwords, or that are designed and crafted to trick other users into disclosing their passwords. It also includes electronic eavesdropping on communications facilities;

- Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted

- Any action that invades the privacy of individuals or entities that are the creators, authors, users, or subjects of information resources;

- Misrepresenting in any manner, your identity, your account or a computing device in an Email or other electronic communication;

- Sending chain letters, advertisements, or solicitations of any type;

- Sending mass mailings to individuals who have not expressly agreed to be contacted in this manner;

- Knowingly sharing a personal account which includes use of a two-factor authentication device such as a token, grid card, soft token, etc.;

- Interfering with or disrupting network users, services, or equipment. Such disruptions could include, but are not limited to (1) distribution of unsolicited advertising or messages, (2) propagation of computer worms or viruses, and (3) using the network to gain unauthorized entry to another machine on the network;

- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojan horses, and worms;

- Disclosing confidential or proprietary information.

- Use of any Dial-in desktop modems is prohibited unless specifically approved by the MDOT Change Process. (CAB) Change Advisory Board

- Use of remote control software is prohibited unless specifically approved by the MDOT Change Process. (CAB) Change Advisory Board

- Use of a network monitoring tool is prohibited unless specifically approved through the MDOT Change process-(CAB) Change Advisory Board

3.5.6 Representation

Remote Access Users shall not give the impression that they are representing, giving opinions or otherwise making statements on behalf of MDOT or any unit of the State unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing this Agency or State.

3.5.7 Interference

Remote Access shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities or unwarranted or unsolicited interference with others' use of Remote Access systems. Such uses include, but are not limited to chain letters, "spam", "letter-bombs", and willful transmission of known computer viruses or other agents that are engineered to damage system resources, or could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities.

3.5.8 No Expectation of Privacy

Privacy of Remote Access is not guaranteed. Authorized State employees may access and disclose the contents of all messages created, sent, or received using the State's email system to authorized State supervisory personnel. The State affords electronic mail privacy protections comparable to that which it traditionally affords paper mail and telephone communications within the context of the State's legal and other obligations. The State shall make every reasonable effort to avoid viewing Union-related messages initiated by Union staff or bargaining unit members in accordance with Union agreements.

3.5.9 Security

The following specific guidance relating to Remote Access security is provided:

Strong Authentication

All users connecting from a remote host to the internal enterprise network must use two-factor authentication employing a method tested and approved by the Security Working Group.

VPN Encryption

All users connecting from a remote host to the internal enterprise network must use an encryption method that has been tested and approved by the Remote Access Group.

Virus Scan Software and Personal Firewalls

All users connecting from a remote host to the internal enterprise network must procure, install, and operate personal anti-virus and malware protection software. All users connecting from a remote host to the internal enterprise network via the Internet must procure, install and operate personal firewall software. Users should consult the INFOSEC group for guidance on acceptable approaches.

Users are responsible for assuring that their operating system and application software is patched against known vulnerabilities.

All users connecting from a remote host to the internal enterprise network may be subject to a coordinated vulnerability assessment by MDOT or upon MDOT direction of their security contractor to test for proper security implementation at the remote host.

Authentication Token Policy

All users in possession of a security token are responsible for guarding and insuring the safekeeping of their token and must not share or redistribute tokens.

Users must report lost or stolen tokens to the remote access administrator or TBU Service Desk immediately. In the event a token is stolen, a police report must be filed for the missing article.

VPN Client Updates

VPN client updates are distributed to each TBU Remote Access Administrator and become the TBU Remote Access Administrator responsibility to distribute the update to their users.

Disclaimer

MDOT assumes no responsibility for any hardware, software, operating system problems, or the loss of any functionality or data to any personal user device used by any MDOT TBU Remote Access User.

3.5.10 Records Retention

State Records communicated using Remote Access must be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed, and accessible in an existing filing system outside the Remote Access system in accordance with each Department's standard practices.

Examples of Remote Access messages that typically are records include:

- Policies and directives,
- Correspondence or memoranda related to official business,

- Work schedules and assignments,
- Agendas and minutes of meetings,
- Drafts of documents that are circulated for comment or approval,
- Any document that initiates, authorizes, or completes a business transaction,
- Final reports or recommendations.

Some examples of messages that typically do not constitute records are:

- Personal messages and announcements,
- Copies or extracts of documents distributed for convenience or reference,
- Phone message slips,
- Announcements of social events

Records communicated via Remote Access will be disposed of within the record keeping system in which they have been filed in accordance with {the Records Disposition Authorization (RDA) approved by State Archives and Records Administration (SARA). Program managers should consult with the Agency Records Management Officer concerning RDAs applicable to their program's records}.

3.6 Definitions and Terminology

The following table defines the terms used to describe the various devices, entities or groups within this document.

The Network or Enterprise Network	MDOT and TBU network components.
Remote Access User	MDOT or TBU Employee/Contractor or Government Employee who has a job related/defined requirement to access the MDOT and TBU networks from a remote location.
Internet Users	Any remote access user connecting to the Enterprise network via an Internet Service Provider broadband connection from the Internet.
Transportation Business Units	The MDOT Transportation Business Units are defined as MDOT HQ (TSO), MAA, MDTA, MPA, MTA, MVA, SHA
MDOT	All TBUs (MDOT HQ, MAA, MDTA, MPA, MTA, MVA, SHA) within the organizational structure of the MD Dept. of Transportation.
User's Supervisor	The User's Organizational Group Supervisor

IT COTR (Information Technology Contracting Officers' Technical Representative)	The IT COTR for one of the following organizational groups: MDOT HQ, MAA, MDTA, MPA, MTA, MVA, SHA
Remote Access Administrator	The individual(s) designated as the Remote Access Administrator(s) for one of the following organizational groups: MDOT HQ, MAA, MDTA, MPA, MTA, MVA, SHA
NOC	The MDOT Network Operations Center (NOC).
INFOSEC	The Information Security group within MDOT and its contractor

3.6.1 MDOT Remote Access Categories

Remote Access – Network Connection

This refers to remote access to the MDOT and TBU network that provides a direct connection to the network. This access requires two-factor authentication.

Remote Access – Service Access

This refers to remote access to the MDOT and TBU services and applications contained on the internal network. This access is offered through SSL connection via the MDOT Secure Portal (a form of secure reverse proxy)

Section 4: Password Policy

4.1 Purpose

The purpose of this policy is to insure when choosing a password, that it is extremely difficult for a potential intruder to make educated guesses about the selected password. This leaves the intruder no alternative but a brute-force search, trying every possible combination of letters, numbers, and punctuation. A search of this sort, even conducted on a computer trying one million passwords per second (most machines can try less than one hundred per second), would require, on the average, over one hundred years to complete. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO. In the event of a conflict between State, MDOT or TBU policy, the most stringent shall apply.

4.2 Scope

This policy applies to all MDOT employees, staff subordinate to MDOT contracts, as well as any individual using MDOT resources. This policy applies to passwords required for all network and computer systems. Any device that requires an exception to this policy must be submitted and approved by the SWG.

4.3 Policy Statement

User accounts are provided for the purpose of conducting the business of this Agency and supporting the mission of each department. Computers and networks provide access to local and remote resources, as well as the ability to communicate with other users worldwide. Such open access is a privilege requiring individuals to act responsibly. Users must respect the rights of other users, the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

4.4 Responsibilities

Agency executive management will ensure that program unit management and unit supervisors implement the policy. Each staff member with supervisory responsibilities must ensure that their subordinates are aware of their rights and obligations under this policy. The unique needs of each TBU's business and technical environments may include additional guidance as long as it is consistent with and meets the minimum requirements of State policies, standards and guidelines as well as regulatory mandates, such as Payment Card Industry (PCI), and the requirements of other agencies MDOT interfaces with, such as the U.S. Department of Justice, Federal Bureau of Investigation – "CJIS Security Policy". TBU executive management will ensure that program unit management and unit supervisors implement the policy.

4.5 Guidance

The following are general password policies applicable for most systems and must be implemented if the system (operating system or software application) supports it:

Passwords and User IDs are unique to each authorized user.

Passwords for users-consist of a minimum of 8 alphanumeric characters (no common names or phrases). There shall be computer-controlled lists of prescribed password rules. Periodic testing to identify any password weaknesses (e.g., letter and number sequences, character repetition, initials, common words, and standard names) must be performed at least on a yearly basis where applicable.

The root or administrator account has a minimum password length of 11 characters.

Passwords are not the same as the User ID.

Passwords must not consist of all numbers, all special characters, or all alphabetic characters.

Users, Root and Administrators have at least one non-letter character in their password.

Passwords are changed every 45 days for users and every 30 days for system administrators. Most systems can enforce password change with an automatic expiration and prevent repeated or reused passwords.

Password history does not allow users to reuse any password in his/her last 10 attempts.

User accounts disabled after 4 consecutive failed login attempts.

Sessions suspended or locked by means such as a password-protected screensaver after 15 minutes of inactivity and require the password to be reentered to resume the session.

User accounts are disabled after 60 days of inactivity and deleted after 90 days of inactivity unless exempted by the TBU COTR or a manager of the TBU COTR.

User accounts are removed or disabled within 72 hours after notice to the TBU COTR that there has been termination of employment of the user.

Where applicable, successful logons should display the date and time of the last logon and logoff.

Users not allowed to use common passwords and passwords must not be based on personal information, i.e. username, social security number, children's names, pets' names, hobbies, anniversary dates, etc.

Passwords are kept private i.e., not shared, coded into programs, or written down.

When an employee has a change in job duties and no longer needs access to a system, the account will be removed immediately.

4.5.1 Acceptable Use

Computers and networks are provided for the purpose of conducting the business of this Agency and to support the mission of each department. The following list, although not all-inclusive, provides some examples of acceptable use:

- Communication with federal, state or local government personnel, vendors and other private businesses;
- Communication and information exchange for professional development or to maintain knowledge or skills;
- Activities involving State association, government advisory or standard activities;
- Communications for administrative purposes
- Group or shared ids are prohibited unless they are documented as Steady State Accounts or Functional ID's. Steady State Accounts, Functional ID's are user accounts associated with a group or role that may be used by multiple individuals (e.g., Emergency Problem/Fix Ids) or that are associated with a particular production job process (e.g., ACF2 id used to run production jobs). Passwords associated with functional ids are exempt from the password sharing and change requirements specified above

4.5.2 Restrictions

MDOT services may not be used for unlawful activities, commercial purposes not under the auspices of this Agency, personal financial gain, or personal use inconsistent with guidelines contained in this policy, or uses that violate other State policies or guidelines.

4.5.3 Representation

Users shall not give the impression that they are representing, giving opinions or otherwise making statements on behalf of MDOT or any unit of the State unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing the MDOT or State

4.5.4 Interference

Services provided to MDOT shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities, or unwarranted or solicited interference with others' use of the systems provided

4.5.5 No Expectation of Privacy

Privacy of services such as email is not guaranteed. Authorized State employees may access and disclose the contents of all messages created, sent or received using the services provided by MDOT. The State affords electronic mail privacy protections comparable to that which it traditionally afforded paper mail and telephone communications within the context of the State's legal and other obligations.

4.5.6 Security

Password security is the complete and sole responsibility of each individual. Users must take all reasonable precautions to prevent the use of the account by unauthorized individuals.

No user will be required to disclose his or her password.

Systems may be reviewed on a periodic basis to ensure the password policy compliance is being enforced.

4.5.7 Records Retention

State Records communicated electronically must be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed and accessible in an existing filing system in accordance with each Department's standard practices.

Section 5: External &Third-Party Networks Policy

5.1 Purpose

The purpose of this policy is to describe the "permitted uses", connection methods, and security controls for external (public) and remote, Third Party Networks connecting to the Maryland Department of Transportation (MDOT) network and devices.

The MDOT network allows access from the public to connect to their public servers that are located in the DMZ or service network. The DMZ (demilitarized zone) is a section of the network that resides between the public (untrusted) and the internal (trusted) network. Publicly accessible servers such as Web servers and FTP servers reside in the DMZ.

Third Party Networks are defined as networks that are not part of MDOT, or their network address space, requiring remote connectivity and access to devices within the MDOT Network. This policy also applies to Virtual Private Network (VPN) connections from MDOT to a Third-Party Network for accessing resources on their network. This policy requires that all Third Party Network connections will require the submission of a Remote Access Form as defined the in the guidance of Section 4, Remote Access Policy of the MDOT Security Plan. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO.

5.2 Scope

This policy applies to all MDOT employees, staff subordinate to MDOT contracts, and to any individual using MDOT resources. This policy applies to all agencies and organizations connecting to the MDOT network.

5.3 Policy Statement

Network services are provided for the purpose of conducting the business of this Department and supporting the mission of each Transportation Business Unit (TBU). Computers and networks provide access to local and remote resources as well as the ability to communicate with other users worldwide. Such access is a privilege and requires that individuals act responsibly and observe all relevant laws, regulations and contractual obligations. All Third Party or External Networks are considered or assumed to be un-trusted and are subject to review and compliance with the requirements specified in this policy.

5.4 Responsibilities

Each TBU is responsible for developing policy that is entirely consistent with this MDOT policy, or adopting this policy as the TBU policy. The unique needs of each TBU's business

and technical environments may include additional guidance as long as it is consistent with and meets the minimum requirements of State policies, standards and guidelines as well as regulatory mandates, such as Payment Card Industry (PCI), and the requirements of other agencies MDOT interfaces with, such as the U.S. Department of Justice, Federal Bureau of Investigation – "CJIS Security Policy". TBU executive management will ensure that program unit management and unit supervisors implement the policy.

5.5 Guidance

In strictly controlled situations, MDOT will allow Third Parties to access MDOT internal networks and computer systems. Both the owner of the MDOT information to which the Third Party will be granted access and the Third Party's Management Representative, must agree in writing, to such access before it is established. The Management Representative from the Third Party is also obligated to sign the MDOT Network Connection Terms and Conditions for Third Party Network Access" disclaimer (Appendix C). The decision-making process for granting such access includes consideration of the controls on the systems to be connected, the Third Party's security policies, and a network diagram of the relevant network segment(s) that will be connected to MDOT. The diagram, to be provided by the Third Party or developed internally must include the IP addresses, protocols, and equipment relevant to the connection.

MDOT will terminate the connection of Third Party network to the MDOT network at the conclusion or termination of a contract or project or at any such time that the connection is no longer required. With the approval of the Department CIO, MDOT reserves the right to terminate any connection in which a security breach is believed to be occurring or has occurred and corrective action has not been taken that meets the requirements of MDOT.

5.5.1 Acceptable Use

All network traffic passed from external networks must pass through an MDOT firewall. The following methods are accepted for permitting traffic from the public or Third-Party networks to MDOT's network:

Private leased line: A private leased line (e.g., frame relay, CCT1, TLS, etc.) can be connected from a Third-Party network to the MDOT vendor service network. The Third-Party network will be responsible for purchasing and providing the leased line service to include the circuit and associated hardware (routers, CSU/DSUs, cables, etc.) to establish the connection outside the MDOT network. Third Party responsibilities shall also include installation, maintenance, and problem solving of the network circuit and hardware. Network devices are preferred to be rack mountable. Device must be SNMPv2 manageable. Third Party is requested to provide MDOT, at a minimum, a read-only SNMPv2 Community String to permit device monitoring (CPU, memory, interfaces, etc.) by the MDOT Network Operation Center (NOC) network management tools. MDOT personnel are responsible for implementing the appropriate changes to the MDOT router(s) and MDOT firewall configuration to allow the traffic from the Third-

Party network to the entities within the MDOT network that is needed. Any data being passed through a private leased line that is deemed sensitive or critical must be encrypted. MDOT provides no security management of Third Parties connecting to this shared vendor service network. Vendors should provide their own security of that connection.

Internet from Third Party Networks: Any traffic being passed from the Third-Party network to MDOT using the Internet requires encryption. MDOT will require a Virtual Private Network (VPN) tunnel to be established from the Third-Party network to the MDOT enterprise firewall or to a VPN device/product used exclusively for that system approved by MDOT. The VPN must be established in one of the following methods: (a) firewall-to-firewall, (b) approved VPN client software to MDOT firewall, or (c) approved router to MDOT firewall. The VPN must employ IPSEC encapsulation; AES-256 encryption (Advanced Encryption Standard) and SHA5 hashing algorithm are required unless otherwise approved by the MDOT Security Working Group.

5.5.2 Internet from the public

All access from the general public to MDOT public servers must be terminated at the DMZ. The firewall must be configured to direct all traffic (including http/https) from the general public or from Third Party Networks only to the DMZ, creating a separation of the DMZ from the internal network. Any Web server in the DMZ that accepts or processes credit card payments are subject to PCI compliancy restrictions.

Network access granted by MDOT to the Third-Party network is restricted to only the hosts, protocols, and ports that are needed by the Third Party network in order to support their project or contract requirements. The Third-Party network is responsible for providing MDOT with this information in writing. All configuration changes made to MDOT network hardware or software are subject to review and approval of the MDOT Change Advisory Board (CAB). The MDOT CAB meets weekly to review and approve/disapprove network configuration updates.

Access granted from the public to servers in the MDOT DMZ are restricted to only the hosts and basic protocols that are required. All configuration changes needed for access from the public to the DMZ are subject to the review and approval for the MDOT CAB. Public servers in the DMZ are assigned a public IP address registered to MDOT which is translated to a private IP address assigned for the MDOT DMZ.

5.5.3 Acceptable and Prohibited Cryptographic Protocols and Cipher Suites

Cryptographic protocols are protocols that are designed to provide and assure secure communications offering privacy and encryption of data. The combination of authentication, encryption, message authentication code (MAC) and key exchange algorithms that are used to negotiate the security settings for the cryptographic protocol is called a *cipher suite*. Over the course of time, protocols and cipher suites are

strengthened as hacking becomes sophisticated, thus older protocols are no longer recommended and supported. MDOT follows this paradigm to assure that a low risk factor exists in our network.

The following cryptographic protocols are not permitted in MDOT:

SSLv2, SSLv3, SSHv1

The TLSv1 cryptographic protocol is currently allowed but not preferred by MDOT. The following cryptographic protocols are permitted in MDOT:

TLS1.1, TLS1.2

The following weak cipher suites are not permitted in MDOT:

RC4, MD4, MD5, export-grade cipher suites

5.5.4 Representation

Third Parties shall not give the impression that they are representing, giving opinions or otherwise making statements on behalf of MDOT, TBU, or any unit of the State unless appropriately authorized to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing MDOT or the State.

5.5.5 Interference

Services provided to MDOT and its TBUs shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive demand on any network resource or computing facilities, or unwarranted or unsolicited interference with others' use of the systems provided.

5.5.6 No Expectation of Privacy

Privacy of services and communications, such as email, is not guaranteed. Authorized State employees may access and disclose the contents of all messages created, sent or received using the services provided by this Agency. The State does afford electronic mail privacy protections comparable to that which it traditionally affords paper mail and telephone communications within the context of the State's legal and other obligations.

5.5.7 Security

As a condition of access to MDOT's computer network, every Third-Party network must secure its own connected systems in a manner consistent with MDOT's requirements. MDOT reserves the right to immediately suspend network connections with Third Party systems not meeting such requirements or if security concerns arise, until those requirements are met.

All Third Party external network connections will be brought before the MDOT Security Working Group for review and approval. MDOT reserves the right to perform a network vulnerability assessment (scan) of any mission critical hosts on the Third-Party network after providing prior written notification of MDOT's intent to do so and specify a time range during which the scan will occur.

Routing of any private Internet Protocol addresses is prohibited. A private IP address is defined in RFC 1918, in which the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private Internets:

10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Public IP addresses are defined as those that have been legally registered through the InterNIC. MDOT will not route their registered IP addresses assigned to internal hosts over the Internet.

5.5.8 Records Retention

State Records must be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed and accessible in an existing filing system in accordance with each Department's standard practices.

Records communicated via Email are disposed of within the record keeping system in which they have been filed in accordance with [the Records Disposition Authorization (RDA) approved by State Archives and Records Administration (SARA). Program managers should consult with the Agency Records Management Officer concerning RDAs applicable to their program's records.

Section 6: Kiosks Security Standards

The following standards should be followed whenever possible and if the facility can accommodate them.

6.1 Operating System Security

A. Password Protect the BIOS (8-character minimum, (larger when possible).

B. Operating System should the latest possible release of Windows whenever possible.

C. Operating System should auto-logon with a user account that has a password that adheres to the MDOT Security Policy for password complexity

D. The Administrator account should be renamed.

E. Block Internet access[3], assign a static IP address to Kiosk and remove DNS.

F. Create a Kiosk user profile and augment with policy editor.

1. Remove Run command from Start menu.
2. Remove folders from Settings on Start menu.
3. Remove Taskbar from Settings on Start menu.
4. Remove Find command from Start menu.
5. Hide drives on My Computer
6. Hide Network Neighborhood
7. Hide all items on Desktop
8. Disable Shutdown Command
9. Disable Registry Editing Tools

6.2 Physical Security

A. Configure switch port to only accept MAC address of Kiosk PC.

B. Bolt Kiosk in place.

C. Secure Kiosk access panels with commercial grade lock.

[3] When business reasons call for internet access, the MDOT Change Process will be followed to assure the necessary mitigation takes place.

D. Network cable should be placed in a conduit (ex. Greenfield) if the cable can't be run through the floor under the Kiosk.

E. Network cable should be permanently attached to the jack or encased in a strong locked cover if it is accessible.

F. Request the Kiosk to be placed in view of a security camera.

G. A physical site assessment must be performed by the MDOT Information Security team before the kiosk is approved for production and public accessibility. This must be noted in the Maximo Service Request. A letter stating the customer's knowledge of the visit and an attempt being made to challenge existing security procedures will be provided to the INFOSEC team doing the visit and signed by the customer.

Sample Customer Acknowledgement Letter.

October 09, 2013

To Whom It May Concern:

The MDOT (insert TBU name) has engaged personnel listed below to perform a vulnerability assessment and analysis beginning on MM/DD/YYYY and completing on MM/DD/YYYY. In the process of conducting this authorized exercise, the authorized personnel will ignore or challenge existing TBU and MDOT system security procedures as necessary to ensure that an effective assessment is performed. To verify the validity of this letter and authorized personnel, please check with the primary contact listed for the facility. If the primary contact cannot be located, please call [applicable client personnel and telephone number(s)] for verification.

This assessment is being performed at (list locations and/or list of network addresses)

AUTHORIZED PERSONNEL

NAME
NAME

LOCATION (S)	**PRIMARY CONTACT (S)**
As Applicable	As Applicable

Thank you for your cooperation.

Signature

Name of Client Authorized Manager

Title /Position
Telephone Number
Address

Section 7: Internet Web Hosting Policy

7.1 Purpose

The purpose of this policy is to maximize the security of Web servers that are connected to the Internet and provide public information access. The focus is on the policies and procedures that must be in place to support any technical security features for the implementation and daily maintenance of Web servers. Without implementing proper security procedures, Web servers can be attacked directly, or used as jumping off points to attack an organization's internal networks. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO.

7.2 Scope

This policy applies to all Internet Web server systems that are being built or in working condition regardless of whether they are hosted within MDOT or by a Third Party. Close attention should be made not only to the Web server itself, but also the security needs and requirements of the local network and other interconnected networks. In the case of collaborative efforts between MDOT and another governmental entity, MDOT management shall exercise due diligence to ensure that the intent of this policy is adhered to by the hosting party.

7.3 Policy Statement

There are many areas of Web servers to secure such as the underlying operating system, the Web server software, server scripts, and other associated components. All Agency Web servers that are accessible from the Internet must adhere to the following standards for operation and maintenance:

7.3.1 MDOT Hosting Policy:

1. Information placed on any Web site is subject to the same privacy restrictions as releasing non-electronic information. Accordingly, before information is placed on the Internet, it must be reviewed and approved for release in the same manner as other official memos, reports, or other official non-electronic information.

2. A public Web server must not serve as a repository for confidential data, although it can act as a proxy for access to confidential data located on more secure hosts.

3. Users are forbidden to download, install or run Web server software without prior approval by the user's Agency authorized system administrator.

4. Any control of Web servers must be done from the console or properly secured remote sessions by authorized administrators using encryption.

5. Web server software and the underlying operating system must employ all security patches and configuration options appropriate to the environment in which it is operating. Security patches must be maintained continually and all unnecessary services must be disabled.

6. Place Web servers on subnets separate from internal networks.

7. Firewalls and routers must be in place and configured to restrict attacks from public and internal networks as well. Only traffic needed for browsing and business applications management is allowed through the firewall to access that server.

8. Since using a computer simultaneously as a public Web server and for other public Web services poses risks, a computer must be dedicated to the sole function as a Web Server. Specifically, business or personal files are vulnerable to a malicious Web user if access is gained to a directory on your computer.

9. Keep the computer free of any networked or shared drives to another system. Access to remote machines opens an avenue for a malicious user to breach security.

10. Locate the computer in a physically secure area and restrict access to it by assigning passwords to authorized users. Ensure MDOT password policy is followed.

11. System administrators and security personnel must have defined responsibilities and authority to examine file systems on a regular basis for any unexpected changes. A review of logs on a regular basis by authorized personnel to record and report anomalies to your organization's designated security point of contact is desirable.

12. Procedures for Web server users to report any dramatically unexpected changes on the Web site to system administrators or your organization's designated security point of contact must be in place.

13. An MDOT-approved Third Party will perform Web server security assessments bi-monthly unless unforeseen events require immediate assessment. Also, security assessments must be accomplished after configuration changes such as operating system patches, web page script changes (not page content), etc. The Modal COTR and/or IT Manager will be informed before the assessment is done and receive a copy of the results.

7.3.2 Third Party Hosting Policy:

MDOT hosting policies in sub-paragraphs 1, 2, 5, 7, 9, and 10 of paragraph 9.3.1 above also apply to Third Party Hosts. In addition, the following policies also apply:

1. Procedures for Web server users to report any dramatically unexpected changes on the Web site to system administrators or your organization's designated security point of contact must be in place. The Third-Party Host must be able to take off-line any portion of the Website that has been compromised.

2. The State will contract a Third Party to perform Web server security assessments after the initial assessment, at the discretion of MDOT, unless unforeseen events require immediate assessment. The Third-Party Host will provide written authorization for MDOT to perform these security assessments as part of the original contract. Also, security assessments must be accomplished after configuration changes such as operating system patches, web page script changes, etc. The Modal COTR, IT Manager and Third-Party Host will be informed before the assessment is done and receive a copy of the results.

3. Non-compliance with policy directives may result in revocation of the Web Hosting contract. Additionally, MDOT content will be removed from the server and MDOT will retain the rights to the domain name.

7.4 Responsibilities

Agency executive management will ensure that program unit management and unit supervisors implement policy.

7.5 Guidance

This section establishes "high level" guidelines and standards supporting the agency policy. Guidelines are recommendations derived from best practices or experiences. Detail level implementing guidelines and procedures should not be included in the policy but should be contained in supporting documentation and referenced. Standards are mandatory requirements, which may be included in the policy text or supporting documentation and appropriately referenced. Electronic links must be provided whenever practical.

Agencies must consider addressing the following areas in the Guidelines section of their policy:

7.5.1 Security

Web server engineers or system administrators must not disclose any server structure or working information to any unauthorized personnel. All authorized personnel, whether State employees or Contractors, must sign a Non-Disclosure Agreement.

7.5.2 Records Retention

State Records communicated electronically must be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed and accessible in an existing filing system in accordance with each Department's standard practices. Retention of those records is the responsibility of the record owner.

Section 8: Intranet Web Hosting Policy

8.1 Purpose

The purpose of this policy is to maximize the security of Web servers that are connected to an Intranet. The focus is on the policies and procedures that must be in place to support any technical security features for the implementation and daily maintenance of the Web servers. Without implementing proper security procedures, Web servers can be attacked directly, or used as jumping off points to attack an organization's internal networks. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO.

8.2 Scope

This policy applies to all Intranet Web server systems that are being built or in working condition regardless of whether they are hosted within the MDOT or by a Third Party. Close attention is required for the Web server as well as the security needs and requirements of the Intranet since they frequently house sensitive corporate information not intended to be viewed by anyone outside the Agency. Intranets clearly illustrate how challenges to security are not so much technical as they are procedural.

8.3 Policy Statement

There are many areas of Web servers to secure including the underlying operating system, the server software, server scripts, and other associated components. Noteworthy, Intranets require strict internal security policies and procedures to control access to sensitive corporate data from within. Even though Intranet Web servers are not accessible from the Internet, they remain susceptible to the same attacks including penetrations from the Internet via other systems on the "inside network", and also through Internet Web browsing from the server. All Agency Web servers must adhere to the following standards for operation and maintenance:

1. Information placed on any site is subject to the same privacy restrictions when releasing non-electronic information. Accordingly, before information is place on the Intranet, it must be reviewed and approved for release in the same manner as other official memos, reports or other official non-electronic information.

2. Users must not run Web server software without prior approval by a user's Agency-authorized System Administrator.

3. Any control of Web servers must be done from the console or properly secured remote sessions by authorized administrators using encryption.

4. Server software and the underlying operating system must employ all security patches no later than one month of release and configuration options appropriate to the environment in which it is operating. Security patches must be maintained continually and all unnecessary services must be disabled.

5. Locate the computer in a physically secure area and restrict access to it by assigning passwords to authorized users.

6. System administrators and security personnel must have defined responsibilities and authority to examine file systems on a regular basis for any unexpected changes. Additionally, authorized personnel must review logs regularly to record and report anomalies to your organization's designated Security Officer.

7. Procedures for Web Server users to report any dramatically unexpected changes on the site to system administrators or your organization's designated Security Officer must be in place.

8. A Third Party will perform Web server security assessments annually unless unforeseen events require immediate assessment. Also, security assessments must be accomplished after configuration changes such as operating system patches, web page script changes, etc. The Modal and/or IT Manager will be informed before the assessment is done and receive a copy of the results.

8.4 Responsibilities

Agency executive management will ensure that program unit management and unit supervisors implement policy.

8.5 Guidance

This section establishes "high level" guidelines and standards supporting the Agency policy. Guidelines are recommendations derived from best practices or experiences. Detail level implementing guidelines and procedures should not be included in the policy but should be contained in supporting documentation and referenced. Standards are mandatory requirements, which may be included in the policy text or supporting documentation and appropriately referenced. Electronic links must be provided whenever practical.

Agencies must consider addressing the following areas in the Guidelines section of their policy:

8.5.1 Security

Web server engineers or system administrators must not disclose any server structure or working information to any unauthorized personnel. All authorized personnel, whether State employees or Contractors, must sign a Non-Disclosure Agreement.

8.5.2 Records Retention

State Records communicated electronically must be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed

and accessible in an existing filing system in accordance with each Department's standard practices. Retention of those records is the responsibility of the record owner.

Section 9: Wireless Communication Policy

9.1 Purpose

The purpose of this document is to define a policy for securing wireless connections within MDOT's network. Due to the inherently insecure nature of this technology, only secure wireless systems that meet the requirements in this policy are approved for connection to the MDOT network. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO.

9.2 Scope

This policy applies to all MDOT employees, and staff subordinate to MDOT contracts. It is recommended that the "Policy Statement" be included in any contract award process. This policy covers all wireless networking devices (e.g., Wireless Access Points, bridges, computing devices, etc.) connected to any of MDOT's internal networks. Wireless devices and/or networks without any connectivity to MDOT's networks do not fall under the purview of this policy.

9.3 Policy Statement

Computers and networks provide access to MDOT and remote resources, as well as the ability to communicate with other users worldwide. The security and integrity of this network must be upheld when utilizing wireless networking devices on the MDOT network.

In keeping with State of Maryland Department of Information Technology (DoIT) policy (Version 2.2) regarding Wireless (section 7.8), the following guidance will be observed:

- Establish a process for documenting all wireless access points
- Ensure proper security mechanisms are in place to prevent the theft, alteration. Or misuse of access points
- Restrict hardware implementation to utilize Wi-Fi certified devices that are configured to use the latest security features available
- Change default administrator credentials
- Change default SNMP strings if used, otherwise disable SNMP
- Change default SSID
- Deploy secure access point management protocols and disable telnet
- Strategically place and configure access points so that the SSID broadcast range does not exceed the physical perimeter of the building (unless the wireless solution is designed for providing outside connectivity).
- Require wireless users to provide unique authentication over encrypted channels if accessing internal LAN services

- Require wireless users to utilize encrypted data transmission if accessing internal LAN services

This MDOT/MDTA Wireless Communication Policy provides this additional guidance:

- No wireless access points shall be connected to the MDOT network without following the MDOT Change Management process.
- No end user device connected to the MDOT network (either wired or wireless) shall offer or allow connections to or from other networks
- No end user device will broadcast MDOT SSIDs or otherwise masquerade as a device providing connections to the MDOT network
- No MDOT wireless network management interfaces shall be accessible from the wireless network
- Wireless networks providing access to internal MDOT resources require WPA2 (Wi-Fi Protected Access - Enterprise) with two factor authentication.
- Wireless networks providing guest access to the Internet shall implement WEP (Wired Equivalent Privacy) at a minimum.
- Guest wireless network accounts will be unique and will be configured to expire passwords after eight hours. Exceptions to this policy must follow the MDOT Change Management process. For example, a one-week training class requiring guest wireless access may require an exception to the policy.

9.4 Responsibilities

Each Agency is responsible for developing procedure that is entirely consistent with this MDOT policy. The unique needs of each Agency's business and technical environments may include additional guidance as long as it is consistent with and meets the minimum requirements of MDOT policies, standards and guidelines. Agency executive management will ensure that program unit management and unit supervisors implement the policy.

9.5 Guidance

All wireless networking devices providing a wired connection to the MDOT network must have approval from the Security Working Group and be submitted for review via the Change Management process prior to being connected to the MDOT network. Due to the highly evolving nature of this technology, an MDOT Wireless Standards document (see Appendix D) will be kept on an on-going basis that contains current MDOT implementations of these technologies, known issues, and recommendations.

Wireless devices found to be non-compliant with this or other appropriate policies (ie. Remote Access Policy, Email and Internet Use Policy) will have their connection terminated **immediately**.

Section 10: Secure FTP Policy

10.1 Purpose

The purpose of this policy is to support the appropriate use of secure and non-secure FTP access privileges for both MDOT and external users. Well designed and properly managed systems expedite business communications, reduce paperwork, and automate routine office tasks thereby increasing productivity and reducing costs. This policy is considered sensitive information and should not be shared outside of MDOT/MDTA without the expressed written permission of the MDOT CIO.

10.2 Scope

This policy applies to an individual, government agency, or business-trading partner who has been given authorization to access the Maryland Department of Transportation (MDOT) Secure FTP Server from a remote site. This policy applies to all MDOT/MDTA Modal Agencies operating as part of the Maryland Department of Transportation. Amendments, changes and/or additions to this policy will follow a structured review and approval process.

10.3 Terminology

The following table defines terms used to describe various devices, entities and groups within this document:

The Network or Enterprise Network	The combined MDOT Network and associated MDTA Network components.
Secure FTP Server	Private transfer file transfer system offering enterprise grade security.
MDOT	Maryland Department of Transportation
MDTA	Maryland Transportation Authority
NOC	Maryland Department of Transportation Headquarters
CCB	Configuration Control Board
CIO	Chief Information Officer
CCR	Configuration Change Request
DPPA	Driver's Privacy Protection Act
FTP	File Transfer Protocol

RDA	Records Disposition Authorization
SARA	State Archives and Records Administration

10.4 Policy Statement

Secure FTP access is made available for users and entities that are responsible for policy review, approval, implementation, enforcement, as well as equipment procurement and maintenance. Computers and networks provide access to remote resources, as well as the ability to communicate with other users worldwide. Open access is a privilege and requires that individuals act responsibly. Users must respect the rights of other users as well as the integrity of the systems, related physical resources, relevant laws, regulations and contractual obligations.

MDOT HQ and the Configuration Advisory Board (CAB) are responsible for approving; implementing and enforcing the MDOT/MDTA Secure FTP Access Policy. The request is submitted to the Security Working Group for discussion and review. If agreed upon, the request is presented to the CAB. When accepted by the CAB, the request is presented to the IT Modal managers and, upon approval, is incorporated into this policy.

Secure FTP Access Policy is developed by the MDOT HQ sanctioned Security Working Group and submitted to MDOT CIO and the corresponding CCB for interim approval. The MDOT CIO will present the proposed policy to the IT Modal Managers/IT Teams for final review and approval.

Approved Secure FTP access Policy is implemented under the direction of the MDOT HQ and the CAB and consists of tracking the approved Change Requests (CRs), ensuring that approved work is progressing on the CAB schedule.

10.5 Responsibilities

Agency executive management will ensure that program unit management and unit supervisors implement policy. Individuals with supervisory responsibilities must ensure that their subordinates are aware of their rights and obligations under this policy. The following sections define the Secure FTP Access responsibilities of the individuals listed below:

- Secure FTP access User
- System Administrator
- Secure FTP Access Administrator
- NOC Help Desk

10.5.1 Secure FTP Access User

Secure FTP Access Users are defined as business trading partners who require secure FTP access to the MDOT/MDTA Secure FTP Server.

If required, the Secure FTP user is responsible for obtaining the Request Form from the prospective MDOT/MDTA Modal Agency, completing and signing the first section of the Secure FTP access Request Form, and forwarding it to the Agency's Project Coordinator. Modal Agencies may assign this responsibility to their Project Coordinators.

The Secure FTP Access User is responsible for reporting Secure FTP access Client or Application Software problems to the appropriate Help Desk.

The Secure FTP access User is responsible for all system hardware and software maintenance to their personal computer. MDOT and MDTA are not responsible for the condition of the secure FTP access User's personal computer.

10.5.2 System Administrator

The Agency's System Administrator is responsible for reviewing the Secure FTP Access Request Form to ensure that the user has completed and signed the portion of the form designated for the user.

The System Administrator authorizes the request by signing the FTP Access Request Form and specifying the types of access the User will be granted. The Secure FTP Access Administrator who updates access controls processes the form.

10.5.3 Secure FTP Access Administrator

The Secure FTP Access Administrator is responsible for the following:

- Coordinating activities associated with the Secure FTP access Request Form. He/she ensures the information on the form is correct and signed by both the user and the Agency's System Administrator.
- Providing the NOC Help Desk with the information required in creating Secure FTP access directories. In this case, the Secure FTP Access Administrator faxes a copy of the Secure FTP access Request Form to the NOC Help Desk.
- Providing the User with passwords, configuration information, installation software, and manuals, required to access the Secure FTP Server remotely.
- Providing training to the Agency's Project Coordinator on the use of applications required for Secure FTP access, if required.
- Maintaining a file containing the signed copies of the Secure FTP Access Forms.
- Notifying the Agencies Project Coordinator when the account is setup.

10.6 NOC Help Desk

The NOC will provide priority level "Critical" support for Secure FTP Server specific problems as contractually agreed to with MDOT.

10.7 Guidance

A User wanting to access the MDOT Secure FTP Server must obtain authorization from the prospective MDOT Modal Agency. The User can obtain the Secure FTP Access Request Process from the Agencies FTP Access Administrator.

The Secure FTP client should complete, sign and return the following documents, if required by the Modal FTP Administrator:

- The Agency's FTP Driver's Privacy Protection Act (DPPA) compliance contract, which outlines the Users responsibilities under the Federal DPPA.
- Third Party External Communications Network Security Policy and MDOT Network Connection Terms and conditions for Third Party networks.
- The Agency's FTP Access Request Form.

Upon receipt and approval of the signed Secure FTP Documents, each Modal will transmit in a responsible and secure process, the Account User ID and password to either internal or external Users depending upon the location of the User. After the User signs on and modifies the default password, he/she should perform a verification test. Directions will be provided on whom to contact for lockouts of User ID and passwords if applicable.

10.8 Acceptable Use

Access to Secure FTP is provided for the purpose of conducting the business of and to support the mission of each department of MDOT. The following list, although not all-inclusive, provides some examples of acceptable use:

- Communication with Federal, State or Local Government personnel, vendors, and other private businesses;
- Communication and information exchange for professional development or to maintain knowledge or skills;
- Activities involving State-association, Government-advisory, or standards;
- Communications for administrative purposes.

10.9 Restrictions

Secure FTP access may not be used for unlawful activities, or uses that violate other State policies or guidelines. The latter include, but are not limited to, policies and guidelines regarding intellectual property or regarding sexual or other forms of harassment. The following list, although not all-inclusive provides some examples of unacceptable use of Secure FTP access:

- Engaging in any illegal or wrongful conduct, including communications which violate any laws or regulations, including copyrights, patent protections, license agreements, or other intellectual property rights of third parties;
- Transmitting threatening, obscene, defamatory, fraudulent or harassing messages, even as a prank;
- Use for any purpose that is against State or Public policy or contrary to the State's best interest;
- Intentionally seeking information about, obtaining copies of, or modifying files, other data, or passwords belonging to other users, unless explicitly authorized to do so by those users;
- Attempts to gain unauthorized access to any information facility, whether successful or not. This includes running programs that attempt to calculate or guess passwords, or that are designed and crafted to trick other users into disclosing their passwords. It also includes electronic eavesdropping on communications facilities;
- Any action that invades the privacy of individuals or entities that are the creators, authors, users, or subjects of information resources;
- Misrepresenting in any manner, your identity, your account or a computer in electronic communication;
- Knowingly sharing a personal account;
- Interfering with or disrupting network users, services, or equipment. Such disruptions could include, but are not limited to (1) distribution of unsolicited advertising or messages, (2) propagation of computer worms or viruses, and (3) using the network to gain unauthorized entry to another machine on the network;
- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojan horses, and worms;
- Unauthorized Disclosure of confidential or proprietary information.

10.10 Representation

Secure FTP Access Users shall not give the impression that they are representing, giving opinions or otherwise making statements on behalf of MDOT or any unit of the State unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing this Agency or State.

10.11 Interference

Secure FTP access shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities or unwarranted or unsolicited interference with others' use of Secure FTP access systems. Such uses include, but are not limited to chain letters, "Spam", "letter-bombs", and willful transmission of known computer viruses or other agents that are engineered to damage system resources, or could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities.

10.12 No Expectation of Privacy

Privacy of Secure FTP Access is not guaranteed. Authorized State Employees may access and disclose the contents of all messages created, sent or received using the MDOT/MDTA Secure MDOT/MDTA Secure FTP Server.

10.13 Security

The following specific guidance relating to Secure FTP access security is provided:

- **Encryption**

All external users connecting to the Secure FTP server will use a minimum of 128-bit encryption. The server will only allow connections with 128-bit encryption or better if originating from an external network.

- **Disclaimer**

Modal Secure FTP Access Users are defined as Government Agencies or Businesses who require secure FTP access to the MDOT Server. Access to the MDOT Secure FTP server is considered a privilege.

MDOT assumes no responsibility for any hardware, operating system, or software application problems encountered by any MDOT Modal Secure FTP Access User when installing/using the designated security applications to connect to the MDOT Secure FTP Server.

10.14 Records Retention

Files transferred using Secure FTP access must be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Files

needed to support program functions should be retained, managed, and accessible in an existing filing system outside the Secure FTP access system in accordance with each Department's standard practices.

Records transferred via Secure FTP access will be disposed of within the record keeping system in which they have been filed in accordance with {the Records Disposition Authorization (RDA) approved by State Archives and Records Administration (SARA). Program managers should consult with the Agency Records Management Officer concerning RDAs applicable to their program's records}.

10.15 Secure FTP Access Administrators

Each Modal /Agency will assign their own Secure FTP Access Administrator.

Section 11: Vulnerability Assessment Scan Policy

11. 1 Vulnerability Assessment Scanning

11.1.1 Responsibilities

The Office of Transportation Technology Services (OTTS) IT Security office or the network managed services (NMS) contractor will perform server vulnerability assessment (VA) scans on a regular basis (scheduled or on request) unless unforeseen events require immediate assessment. Also, security assessments scans must be initiated after major application configuration changes. The Transportation Business Unit (TBU) Contracting Officers' Technical Representative (COTR) and/or IT Manager will be informed before the assessment is done and receive a copy of the results.

11.1.2 Types of Scans

A *vulnerability assessment scan* is defined as a systematic examination of a system to identify those critical infrastructures or related components that may be at risk from an attack and the determination of appropriate procedures that can be implemented to reduce that risk.

A *discovery scan* runs on MDOT's subnets detecting all IP based hosts. Ports are scanned and services associated with those ports are enumerated. No vulnerabilities are determined during these scans.

A special Web server scan is run for Web servers that are located on the DMZ or internal MDOT network. This scan will crawl or spider each Web page, following all the links, perform code analysis, and perform vulnerability detection.

11.2 Frequency of VA scans

11.2.1 Pre-Production On Demand VA Scans

All new servers that are being placed in a production environment must pass a vulnerability assessment (VA) scan. The initial VA scans are performed by the server administrator/TBU management after the operating system is installed and ready for the test and development environment. This will give them the opportunity to remediate any vulnerabilities that are reported before submitting the request for the final scan to the OTTS IT Security or NMS contractor for the final scan. The final scan is performed by OTTS IT Security or NMS contractor personnel after the server is configured and the developer installs the application code onto the server, readying it for the production environment.

Additionally, assessments must be performed after major configuration changes deemed appropriate during the Security Review of the Change Request approval process.

11.2.2 Ongoing/Monthly Scheduled Scans

Vulnerability assessment scans of each TBU are run monthly. This consists of scanning all TBU resources including servers and workstations. During the scan, ports are scanned and services are enumerated. Based on the operating system, the assessment may require to login into the system or application, which requires credentials that are provided by the server administrator to be in place for the scan. All of the data gathered is processed through a very extensive matrix to determine vulnerabilities with remediation recommendations.

Discovery scans are also run ongoing throughout the network.

11.3 Criteria

The OTTS Office of IT Security or NMS contractor will determine based on the results of the scan whether the server passes or requires remediation. A risk score is provided in the report. Judgment is made on the severity of the vulnerability and the risk that it poses to the integrity of the MDOT network (likelihood of attack or exploitation).

The server administrator is expected to mitigate any of the vulnerabilities those are deemed to pose a high risk to the MDOT network. After remediation, another scan will be run to determine if the risk still exist. In cases where the server administrator/TBU management cannot remediate the vulnerability but requires placement of the server in the network, they must accept the risk and initiate a Safeguard Implementation Plan (SIP, Section 16) with the OTTS Office of IT Security.

11.4 Scans from Third Party Vendors

Any Web server that process or stores credit card data for online electronic transactions are subject to a scan to meet Payment Card Industry Data Security Standards (PCI DSS) requirements. The PCI scan must be performed by an external (Third-Party) Approved Scanning Vendor (APS). The TBU IT leads must arrange these scans with the OTTS Office of IT Security or NMS contractor, and make sure that the scheduled task is on the NOC calendar. A Service Request/Change Request must be opened if the scan requires temporary firewall changes to allow the scan to take place.

Any server(s) for which a TBU's business system or application is resident on that is hosted by a Third Party outside of the MDOT network must have a VA scan run quarterly by the Third-Party vendor. The vendor is responsible for providing the scan report to the TBU COTR and the OTTS Office of IT Security. The vendor is responsible for remediating any high or critical risk vulnerability under the direction of the OTTS Office of IT Security.

11.5 Communication of New Vulnerabilities

As new vulnerabilities are discovered or announced, the MDOT NMS InfoSec contractor or OTTS Security Team shall inform each COTR via email with a description of the vulnerability,

it's risk to the MDOT environment and where possible and practical, a means to mitigate or protect the TBU from the risk that the vulnerability presents. Sources of such vulnerability information include but are not limited to:

MS-ISAC

US-CERT

Vendor sites such as Cisco, Adobe, etc.

SANS Institute

Section 12: Computer and Network Equipment Disposal Policy

12.1 Purpose

The purpose of this policy is to describe the permitted disposal methods for devices that may contain data storage either on hard disk, removable media, or within memory. This includes, but is not limited to, computers, servers, routers, switches, copiers, printers, faxes, multipurpose devices, cameras, and other related equipment. Data left on hard drives, Random Access Memory (RAM), Flash Memory or Non-Volatile Memory can contain proprietary information or data that is sensitive to the security of the network and MDOT information. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO.

12.2 Scope

This policy applies to all MDOT and MDOT Transportation Business Units (TBUs) employees, and personnel subordinate to MDOT and TBU contracts. This applies to all network and stand-alone computer systems (desktops, workstations, laptops, and servers), routers, switches, hubs, concentrators, firewalls or other network related items. It also applies to systems not located within MDOT that are provided as a service to MDOT. Policy Statement

12.3 Policy Statement

Computers and networks provide access to MDOT and remote resources, as well as the ability to communicate with other users worldwide. Proprietary and/or sensitive data may be permanently stored or cached on the hard drive, RAM, Flash Memory, or Non-Volatile Memory. Proper disposal of this data is required to protect the confidentiality of data and to ensure security of the network.

12.4 Responsibilities

Each Transportation Business Unit (TBU) is responsible for developing an expanded procedure that is entirely consistent with this MDOT policy. The unique needs of each TBU's business and technical environments may include additional guidance as long as it is consistent with and meets the minimum requirements of MDOT and State policies, standards and guidelines as well as regulatory mandates, such as Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), and the requirements of other agencies MDOT interfaces with, such as the U.S. Department of Justice, Federal Bureau of Investigation – "CJIS Security Policy".

Agency and TBU executive management will ensure that program unit management and unit supervisors implement policy. Individuals with supervisory responsibilities must ensure that their subordinates are aware of their responsibilities.

The MDOT CIO requires that each TBU send a report to the MDOT CIO Office that indicates specific information about equipment that has had to be "sanitized" prior to disposal. That information can be found on the MDOT NOC Portal under equipment sanitization reporting procedure.

12.5 Guidance

Once Computer and/or Network Equipment has been identified as "Excess for Disposal" the equipment will be advertised to all MDOT TBU for five (5) business days to determine if there is interest in acquiring the equipment. Any equipment that is to be reused by a TBU must have the hard drive wiped and reimaged. Any equipment not requested by a TBU will be disposed of as mandated in DGS' Inventory Standards & Support Services Division (ISSSD) Inventory Control Manual.

As stated in Section 6.4 of the Department of Information Technology's (DoIT's) Information **Security Policy Version 3.1; "**To eliminate the possibility of inadvertently releasing residual representation of State data, State agencies will either destroy the electronic storage media (provide evidence of destruction documentation) or ensure that the electronic storage media has been sanitized in accordance with NIST SP800-88 *Guidelines for Media Sanitization*. The removed hard drives may either be sanitized with a disk wiping utility and re-used within an agency or must be physically destroyed such that they are permanently rendered functionally useless. Agency CIOs will be responsible for the hard drive removal, recycling, destruction and/or disposal process.

A request for waiver is to be submitted to DoIT's Enterprise Information Services for authorization of disposal of a device with a hard drive and/or electronic memory with justifying documentation to support that the media has been overwritten in accordance with U.S. Department of Defense media sanitization standards.

As stated in Section 6.5 of the Department of Information Technology's (DoIT) Information Security Policy version 3.1, "To eliminate the possibility of inadvertently releasing residual representation of State data, State agencies will either destroy the electronic storage media or ensure that the electronic storage media has been sanitized in accordance with NIST SP800-88 *Guidelines for Media Sanitization*. Note: Disposal of electronic storage media should be in compliance with the agency's document retention policy and litigation hold procedures. Additionally, the procedures performed to sanitize electronic media should be documented and retained for audit verification purposes. This policy applies to all electronic storage media equipment that is owned or leased by the State (including, but not limited to: workstations, servers, laptops, cell phones and Multi-Function Printers/Copiers)."

Additional guidance will be provided using NIST Special Publication 800-88 Table A-1 Media Sanitization decision matrix.

Section 13: Network Access Policy

13.1 Purpose

The purpose of this policy is to describe the criteria a computer system must meet before being able to connect to the MDOT network. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO. Scope

This policy applies to anyone that needs to connect a microcomputer or server to the MDOT network including, but not limited to all MDOT employees, staff subordinate to MDOT contracts, and visitors. This applies to all computer systems (desktops, workstations, laptops, and servers) that need access to the MDOT network.

13.2 Policy Statement

Computers and networks provide access to MDOT and resources, as well as the ability to communicate with other users worldwide. All systems must be secure and up to MDOT standards before they will be allowed access to the network.

13.3 Responsibilities

Each Agency is responsible for developing policy and/or procedure that is entirely consistent with this MDOT policy. The unique needs of each Agency's business and technical environments may include additional guidance as long as it is consistent with and meets the minimum requirements of MDOT policies, standards and guidelines. Agency executive management will ensure that program unit management and unit supervisors implement the policy.

13.4 Guidance

All computer systems must meet MDOT standards before access will be allowed on the MDOT network. MDOT has a policy of disabling unused network ports. The Modal Help Desk should be contacted to request access to the MDOT network and a Help Desk ticket will be created to ensure compliance with this policy. If currently disabled, the port will be activated within 24 hours of contacting the Help Desk. The following standards must be met before connection to the MDOT network is allowed.

- **Operating system patches up to date**

  Any microcomputer system and server must be up to date with the latest security patches for the operating system. The server administrator must apply all of the latest security patches and updates within a month after the updates are announced or immediately if the update is critical.

- **MDOT/MDTA has an account with administrative rights to the system**

Any microcomputer system and server that will be directly connected to the MDOT network longer than one day must have an MDOT account with administrative rights to the system accessible by the Modal technical staff. Any exceptions to this must be granted by the MDOT CIO in writing.

- **Antivirus Protection**

  Antivirus protection must be installed on the microcomputer system or server. The software must be configured to run at startup and stay memory-resident to check for viruses during normal activity. The software must also be up to date with the latest virus signatures.

If new and/or third-party systems (including laptops) need to be connected to the network in order to be patched, updated, or any other reason in order to meet MDOT standards, this activity can be performed by connecting to the secure build areas that are segregated from the MDOT network at the discretion of the Modal. It is the responsibility of the Third Party to update third-party systems.

Section 14: Safeguard Implementation Policy

14.1 Purpose

A. The State of Maryland Department of Transportation (MDOT) recognizes the need to mitigate and ultimately correct risks introduced to the MDOT Enterprise to the extent that it is plausible and possible.

B. MDOT further recognizes that it needs to be able to continue to serve its customers while mitigating or correcting a discovered risk to the enterprise unless the risk is so extreme that it requires immediate resolution to avoid potential loss or disclosure of critical IT Resources, Systems or Data.

C. MDOT requires Safeguard Implementation Plans to assist the organization in managing an identified risk in a controlled and structured manner. These plans contain information on risk details, strategies to mitigate impact, procedures to be implemented, and communication processes to be followed in response to the identification of a specific risk(s) to the MDOT Enterprise.

14.2 Scope

A. This policy applies to the Maryland Department of Transportation (MDOT) organizations, their staff, and their contractors that manage and maintain computing devices and data communication devices that connect to the MDOT Enterprise Network.

14.3 Policy Statement

A. The Maryland Department of Transportation Office of Transportation Technology Services (OTTS) shall develop and maintain a Safeguard Implementation Plan (SIP) for any risk that is identified within the MDOT Enterprise[4].

B. The SIP will contain information pertinent to the nature and severity of the risk, a risk level rating, recommended controls, and selected controls for mitigating the risk. Additionally, a projected date for the implementation of each risk migration strategy will be stated and accepted by the parties responsible for the implementation of those strategies.

C. In the event that the risk is determined to be high and the required mitigating strategies cannot be implemented (not technically or financially feasible or cannot be implemented within a one-year period) the SIP documents will be accompanied by a "Management Risk Acceptance Memo" and signed by the Designated Approving Authority for the system in question, the Transportation Business Unit Chief Information Officer, and the MDOT Chief Information Officer.

[4] The Safeguard Implementation Plan shall use the NIST 800-30 Appendix C as a guide for gathering the required information.

D. The SIP and any associated Management Risk Acceptance Memos will be maintained and tracked by the MDOT Office of Transportation Technology Services (OTTS) Office of Data Security (OOS) to assure that the appropriate risk mitigation strategies are put in place in the time frames defined. The MDOT CIO and TBU CIO/Director of IT will be notified of any strategy that is in danger of not being completed or that may require an extension due to unforeseen circumstances.

14.4 Responsibilities

A. The Designated Approving Authority (DAA) is the application or system owner, responsible for assuring that vulnerabilities and associated risks are mitigated to the extent technically and financially feasible, within the milestones defined in the SIP. The DAA must also accept any remaining, or residual, risks associated with the application or system.

B. The Transportation Business Unit (TBU) Chief Information Officer, or his equivalent, shares the responsibilities of the Designated Approving Authority and accepts the risk on behalf of the TBU.

C. The MDOT Chief Information Officer, or his designee, is responsible for accepting risks for the MDOT Enterprise Network and for assuring that Safeguard Implementation Plans are adhered to.

D. The Office of Transportation Technology Services is responsible for coordinating and managing the risk and vulnerability assessment process as well as the creation, management, and monitoring of the SIP and associated documents including the "Authority to Operate" and the "Management Risk Acceptance Memo". This office is also responsible for maintaining this policy and any accompanying procedures.

14.5 Guidance

A. The Safeguard Implementation Plan seeks to follow the guidance provided in the National Institute for Standards and Technology (NIST) Special Publication (SP) 800-30 "Risk Management for Information Technology Systems".

14.6 Forms

A. Safeguard Implementation Plan

B. Vulnerability and Risk Assessment with Authority to Operate

C. Risk Acceptance Memo

Section 15: Cloud Computing Policy

15.1 Purpose

The National Institute of Standards and Technology (NIST) defines Cloud Computing as: “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”.

15.2 Scope

This policy applies to the Maryland Department of Transportation (MDOT) organizations and their staff, that wish to utilize Cloud base services. For the purposes of this policy it is relative to Software as a Service (SAAS), Hardware as a Service and Infrastructure as a service. The scope of this policy is only relevant to publicly available Cloud services, not any MDOT Corporate Cloud services that MDOT may or may not engage in.

15.3 Policy Statement

Cloud computing can offer benefits in the cost, performance, and delivery of information technology services and that the use of cloud computing services will grow significantly over time. This policy is intended to ensure that the use of these services is managed in accordance with the existing Maryland Department of information technology security policies, statutory protections of personal information, security requirements and that all risk factors are considered.

Prior to procuring a cloud computing solution, the following issues must be considered in determining the appropriateness:

A. Relevant statutory and policy requirements for the system or data that is being considered, including privacy and personally identifiable information in the data. Resources, State of Maryland Technology Security Policies and Standards and NIST Special Publication 800-144 - Guidelines on Security and Privacy in Public Cloud Computing
B. Records management and retention requirements and the ability to comply under a cloud environment.
C. Procurement and financial implications - there is usually little upfront cost to these solutions but typically a monthly service fee associated with using the cloud solution. Consider the entire life-cycle costs.
D. Issue of interoperability with existing system(s).

15.4 Responsibilities

A. The Initiator of the request is responsible for submitting the Cloud Computing request form and assuring that all appropriate reviews and sign off's have occurred prior to submitting the Service Request. It should be noted that a cloud computing request form must be submitted for each new application or service being considered. Applications negotiated prior to the writing of the policy

B. The Designated IT Authority (DIA) is responsible for assuring that the data to be stored in a cloud based service has been properly classified using the MDOT Standard Data Classification template.

C The Designated Approving Authority (DAA) is responsible for providing the business justification and any cost information associated with using a Cloud based service to perform the business function. They are also the Agency Head or delegated authority for the business giving them the authority to approve the submission of the cloud computing request.

D. The request for using a Cloud based service will be submitted as a Normal Enterprise Change Request (CR) from the Service Request, which is reviewed by the MDOT NMS security, WAN, and systems sections and approved by the MDOT Change Manager. The Cloud Computing request form and the MDOT Standard Data Classification template is attached to the CR.

15.5 Guidance

The MDOT Cloud Computing policy follows guidance provided in the State of Maryland Technology Security Policies and Standards and NIST Special Publication 800-144 - Guidelines on Security and Privacy in Public Cloud Computing

Section 16: Mobile Device Access

16.1 Purpose

Mobile access to vital business applications and information empowers workers to be more productive, efficient, and flexible. This enables access to business systems and network resources from mobile devices such as smart phones and tablets. The access is controlled through a Mobile Device Management (MDM) tool to assure confidentiality, integrity, and availability.

16.2 Scope

This policy applies to the Maryland Department of Transportation (MDOT) Transportation Business Units (TBUs) and their staff that wish to utilize mobile devices to access the MDOT network. For the purposes of this policy it is relative to the centrally managed MDM suite in regard to granting access to employees and contractors. The mobile devices include smart phones and tablets that are both state-issued and personally owned (Bring Your Own Device or BYOD). Mobile devices that this policy applies to include iOS, Android, and Windows smartphones and tablets

16.3 Policy Statement

Mobile device access offer benefits by enabling MDOT employees and contractors to gain access to the network from their mobile devices, resulting in increased productivity and efficiency. There is also a risk that comes with this convenience, as the features that make smart devices beneficial to employees are also attractive to hackers, data thieves, malware distributors, and other criminals.

This policy is intended to ensure that the use of these services is managed in accordance with the existing Maryland Department of Information Technology security policies, statutory protections of personal information, security requirements and that all risk factors are considered.

Mobile device access to the MDOT network is a privilege for authorized users. Users must sign the MDOT Mobile Device Management Acceptable Use Policy found in the appendix prior to being granted the access.

16.4 Guidance

The MDOT Mobile Device Management policy follows guidance provided in the State of Maryland Technology Security Policies and Standards and NIST Special Publication 800-124 - Guidelines on Managing the Security of Mobile Devices in the Enterprises.

16.5 Device Control

A mobile device serves many purposes, and can have personal and non-work related data stored within it. Also with the use of personally-owned devices (the BYOD concept), there is no assurance that the device is trustworthy. Organizations must assume that all mobile devices are un-trusted until proper measures to secure and monitor the device. The MDM is a technical solution that achieves degrees of trust in BYOD and State-issued devices. It also provides encryption of data in transit and on the device itself.

For personally-owned devices, all MDOT software and data will be maintained in a secure, isolated sandbox/secure container on the mobile device, separated from personal content on the device. This is known as *containerization.* A separate container for MDOT must be present on all mobile devices that are granted access to the MDOT network. This policy only applies to the MDOT container on the device set up by the MDM product, not to the entire device. (Note: for personally owned devices, some wireless carriers charge an extra fee if connecting to another network that passes through an MDM vendor).

For State-owned devices, containerization is not needed. These devices will be fully managed by the MDM and the TBU administrators.

16.6 Authentication Controls

All MDOT employees and contractors that are granted the privilege of using a mobile device to access the MDOT network are set up with a username and password through the MDM system. User accounts must <u>not</u> be shared with other individuals. The following password guidelines in accordance with MDOT and State DoIT are in place for authenticating to mobile devices:

1. New accounts must be set up with a pre-expiring password, forcing the user to create their own password.

2. Passwords must expire every 45 days.

3. The password length must be between 8 and 16 characters.

4. All passwords require an upper and lower-case letter, at least one number and at least one special character.

5. Any device that is idle for 15 minutes will be locked and require the password to be entered to unlock it.

6. User accounts will be disabled after 6 consecutive failed login attempts. Only the MDM administrators can unlock accounts.

16.7 Application Access

Mobile devices afford access to features that may be beneficial for work-related purposes. Some of these features include text messaging, a camera, GPS (Global Positioning System), and other apps. It is at the discretion of the TBU authorizer and MDM administrator to grant access to these features, which are maintained in the MDOT container of the device.

Access to the Internet (Web sites) will pass through the proxy server, enforcing the same controls in place for the employee/contractor working from a desktop. Mobile devices will have access to corporate email within the MDOT container of the device.

16.8 Compliancy Requirements

It is the responsibility of the mobile device user to maintain the most current version of software on their device. Users are responsible for assuring that the latest patches and versions on the device (state-owned or personal) must be present to assure the most sound security practices. This includes:

- The most current version of the MDM software.
- For smartphones, the device must have the most current IOS/Android software.
- Any applications present in the container.
- The MDM will automatically detect if a device has been jailbroken or rooted when logging onto the network. Any device that is detected as jailbroken or rooted will result in the container being erased. *Jailbreaking* is any third-party iPhone application which is installed and not approved by Apple. *Rooting* is unlocking the Android operating system so you can install unapproved (by Google) apps, update the OS, or replace the firmware.

16.9 Device Administration

All MDM administrators will be responsible for assigning the access needed for the users, creating the containers, providing any state-owned devices, and tracking usage. Any mobile device that is lost or stolen must be immediately reported by the user to their MDM administrator. Devices reported as lost or stolen must be wiped immediately.

Section 17: PCI Compliancy

17.1 Purpose

The purpose of this section is to identify all requirements that any TBU has which processes transactions involving credit and debit cards on their hosts in exchange for a service or product that they provide.

17.2 Scope

Any organization or merchant that accepts, transmits, or stores cardholder data (credit/debit cards) must be in compliance with Payment Card Industry Data Security Standards (PCI DSS). While the MDOT IT Security Plan addresses some of the policy subjects that are required for PCI DSS compliance, this section will provide the requirements that are specific for PCI DSS compliancy not addressed elsewhere in this plan.

17.3 Required Scans

Every quarter, any TBU that maintains an external-facing host or hosts that accepts, transmits, or stores cardholder data must undergo and pass a vulnerability scan from an external Approved Scanning Vendor (ASV). This involves an automated tool that checks a merchant or service provider's systems for vulnerabilities. The tool will conduct a non-intrusive scan to remotely review networks and Web applications based on the external-facing Internet protocol (IP) addresses provided by the merchant or service provider. The scan identifies vulnerabilities in operating systems, services and devices that could be used by hackers to target the company's private network.

A scan must be conducted by an external scan (ASV or qualified personnel) after any significant change to Internet-facing hosts in the DMZ that store, process, or transmit cardholder data. According to PCI DSS requirement 11.2.3, "The determination of what constitutes a significant change is highly dependent on the configuration of a given environment. If an upgrade or modification could allow access to cardholder data or affect the security of the cardholder data environment, then it could be considered significant"

On a quarterly basis, internal vulnerability assessment scans must be conducted on hosts that accepts, transmits, or stores cardholder data, or when a change is made to that host.

17.4 Penetration Tests

On an annual basis, a penetration test must be conducted by qualified personnel on any host that accepts, transmits, or stores cardholder data. Penetration tests must also be conducted after a significant change occurs on any host within scope of PCI (Cardholder Data Environment).

17.5 Wireless Guidelines

The wireless requirements for PCI DSS relate to whether or not the technology is part of the Cardholder Data Environment (CDE). The CDE is the computer environment where cardholder data is processed, transmitted, or stored and any networks or devices that are directly connected

to that environment. In accordance with PCI DSS Requirement 11.1 and 12.9, TBUs must check for and remove unauthorized wireless devices in the CDE on a regular basis, and maintain quarterly reports showing wireless scans of the network that may connect to the CDE which shows that rogue and unauthorized Wireless Access Points (WAPs) being eliminated, or have methodology in place that can detect authorized and unauthorized access points.

17.6 Network Security

In accordance with PCI DSS standard 1.1.6, firewall and/or router configuration for servers that accepts, transmits, or stores cardholder data must be restricted to the secure Internet Protocols of HTTPS (port 443), SSH (port 22) {note – check PCI DSS 3.1 regarding SSH}, or must be passed across a Virtual Private Network (VPN). Firewall and router configuration must be reviewed bi-annually to assure that the CDE is maintained up to standard.

17.7 Encryption

In accordance with PCI DSS standard 4.1, strong cryptography must be present to safeguard sensitive cardholder data over open, public networks. All hosts that accept, process, or store cardholder data must have an SSL certificate from a trusted Certificate Authority (CA) vendor. These hosts must have the Transport Layer Security (TLS) encryption protocol in place {note: review language with TLS}.

17.8 Access and Maintaining Cardholder Data

Access to any cardholder data must be restricted to only those individuals that require it for business purposes. If the Primary Account Number (PAN) is ever displayed, it must be *masked*, meaning that only up to the first six or the last four digits of the account number can be viewed. No individual will have access to data displaying the full PAN without written consent from the TBU's CIO. A designated manager or director from each TBU must maintain a list of individuals that have access to data with the full PAN, their role and business purpose for that access. This list must be reviewed quarterly to determine if any changes are needed.

In accordance with PCI DSS standard 3.4, any TBU that stores cardholder data must have a data retention and disposal policy in place established. Any credit or debit card numbers that are stored must be rendered unreadable if storage is required.

Appendix A Definitions

Draft Date: 20 September 2001

Security Working Group Approval Date:

CCB Approval Date:

IT Modal Managers Approval Date:

IT Team Approval Date:

Revision Date:

Revision Number: 0

ACCESS The ability to interact with a process, network, or computing resource which permits the disclosure, use or manipulation of either the data processed by the resource, or the resource itself.

DATA OWNERSHIP Those individuals or organizations that originate, maintain, or have primary responsibility for information, and who have sole authority to authorize access to that data.

INFORMATION SECURITY PROGRAM The combination of the policies contained in this document, the documented procedures/practices to implement those policies, a security awareness program to educate all parties (owners and users) of their roles and responsibilities, and a security violation/investigation/reporting/resolution program.

LEAST PRIVILEGE The security concept that only the minimum level of access required to perform an authorized and legitimate job function shall be granted to a user, to be assigned to an individual while holding that job and to be revoked when the function is no longer performed by that individual.

Payment Card Industry (PCI) Compliancy that is adherence to a set of security standardsthat were developed to protect card information during and after a financial transaction.

Payment Card Industry Data Security Standards (PCI DSS) Proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB.

Pen Test (Penetration Test) A tool for testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

PROCESS/RESOURCE OWNERSHIP Those individuals charged with maintaining a process, a network or a computing resource. Owners are responsible for the performance of the resource, which includes the implementation of security controls.

RISK The concept of evaluating the vulnerability of data, combined with the perceived threat to data, within the context of the value of the data, with the purpose of devising risk mitigation strategies.

SECURITY OF INFORMATION The person(s) responsible for establishing, enforcing, and administering security for a given computer resource.

SENSITIVITY OF INFORMATION The importance to the business, particularly with regard to potential harm resulting from inappropriate disclosure, corruption, or unavailability of the data. The sensitivity of data shall be determined by its Data Owner and communicated to all appropriate process/resource owners.

USERS Individuals with access to processes, networks or computing resources, as authorized by data owners and controlled by process/resource owners, for the purpose of using data contained within the system.

VULNERABILITY ASSESSMENT The systematic examination of a system/web server to identify those critical infrastructures or related components that may be at risk from an attack and the determination of appropriate procedures that can be implemented to reduce that risk.

Appendix B References

Annotated Code of Maryland, State Finance and Procurement Article, Sections 3-401 to 3-413 (Laws relating to information processing)

http://misc.state.md.us/cgi-win/web_statutes.exe

Annotated Code of Maryland, State government Article, Sections 10-611 through 10-701 (Laws relating to personal records, and records retention and disposal)

http://mlis.state.md.us/cgi-win/web_statutes.exe

National Institute of Standards and Technology. "Internet Security Policy: A Technical Guide" 7.0 World Wide Web (WWW)

http://csrc.nist.gov/isptg/html/ISPTG-7.html

National Institute of Standards and Technology. "Internet Security Policy: A Technical Guide" 8.0 Electronic Mail

http://csrc.nist.gov/isptg/html/ISPTG-8.html

Public Law 100-235, "Computer Security Act of 1987"

http://www.doc.gov/cio/oipr/csa-1987.html

Public Law 93-579, "The Privacy Act of 1974"

http://www.accessreports.com/statutes/PA.htm

Governor's Public Law 99-474, "Computer Fraud and Abuse Act of 1986"

http://www.panix.com/eck/computer-fraud-act.html

State of Maryland, Executive Order 01.01.194.18 "Privacy and State Data System Security"

http://www.usmh.usmd.edu/datasec/execord.html

United States Criminal Code 1030, "Fraud and Related Activity in Connection with Computers"

http://www.usdoj.gov/criminal/cybercrime/1030_new.html

Appendix C Forms and/or Disclaimers

1. MDOT Network Connection Terms and Conditions for Third Party Networks Disclaimer

Access between a third party network and the Maryland Department of Transportation (MDOT) network will be granted for lawful purposes only, limited to the scope of the service that is being provided to MDOT. Individuals from third party networks shall not transmit, retransmit, or store material or data that is the property of MDOT in violation of any federal or state laws.
Specifically prohibited acts by employees of third party networks include:

1. Unauthorized access to or use of a computer, data or software.
2. Unauthorized copying or disclosure of data or software.
3. Obtaining unauthorized confidential information.
4. Unauthorized modification or altering of data or software.
5. Unauthorized introduction of false information (public records).
6. Unauthorized disruption or interruption of the operation of a computer.
7. Unauthorized disruption of government operations or public services.
8. Unauthorized denial of services to authorized users.
9. Unauthorized taking or destroying data or software.
10. Unauthorized creating/altering a financial instrument or fund transfer.
11. Unauthorized misusing or disclosing passwords.
12. Unauthorized breaching a computer security system.
13. Unauthorized damaging, altering, taking or destroying computer equipment or supplies.
14. Unauthorized devising or executing a scheme to defraud.
15. Unauthorized obtaining or controlling money, property, or services by false pretenses.
16. Unauthorized disclosing of any info regarding the MDOT network such as IP addressing, design, etc.

Any hardware or software operated by a third party network that MDOT determines may cause hazard, interference, or service interruption to MDOT equipment, computers, or the MDOT network will be immediately disconnected by MDOT. Written notification can be provided after the equipment has been removed from the MDOT network explaining why this action was taken. This equipment will only be reconnected after corrective action is taken and MDOT has determined that the threat has been minimized or eliminated.

All authorized users during the term of their access and thereafter, shall hold in strictest confidence and not willfully disclose to any person, firm or corporation without the express authorization of the MDOT Chief Information Officer, any information related to security, operations, techniques, procedures or any other security matters. Any breach of security will be promptly reported to the Director, MDOT Office of Transportation Technology Services, designee or security officer.

I acknowledge that I have read, understand and agree to comply with the foregoing security advisory.

_____ _____
Name Printed or typed Signature

_____ _____
Name of Company Date

_____ _____
Printed typed Name of MDOT Project Manager Signature of MDOT Project Manager

Appendix D Incident Reporting

DBM Incident Report Form

Item	Guidelines
Incident Reference Numbers	Provide a unique incident number for each report. Reference any other applicable incident report numbers. (CERT)
Point of Contact Information	Provide as much POC information as possible; mailing address, e-mail address, telephone numbers (voice, pager, fax). (CERT, NIPC, FIWC)
Disclosure Information	Include a short disclosure or non-disclosure statement about what data should or should not be available to others. (CERT) Information may be shared with "The Public" or "InfraGard Members with Secure Access"? (NIPC)
Physical Location	Provide address for where the system is located. (NIPC, FIWC)
Mission/Mission Critical	What is the mission of the system involved? Is the system critical to the organization's mission? (NIPC, FIWC)
Operating System & Hardware	Provide operating system and hardware information. (NIPC, FIWC)
Security Measures	List what security measures are in place; firewall, IDS, auditing, encryption, etc. (NIPC, FIWC)
How Identified	How was the attack identified? (FIWC)
Hosts Involved	Include host names and IP addresses of sources and destinations involved. (CERT, NIPC, FIWC) Also, dumping data from whois and rwhois can provide additional information.
Description of Activity	Describe the activity. Were any vulnerabilities exploited, modifications made to the system, or software installed? (CERT) Was the attack a virus, denial of service, distributed denial of service, Trojan horse, trap door, or other? (NIPC) Actions attempted. (FIWC)
Evaluation of Attack Success	Did the attacker succeed in penetrating the system? Did damage result? (NIPC, FIWC)
Classification	List classification of system. Was any classified data compromised? (NIPC, FIWC)
Log Extracts	Include log entries that are related to the incident. Remove any unrelated entries to avoid confusion. If numerous log entries exist, include a sample of the entries and the total number of entries generated by the incident. Provide a description of the format may be helpful. (CERT)
Date/Time & Duration	Provide the date, time, and duration of the incident. (NIPC, FIWC)
Time Zone and Clock Accuracy	Provide the time in GMT offset to avoid international time zone confusion. State whether the times in the log are accurate or not. If not, state the difference. If the clock is synchronized with a time source,

	state so. (CERT)
Any Response Expected	State whether the report is for informational purposes only or if you are seeking assistance from an incident handler. (CERT)
Corrective Action	What actions have been taken to mitigate risk; disconnect, backup, checked binaries, etc.? (NIPC)

DoIT Guidance on Incident Reporting

Cybersecurity: Reportable Incidents – Additional Agency Guidance

Currently, DoIT security policy, in accordance with US-CERT and NIST guidelines, outlines specific incident reporting categories as delineated below.

Agency Incident Categories

Category	Type	Description
Category 1	Unauthorized Access	In this category an individual gains logical or physical access without permission to a state agency network, system, application, data, or other resource.
Category 2	Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
Category 3	Malicious Code	*Successful* installation of malicious software (virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.
Category 4	Improper usage	A person violates acceptable computing use policies as defined in Section 11 of the DoIT Security Policy, v.3.1.

It is observed that several agencies are having some difficulty in defining incident *severity* and, therefore, do not have a consistent sense of when a security incident meets the threshold of a reportable event. To help agencies through this inexact science, we will again seek NIST guidance to align to a collection of impact and effort categories that will help to define when incidents should be reported to DoIT.

Consider the following tables:

Functional Impact Categories

Category	Definition	Reportable to DoIT
None	No effect to the organization's ability to provide all services to all users	N
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency	N
Medium	Organization has lost the ability to provide a critical service to a subset of system users	Y

High	Organization is no longer able to provide some critical services to any users	Y

Information Impact Categories

Category	Definition	Reportable to DoIT
None	No information was exfiltrated, changed, deleted or otherwise compromised	N
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated	Y
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated	Y
Integrity Loss	Sensitive or proprietary information was changed or deleted	Y

Recoverability Impact Categories

Category	Definition	Reportable to DoIT
Regular	Time to recovery is predictable with existing resources	N
Supplemented	Time to recovery is predictable with additional resources	Y
Extended	Time to recovery is unpredictable; additional resources and outside help are needed	Y
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation	Y

Effective immediately, please use this guidance for reporting security events to DoIT along with the catch-all condition of "anything beyond normal or out of the ordinary."

APPENDIX E: MDOT Breach Follow-up Policy

Purpose

The purpose of this policy is to define the steps that must be taken by the Maryland Department of Transportation's (MDOT) Transportation Business Units (TBUs) when a breach of an information system is confirmed. The TBUs will work closely with the InfoSec team and the MDOT Chief Information Officer (CIO) throughout this process.

An *incident* is defined as a security event that compromises the integrity, confidentiality, or availability of an information asset. When an incident results in the potential unauthorized disclosure of personal or confidential data, that is defined a *breach*. When a breach occurs resulting in release of data to an unauthorized party, this is defined as *data disclosure.*

The goal of this policy is to provide swift and thorough follow-up to any breached host and system, minimize any impact on any individuals whose information was disclosed, and to comply with both state and federal laws that address this policy. This action is taken in addition to the incident handling guidelines in Section 7 Security Incident Handling and Appendixes C.4 DBM Incident Report Form and C.5 DoIT Guide on Incident Handling.

Applicability

This policy applies to all MDOT TBU server administrators, TBU IT leads, and CIOs who are responsible for the administration and daily operations of a server or device that is breached. They will take responsibility to assure that the appropriate follow-up is taken with those impacted by the breach, and establish correspondence with any parties defined in this policy. Any alleged exposure or compromise of personally identifiable information (PII) or protected health information (PHI) will be investigated as a breach which is outlined in this policy.

PII is defined by NIST (NIST SP800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information) as any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity such as name, social security number, data and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual such as medical, educational, financial, and employment information.

- Examples of PII include but are not limited to:
  Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
- Address information such as street address or email address
- Personal characteristics, including photographic image (especially of face or other identifying characteristics), fingerprints, handwriting, or other biometric data.
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, educational information, financial information)

PHI is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual. This is outlined in the US Health Insurance Portability and Accountability Act (HIPAA).

Responsibilities

When a Security Incident occurs that is confirmed as a breach by the TBU CIO/IT Management that owns the impacted data, they will be responsible for taking follow-up action. The following steps must be taken:

1. Determine the cause of the breach. This is outlined in section 7.4 of the MDOT IT Security Plan, Security Incident Handling section. The cause of the breach, and the countermeasures implemented as corrective action must be documented.
2. Notify the MDOT CIO and MDOT IT Security Offices of the breach.
3. Notify the Office of the Attorney General at the ID Theft Hotline at 410-576-6491 or 410-576-6574 or via email to idtheft@oag.state.md.
4. Notify the Maryland Department of Information Technology. This is documented in Appendix C, item 4 – "MD DoIT Incident Response Form".
5. Identify and notify all impacted individuals of the breach. This can be done via written notice, telephone, or email. Records of this correspondence must be maintained.
6. Notification of the breach must be reported to a consumer reporting agency. Shown below are agencies that can be contacted:
7. Notify the banking institutions to ensure that their card brands are alerted of potential card brand incidents.

Consumer agencies to be notified in the event of a breach.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
http://www.equifax.com
1-800-685-1111

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://www.experian.com
1-888-397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 98234
http://www.transunion.com
1-800-680-7289

Lifelock
60 East Rio Salado Parkway, suite 400
Tempe, AZ 85281
http://www.lifelock.com
1-800-607-7205

References for Card Brands Incident Reporting

VISA
http://usa.visa.com/merchants/protect-your-business/cisp/if-compromised.jsp

Mastercard
http://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf

American Express
https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&frm=TH&tabbed=breach

Discover
http://www.discovernetwork.com/merchants/fraud-protection/

JCB
http://partner.jcbcard.com/security/jcbprogram/index.html