MONTANA DEPARTMENT OF MILITARY AFFAIRS

Information Technology

Policy Manual

Includes all policies pertaining to Information Technology use by the MT Department of Military Affairs

TABLE OF CONTENTS

I - Acceptable Use Policy

Overview

The Department of Military Affairs' (hereby referred to as DMA) intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to DMA's established culture of openness, trust and integrity. We are committed to protecting DMA's employees, partners and the department from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of DMA. These systems are to be used for business purposes in serving the interests of the department and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every DMA employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at DMA. These rules are in place to protect the employee and DMA. Inappropriate use exposes DMA to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct DMA business or interact with internal networks and department systems, whether owned or leased by DMA, the employee, or a third party. All employees, contractors, consultants, temporary and other workers at DMA, and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices and network resources in accordance with DMA policies and standards and local laws and regulation.

This policy applies to employees, contractors, and consultants, temporary and other workers, at DMA, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by DMA.

Policy

General Use and Ownership

DMA proprietary information stored on electronic and computing devices, whether owned or leased by DMA, the employee, or a third party, remains the sole property of DMA. Computer users must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.

Computer users have a responsibility to promptly report the theft, loss or unauthorized disclosure of DMA proprietary information.

Computer users may access, use or share DMA proprietary information only to the extent it is authorized and necessary to fulfill assigned job duties.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual divisions are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

For security and network maintenance purposes, authorized individuals within DMA may monitor equipment, systems and network traffic at any time, per DMA's Audit Policy.

DMA reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.

System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. Computer users must lock the screen or log off when the device is unattended.

Postings by employees from a DMA email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of DMA, unless posting is in the course of business duties.

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of DMA authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing DMA-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

Prohibited System and Network Activities

The following activities are strictly prohibited, with no exceptions:

A. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by DMA.
B. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which DMA or the end user does not have an active license is strictly prohibited.
C. Accessing data, a server or an account for any purpose other than conducting DMA business, even if the computer user has authorized access, is prohibited.
D. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
E. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
F. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

G. Using a DMA computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
H. Making fraudulent offers of products, items, or services originating from any DMA account.
I. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
J. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
K. Port scanning or security scanning is expressly prohibited unless prior notification to DMA is made.
L. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
M. Circumventing user authentication or security of any host, network or account.
N. Introducing honeypots, honeynets, or similar technology on the DMA network.
O. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
P. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
Q. Providing information about, or lists of, DMA employees to parties outside DMA.

Prohibited Email and Communication Activities

When using DMA resources to access and use the Internet, users must realize they represent the department. Whenever employees state an affiliation to the department, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the department". Questions may be addressed to the IT Department.

A. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
B. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
C. Unauthorized use, or forging, of email header information.

D. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
E. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
F. Use of unsolicited email originating from within DMA's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by DMA or connected via DMA's network.
G. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Blogging and Social Media

A. Blogging by employees, whether using DMA's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of DMA's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate DMA's policy, is not detrimental to DMA's best interests, and does not interfere with an employee's regular work duties. Blogging from DMA's systems is also subject to monitoring.
B. DMA's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any department confidential or proprietary information, trade secrets or any other material covered by DMA's Confidential Information Policy when engaged in blogging.
C. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of DMA and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by DMA's Non-Discrimination and Anti-Harassment Policy.
D. Employees may also not attribute personal statements, opinions or beliefs to DMA when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of DMA. Employees assume any and all risk associated with blogging.
E. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, DMA's trademarks, logos and any other DMA intellectual property may also not be used in connection with any blogging activity

Policy Compliance

Compliance Measurement

The DMA team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by Information Systems Support in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

- Data Classification Policy
- Data Protection Standard
- Social Media Policy
- Minimum Access Policy
- Password Policy

Definitions and Terms

- Blogging
- Honeypot
- Honeynet
- Proprietary Information
- Spam

Revision History

Date of Change	Responsible	Summary of Change
September 2015	Information Systems Support	Updated and converted to a new format

II - Email Policy

Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

Purpose

The purpose of this email policy is to ensure the proper use of the Department of Military Affairs' (hereby referred to as DMA) email system and make users aware of what DMA deems acceptable and unacceptable use of the State of Montana's email system. This policy outlines the minimum requirements for use of email within the DMA Network.

Scope

This policy covers appropriate use of any email sent from a DMA email address and applies to all employees, vendors, and agents operating on behalf of DMA.

Policy

A. All use of email must be consistent with DMA policies and procedures of ethical conduct, safety, compliance with applicable laws, and proper business practices.

B. A DMA email account should be used primarily for DMA business-related purposes; personal communication is permitted on a limited basis, but non-DMA related commercial uses are prohibited.

A. All DMA data contained within an email message or an attachment must be secured according to the Data Protection Standard.

B. Email should be retained only if it qualifies as a DMA business record. An email is a DMA business record if there is a legitimate and ongoing business reason to preserve the information contained in the email.

C. Email that is identified as a DMA business record shall be retained according to the DMA Record Retention Schedule.

D. The DMA state email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any DMA employee should report the matter to their supervisor immediately.

E. Users are prohibited from automatically forwarding DMA email to a third party email system (noted in F below). Individual messages which are forwarded by the user must not contain DMA confidential or above information.

F. Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct DMA business, to create or memorialize any binding transactions, or to store or retain email on behalf of DMA. Such communications and transactions should be conducted through proper channels using DMA -approved documentation.

G. Using a reasonable amount of DMA resources for personal email is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke email from a DMA email account is prohibited.

H. DMA employees shall have no expectation of privacy in anything they store, send or receive on the department's email system.

I. DMA may monitor messages without prior notice. DMA is not obliged to monitor email messages.

Policy Compliance

Compliance Measurement

Information Systems Support will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by Information Systems Support in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

- Data Protection Standard

Definitions and Terms

None

Revision History

Date of Change	Responsible	Summary of Change
September 2015	Information Systems Support	Updated and converted to a new format

III - Ethics Policy

Overview

The Department of Military Affairs (hereby referred to as DMA) is committed to protecting employees, partners, vendors, and the department from illegal or damaging actions by individuals, either knowingly or unknowingly. When DMA addresses issues proactively and uses correct judgment it will help set us apart from other departments.

DMA will not tolerate any wrongdoing or impropriety at any time. DMA will take the appropriate measures to act quickly in correcting the issue if the ethical code is broken.

Purpose

The purpose of this policy is to establish a culture of openness, trust and to emphasize the employee's and consumer's expectation to be treated to fair business practices. This policy will serve to guide business behavior to ensure ethical conduct. Effective ethics is a team effort involving the participation and support of every DMA employee. All employees should familiarize themselves with the ethics guidelines that follow.

Scope

This policy applies to employees, contractors, consultants, temporary and other workers at DMA, including all personnel affiliated with third parties.

Policy

Executive Commitment to Ethics

A. Senior leaders and executives within DMA must set a prime example. In any business practice, honesty and integrity must be top priority for executives.

B. Executives must have an open door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force.

C. All employees must disclose any conflict of interests regarding his/her position and employment within DMA.

Employee Commitment to Ethics

A. DMA employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.
B. Every employee needs to apply effort and intelligence in maintaining ethics value.
C. Employees must disclose any conflict of interest regarding their position within DMA.
D. Employees should consider the following questions:
    - Is the behavior legal?
    - Does the behavior comply with all appropriate DMA policies?
    - Does the behavior reflect DMA values and culture?
    - Could the behavior adversely affect DMA stakeholders?
    - Would you feel personally concerned if the behavior appeared in a news headline?
    - Could the behavior adversely affect DMA if all employees did it?

DMA Awareness

Promotion of ethical conduct within interpersonal communications of employees will be rewarded.

DMA will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the DMA.

Maintaining Ethical Practices

DMA will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, and director needs to consistently maintain an ethical stance and support ethical behavior.

Employees at DMA should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

DMA has established a best practice disclosure committee to make sure the ethical code is delivered to all employees and that concerns regarding the code can be addressed.

Employees are required to recertify their compliance to Ethics Policy on an annual basis.

Unethical Behavior

DMA will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.

DMA will not tolerate harassment or discrimination.

Unauthorized use of DMA operational, personnel, financial, source code, and technical information integral to the success of DMA will not be tolerated.

DMA will not permit impropriety at any time and we will act ethically and responsibly in accordance with law.

DMA employees will not use department assets or business relationships for personal use or gain.

Policy Compliance

Compliance Measurement

The HR Officer will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback.

Exceptions

None

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

None

Definitions and Terms

None

Revision History

Date of Change	Responsible	Summary of Change
September 2015	Human Resources	Updated and converted to a new format.

IV - Password Protection Policy

Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of DMA's resources. All users, including contractors and vendors with access to DMA systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any DMA facility, has access to the DMA network, or stores any non-public DMA information.

Policy

Password Creation

A. All user-level and system-level passwords must conform to the Password Construction Guidelines.

B. Users must not use the same password for DMA accounts as for other non-DMA access (for example, personal ISP account, option trading, banking, and so on).

C. Where possible, users must not use the same password for various DMA access needs.

D. User accounts that have system-level privileges granted through group memberships or programs such as “sudo” must have a unique password from all other accounts held by that user to access system-level privileges.

E. Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

Password Change

A. All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on, at least, a 60 day basis.
B. All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every 60 days. The recommended change interval is every 45 days.
C. Password cracking or guessing may be performed on a periodic or random basis by the Information Department or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

Password Protection

A. Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential department information. DMA Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.
B. Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication.
C. Passwords must not be revealed over the phone to anyone.
D. Do not reveal a password on questionnaires or security forms.
E. Do not hint at the format of a password (for example, "my family name").
F. Do not share DMA passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
G. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
H. Do not use the "Remember Password" feature of applications (for example, web browsers).
I. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

Application Development

Application developers must ensure that their programs contain the following security precautions:

A. Applications must support authentication of individual users, not groups.
B. Applications must not store passwords in clear text or in any easily reversible form.
C. Applications must not transmit passwords in clear text over the network.
D. Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

Use of Passwords and Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

Policy Compliance

Compliance Measurement

Information System Support will verify compliance to this policy through various methods, including but not limited to, periodic walk-thru, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by Information Systems Support in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

Password Construction Guidelines

Definitions and Terms

Simple Network Management Protocol (SNMP)

Revision History

Date of Change	Responsible	Summary of Change
September 2015	Information Systems Support	Updated and converted to a new format.

V - Password Construction Guideline

Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the department network. This guideline provides best practices for creating secure passwords.

Purpose

The purpose of this guidelines is to provide best practices for the created of strong passwords.

Scope

This guideline applies to employees, contractors, consultants, temporary and other workers at Department of Military Affairs (hereby referred to DMA), including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

Statement of Guidelines

All passwords should meet or exceed the following guidelines:

Strong passwords have the following characteristics:

- Contain at least 8 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/).

Poor, or weak, passwords have the following characteristics:

- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.

- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of "Welcome123" "Password123" "Changeme123"

Computer users should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way to Remember" could become the password TmB1w2R! or another variation.

(NOTE: Do not use either of these examples as passwords!)

Passphrases

Passphrases generally are used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to unlock the private key, the user cannot gain access.

A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

Guideline Compliance

Compliance Measurement

Information Systems Support will verify compliance to this guideline through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the guideline must be approved by Information Systems Support in advance.

Non-Compliance

An employee found to have violated this guideline may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

None.

Definitions and Terms

None.

Revision History

Date of Change	Responsible	Summary of Change
September 2015	Information Systems Support	Separated from the Password Policy and converted to a new format.

VI - Software Installation Policy

Overview

Employees are not allowed to install software on Department of Military Affairs (hereby referred to DMA) computing devices without prior authorization. Unauthorized installation of software opens the organization up to unnecessary exposure. Conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can be used to hack the organization's network are examples of the problems that can be introduced when employees install software on department equipment.

Purpose

The purpose of this policy is to outline the requirements for installing software on department owned computing devices to minimize the risk of loss of program functionality, the exposure of sensitive information contained within department's computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

Scope

This policy applies to all DMA employees, contractors, vendors and agents with DMA - owned mobile devices. This policy covers all computers, servers, smartphones, tablets and other computing devices operating within DMA.

Policy

A. Employees may not install software on DMA computing devices operated within the DMA network.
B. Software requests must first be approved by the requester's manager and then be made to the Information Technology department or Help Desk in writing or via email.
C. Software must be selected from an approved software list, maintained by the Information Technology department, unless no selection on the list meets the requester's need.
D. The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

Policy Compliance

Compliance Measurement

Information Systems Support will verify compliance with this policy through various methods, including but not limited to, periodic walk-thru, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by Information Systems Support in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

None

Definitions and Terms

None

Revision History

Date of Change	Responsible	Summary of Change
September 2105	Information Systems Support	Updated and converted to a new format.

VII - Wireless Communication Policy

Overview

With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

Purpose

The purpose of this policy is to secure and protect the information assets owned by Department of Military Affairs (hereby referred to as DMA). DMA provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. DMA grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to the DMA network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by Information Systems Support are approved for connectivity to a DMA network.

Scope

All employees, contractors, consultants, temporary and other workers at DMA, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of DMA must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a DMA network or reside on a DMA site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

Policy

General Requirements

All wireless infrastructure devices that reside at a DMA site and connect to a DMA network, or provide access to information classified as DMA Confidential, or above must:

A. Abide by the standards specified in the Wireless Communication Standard.
B. Be installed, supported, and maintained by an approved support team.

C. Use DMA approved authentication protocols and infrastructure.
D. Use DMA approved encryption protocols.
E. Maintain a hardware address (MAC address) that can be registered and tracked.
F. Not interfere with wireless access deployments maintained by other support organizations.

Home Wireless Device Requirements

Wireless infrastructure devices that provide direct access to the DMA corporate network, must conform to the Home Wireless Device Requirements as detailed in the Wireless Communication Standard.

Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the DMA corporate network. Access to the DMA corporate network through this device must use standard remote access authentication.

Policy Compliance

Compliance Measurement

Information Systems Support will verify compliance to this policy through various methods, including but not limited to, periodic walk-thru, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by Information Systems Support in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

Wireless Communication Standard

Definitions and Terms

MAC Address – Media Access Control

Revision History

Date of Change	Responsible	Summary of Change
September 2015	Information Systems Support	Updated and converted to a new format.

VIII - Wireless Communication Standard

Overview & Purpose

This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a Department of Military Affairs (hereby referred to as DMA) network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by the InfoSec Team are approved for connectivity to a DMA network.

Network devices including, but not limited to, hubs, routers, switches, firewalls, remote access devices, modems, or wireless access points, must be installed, supported, and maintained by an Information Support Section.

Scope

All employees, contractors, consultants, temporary and other workers at DMA and its subsidiaries, including all personnel that maintain a wireless infrastructure device on behalf of DMA, must comply with this standard. This standard applies to wireless devices that make a connection the network and all wireless infrastructure devices that provide wireless connectivity to the network.

Information Systems Support must approve exceptions to this standard in advance.

Standard

General Requirements

All wireless infrastructure devices that connect to a DMA network or provide access to DMA Confidential, DMA Highly Confidential, or DMA Restricted information must:

A. Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.
B. Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.
C. All Bluetooth devices must use Secure Simple Pairing with encryption enabled.

Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to a DMA network, such as those behind Enterprise Teleworker (ECT) or hardware VPN, must adhere to the following:

A. Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS
B. When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point
C. Disable broadcast of SSID
D. Change the default SSID name
E. Change the default login and password

Policy Compliance

Compliance Measurement

The Information Systems Support team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thu, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Information Systems Support in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

N/A

Definitions and Terms

- AES
- EAP-FAST
- EAP-TLS
- PEAP
- SSID
- TKIP
- WPA-PSK

Revision History

Date of Change	Responsible	Summary of Change
September 2015	Information Systems Support	Updated and converted to a new format.

IX - Workstation Security Policy

Overview & Purpose

The purpose of this policy is to provide guidance for workstation security for Department of Military Affairs (hereby referred to as DMA) workstations in order to ensure the security of information on the workstation and information the workstation may have access to. Additionally, the policy provides guidance to ensure the requirements of the HIPAA Security Rule "Workstation Security" Standard 164.310(c) are met.

Scope

This policy applies to all DMA employees, contractors, workforce members, vendors and agents with a DMA -owned or personal-workstation connected to the DMA network.

Policy

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and that access to sensitive information is restricted to authorized users.

Workforce members using workstations shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimize the possibility of unauthorized access.

DMA will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

Appropriate measures include:

A. Restricting physical access to workstations to only authorized personnel.
B. Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
C. Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected. The password must comply with DMA Password Policy.
D. Complying with all applicable password policies and procedures. See DMA Password Policy.
E. Ensuring workstations are used for authorized business purposes only.

F. Never installing unauthorized software on workstations.
G. Storing all sensitive information, including protected health information (PHI) on network servers
H. Keeping food and drink away from workstations in order to avoid accidental spills.
I. Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
J. Complying with the Portable Workstation Encryption Policy
K. Complying with the Baseline Workstation Configuration Standard
L. Installing privacy screen filters or using other physical barriers to alleviate exposing data.
M. Ensuring workstations are left on but logged off in order to facilitate after-hours updates.
N. Exit running applications and close open documents
O. Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
P. If wireless network access is used, ensure access is secure by following the Wireless Communication policy

Policy Compliance

Compliance Measurement

Information Systems Support will verify compliance to this policy through various methods, including but not limited to, periodic walk-thru, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by Information Systems Support in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

- Password Policy
- Portable Workstation Encryption Policy
- Wireless Communication policy
- Workstation Configuration Standard
- HIPPA 164.210

http://www.hipaasurvivalguide.com/hipaa-regulations/164-310.php

About HIPPA
http://abouthipaa.com/about-hipaa/hipaa-hitech-resources/hipaa-security-final-rule/164-308a1i-administrative-safeguards-standard-security-management-process-5-3-2-2/

Definitions and Terms

None

Revision History

Date of Change	Responsible	Summary of Change
September 2015	Information Systems Support	Updated and converted to a new format.