

 <p style="text-align: center;">MILITARY HEALTH SYSTEM (MHS)</p> <p style="text-align: center;">INFORMATION ASSURANCE (IA)</p> <p style="text-align: center;">IMPLEMENTATION GUIDE</p>	IMPLEMENTATION GUIDE No. 5	
	EFFECTIVE DATE 07/19/05	REVISED DATE 02/22/12
<p>Subject:</p> <p style="text-align: center;">PHYSICAL SECURITY</p>		

1 PURPOSE AND SCOPE

The provisions of this guide are policy for all TRICARE Management Activity (TMA) Components (TRICARE Management Activity (TMA) Directorates; TRICARE Regional Offices (TRO), and the Military Electronic Health Record Center (MEHRC) (hereafter referred to as the TMA Component(s)). For TRICARE Contractors, this document is policy if required by contract; otherwise it serves as information assurance guidance. The Chief Information Officers of the Service Medical Departments are encouraged to incorporate this document into their information assurance policies and procedures. The purpose of this implementation guide is to ensure physical security is built upon a system of defense and with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard against espionage, sabotage, damage, and theft. As such, all MHS operations face new and complex physical security challenges across the full spectrum of operations.

1.1 DoDI 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003, Enclosure 4, provides Mission Assurance Category (MAC) controls that define the physical security requirements according to the specific MAC level of the system. This instruction, in conjunction with DoD 5200.08-R, “Physical Security Program,” April 9, 2007, defines the physical security requirements for the protection of DoD assets and resources.

1.2 In conjunction with the physical security requirements provided by DoDI 8500.2 and DoD 5200.8-R, DoD 6025.18R, “DoD Health Information Privacy Regulation,” January, 2003, provides physical security standards for personal health information (PHI), including Contingency Operations, Facility Security Planning, Workstation Use, and Workstation Security. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) addresses specific physical security standards that include Access Controls, Validation Procedures, and Maintenance Records. Additionally, DoD 8580.02R “DoD Health Information Security,” July 12, 2007, implements policy and assigns responsibilities for applying the standards for security of individually identifiable health information.

1.3 Physical security consists of measures designed to protect MHS Information Technology (IT) resources (e.g., installations, personnel, all Information Systems (ISs) and

peripheral equipment, electronic media, documents, bio-medical devices); to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard against espionage, sabotage, damage, and theft. DoD 5200.08-R provides guidelines to be used by federal organizations in structuring, developing, and implementing physical security programs for system information/network facilities.

1.4 IT resources in operating environments (e.g., data centers, healthcare facilities) must be protected with physical and environmental security measures in accordance with DoD and Service guidelines. Such measures may include, but are not limited to guards, access controls, personnel authentication, locks, intrusion detection systems, and fire detection and suppression equipment. MHS policy requires that all information, physical assets, human assets, and systems be protected and preserved by reducing their exposure to vulnerabilities that can threaten, disrupt, or curtail IS operations.

2 POLICY

It is MHS policy that:

2.1 All TMA Components shall protect IS assets by implementing cost-effective physical security measures. Physical access must be restricted to authorized personnel only.

2.2 Physical security measures provide a tangible defense to protect the facility, equipment, and data from theft, tampering, careless misuse, and natural disaster. Physical security planning requirements are provided in Attachment 1 of this Implementation Guide.

2.3 It is the responsibility of facility managers and leaders to ensure all employees abide by the security policy concerning physical access.

3 PROCEDURES

3.1 Information Assurance Managers (IAMs):

3.1.1 Assign responsibility for conducting annual physical security risk analysis for each data center and facility.

3.1.2 Ensure that appropriate security requirements are included in specifications for the acquisition or operation of data centers and facilities. All IT resources shall be protected. The means for providing protection shall be documented.

3.1.3 Ensure that Contingency or Disaster Recovery Plans provide for adequate continuity of operations. Contingency and Disaster Recovery Plans should incorporate all applicable DoD requirements and additional guidance as contained in National Institute of Standards and Technology (NIST) Special Publication 800-34 Revision .1, "Contingency Planning Guide for Federal Information Systems," dated May 2010.

3.1.4 Ensure that an exhaustive facility IT inventory is created and maintained.

3.1.5 Prepare a Physical Security Plan, addressing at least the following areas: fire, water damage, air conditioning, electricity, natural disasters (e.g., lightning strikes), access control, housekeeping, and other considerations, such as bomb threats and civil disturbances. The plan shall comply with HIPAA, as applicable and address specific areas in the plan, to include:

3.1.5.1 Wireless Technology. Appropriate physical security measures shall be employed to protect all MHS mobile hardware, software, and data contained therein, or data accessible via the mobile hardware, commensurate with the classification or sensitivity level of the data and systems involved. Specific safeguards, such as approved encryption mechanisms, should be employed to protect information in the event the mobile hardware is lost or stolen. Additional guidance can be found in the MHS IA Implementation Guide 6, “Wireless Local Area Networks (WLANs).”

3.1.5.2 Hardware. Adequate security measures must be in place to protect DoD information resources to include computers, communications equipment, and data storage devices from physical damage, theft, vandalism, and other forms of physical threats. To minimize the risk of theft to equipment, adequate deterrents, such as locked rooms and storage areas, controlled access rooms, and the monitoring of visitors must be performed.

3.1.5.3 Inventory. A current record must be maintained of the physical components of the computing assets. This record must NOT be maintained with the assets.

3.1.5.4 Access Controls. Access to facilities, hardware/software (including programs for testing and revision), and DoD information must be based on the person’s role or function. When access keys or combinations are used, an individual must be designated as responsible for managing, distributing, and logging keys and combinations, such as a key for a room or cabinet. Distribution controls shall be identified to ensure password keys are provided to authorized personnel only.

3.1.5.5 Maintenance Records. Policies and procedures must be in place to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, or locks). These procedures must be documented even when the organization does not control the building they occupy or space is shared with other organizations. If facility security is in part based on the efforts of third parties (e.g., the building’s own security force), that must be documented and be reasonable and appropriate to the circumstances.

3.1.5.6 Portable Equipment Control. Written permission must be obtained to remove equipment from a site. The recipient must provide a reasonable level of protection for that equipment and associated software, data, and media from theft and damage. A record of portable equipment assigned to employees and contractors must be maintained by the individual or group authorized to distribute the equipment.

3.1.5.7 Encryption of Data on Backup Storage Devices to include devices with Personal Health Information (PHI) or Personally Identifiable Information (PII). Refer to Implementation Guide #7, Data Integrity.

3.1.5.8 Backup Storage Facility. Signed legal agreement between Program Office and storage facility must be in place prior to storage of backups.

3.1.5.9 Backup Storage Transport. Identify method of transport (e.g., bonded transport service, privately owned vehicle (POV), etc.), roles and responsibilities of individuals responsible for various stages of transport, and define the actual process for transporting backups to the storage facility (e.g., a minimum of two individuals will accompany backups in a locked container when transporting via POV, individuals will log backups out when departing and log them in when arriving at destination, etc.).

3.1.5.10 Airline Travel. Personnel who are in the possession of laptops and other transportable computers containing Sensitive Information (SI) or PHI must not check these computers into airline luggage systems. These computers must remain in the possession of the traveler as hand luggage.

3.1.6 Continually enforce the plan and update it as required.

3.1.7 Test the plan annually.

3.2 Testing Physical Security Measures

3.2.1 The testing may employ one or more of the following strategies to ensure comprehensive validation of the physical security protections while minimizing negative impacts on the IS/network environment. Facility penetration testing may include periodic, unannounced attempts to access key computing facilities.

3.2.2 The testing may be either iterative or incremental.

3.2.3 Iterative testing accommodates a progressively more aggressive testing. This establishes the confidence in the components of the physical environment without jeopardizing the entire facility.

3.2.4 Incremental testing accommodates segmenting the IS/network environment into physical and logical structures that can be tested individually to establish component stability before combining the component testing into a larger test program.

3.2.5 Effective testing must address specific elements:

3.2.6 Ensure the test is repeatable.

3.2.7 Provide inspection checklists and guidelines for the participants to use.

3.2.8 Develop specific operational scenarios.

3.2.8.1 Document the results, findings, recommendations and lessons learned.

3.3 Implement minimum controls as shown in Attachment 2.

3.4 The MHS Physical Security Assessment Matrix is shown as Attachment 3.

4 REFERENCES

- 1) DoD 5200.08-R, "Physical Security Program," April 9, 2007
- 2) DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
- 3) National Institute of Standards and Technology (NIST) Special Publication 800-34 Revision .1, "Contingency Planning Guide for Federal Information Systems," dated May 2010.
- 4) DoD 6025.18R, "DoD Health Information Privacy Regulation," January, 2003
- 5) DoD 8580.02R , "DoD Health Information Security," July 12, 2007

5 ACRONYMS

DoD.....Department of Defense
DoDIDepartment of Defense Instruction
HIPAAHealth Insurance Portability and Accountability Act
IAInformation Assurance
IS.....Information System
IT.....Information Technology
MACMission Assurance Category
MEHRCMilitary Electronic Health Record Center
MHSMilitary Health System
NIST.....National Institute of Standards and Technology
PEO.....Program Executive Office
PHIPersonal Health Information
TMA.....TRICARE Management Activity
TRO.....TRICARE Regional Office

Physical Security Planning

Security Planning Requirements	Yes	No
Documentation		
Security Policy: Available		
Incidence Response Plan		
Approved		
Tested		
Disaster Recovery Plan		
Approved		
Tested		
Access Control Documentation: Available		
Backup Plan		
Approved		
Tested		
Key Control (logged, maintained, and reviewed)		
Approved		
Implemented		
Physical Access		
Picture Identification: Present and Visible		
Badge: Present and Visible		
Visitors Sign In/Out		
Badge Control Policies		
Approved		
Implemented		
Badge Logs are Audited		
Records Maintained		
Audited		
Access card or token – swiped or presented at automated reader for building/secure area entry or access card presented to security personnel for entry to building/secure area		
Authorized personnel access list displayed inside the data center		
Data backup tapes: Securely stored on-site until moved to off-site storage facility		
Data backup tapes: Securely transported to off-site storage facility		
Data backup tapes: Securely stored off-site storage facility		
Tape deposits (and other storage media): Withdrawals from the data backup library authorized and logged		
Security procedures are implemented to ensure each workstation is protected by allowing only authorized personnel to log on		
Password protection screen saver is set to turn on after 15 minutes of inactivity		
Facilities		
Windows and glass walls are protected by intrusion detection systems (IDS) if less than 18 feet from the ground		
Openings over 96 square inches must be covered by the same material as the wall construction, by iron bars, or 18 gauge wire mesh		
Individual personnel that have access to restricted areas must not allow piggybacking or entry to unauthorized individuals		
Entrance doors: Solid wood, metal, or metal clad wood core		
Emergency doors: Void of all devices on the outside thereby allowing exit but not		

Security Planning Requirements	Yes	No
entry		
Emergency doors: Equipped with emergency bar openers on the inside with a bolt of at least ½ inch throw		
Doors: Hinges on the inside or if door hinges are on the outside, hinges are peened, welded, or equipped with setscrew fastener		
IDS should be placed on the protected side of the doors, windows, or other moveable openings greater than 96 square inches		
Walls, solid and constructed from true floor to next floor or roof		
True floor-to-ceiling walls constructed of a material that resists intrusion		
Secure areas are protected with true floors and true ceilings		
Closed Circuit Television (CCTV) in use		
Roving guard		
Main building access is managed by security personnel		
Security lighting for all exterior doors		
Environmental		
Appropriate handheld fire extinguishers (levels A, B, C), or fixed fire hoses, present and current inspection information visible. (DoDI 8500.2 IA Control Number: PEFS-1)		
Data Center should not contain wet pipes. If not possible, a remote shutoff should be easily accessible within and outside the Data Center		
All wet and dry pipes in the Data Center clearly identified		
Heat Ventilation Air Conditioning (HVAC): Present and working		
Backup air conditioning: Present and in working condition		
Heat and smoke sensors: Present and in working condition. Battery-operated or electric stand-alone smoke detectors installed in the facility. (DoDI 8500.2 IA Control Number: PEFD-1)		
Uninterrupted Power Supplies (UPS): Present and in working condition		
24 hour temperature monitor/alarm: Present and working		
Moisture control devices: Present and working		
Emergency lighting		
Voltage regulators – automatic voltage control is implemented for key IT assets		
Clearing and sanitizing – all documents and devices are sanitized before being released outside of DoD control		
Environmental control training		
Fire suppression system (subject to local safety codes)		
Human Threat		
Intentional and unintentional internal threat policies/procedures in place		
Intentional and unintentional external threat policies/procedures in place		
Power outage policies/procedures in place		
Mobile Computing Devices		
Unattended portable and wireless devices: secured and locked; after hours protection		
Unattended removable media containing SI: secured and locked		
Hard Copy Output Access		
Hard copy sensitive information: shredded or destroyed when no longer needed		
All sensitive hard copy output: immediately picked up from output devices		
All sensitive hard copy output is secured and locked		
Data interception – printers, computer screens, copiers, etc., should be positioned so that casual passersby cannot read the data		

Security Planning Requirements		Yes	No
Marking			
Sensitive data: Marked with the appropriate security label			
Incident Response			
Incident Response Plan/Procedure: Available, tested, and exercised at least annually.			
	Approved		
	Implemented		
	Tested Annually		
All attacks are reported to the Computer Emergency Response Team			

General			
Designate an Information Assurance Manager			
Assess physical security program on an annual basis, when a change occurs, or as appropriate			
Develop and implement a security training program which provides initial and annual training			

Physical Security Minimum Controls

Security Planning Requirements	Yes	No
Computer Facilities/Rooms:		
Limit access to personnel with a demonstrated need.		
Identify and mark all entrance and exit doors.		
Install a lock, as a minimum, on each entrance and exit door.		
Provide key, combination, or access card only to those personnel who require access to perform their official duties.		
Maintain a log of all personnel given a key, combination, or access card, and have them sign the log.		
Change lock combinations whenever a member previously given the combination leaves the organization.		
Post a computer room access roster at eye level on all computer room entrances.		
Post a sign-in sheet for visitors to sign as they enter and exit the computer room.		
Ensure all visitors are escorted while in the computer room.		
If possible, locate the computer room in the center of the building in an area without windows. Additionally, the room should have walls that extend from the actual (not raised) floor to actual (not suspended) ceiling.		
Ensure that signs are posted on the computer room designating the room as a Restricted Area.		
Ensure the computer room has appropriate environmental security controls implemented, which include measures implemented to mitigate damage to IS resources caused by fire, electricity, water, and inadequate/malfunctioning climate controls.		
Grant physical access only to authorized personnel with a need-to-know to computing facilities that process sensitive information or unclassified information that has not been cleared for release. (DoDI 8500.2 IA Control Number: PECF-1)		
Secure every physical access point to facilities housing workstations that process or display sensitive information or unclassified information that has not been cleared for release is controlled during working hours. Guard or lock facilities during non-work hours. (DoDI 8500.2 IA Control Number: PEPF-1)		
Ensure that current signed procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the computing facility. (DoDI 8500.2 IA Control Number: PEVC-1B)		
Policies and procedures are in place to document repairs and modifications to the physical components of a facility that are related to security (hardware, walls, door, locks, etc.).		
Fire and Smoke		
Install smoke detectors (battery-operated or electric stand-alone smoke detectors, DoDI 8500.2 IA Control Number: PEFD-1) near equipment and test them annually.		
Install fire extinguishers in and near computer rooms. Instruct personnel in the proper use of fire extinguishing equipment.		
Ensure installation of an automatic emergency lighting system that illuminates emergency exits and evacuation routes. (DoDI 8500.2 IA Control Number: PEEL-1)		
Ensure periodic fire marshal inspections of the facility and fire extinguishing equipment; resolve deficiencies promptly.		

Security Planning Requirements	Yes	No
(DoDI 8500.2 IA Control Number: PEFI-1)		
Climate		
Some computers tolerate high and low temperatures better than others. Be sure users know their computer's limitations – and do not push the limits.		
Keep all rooms containing computers at reasonable temperatures (follow manufacturers recommendations). Keep the humidity level between 20-80 percent.		
Install gauges and alarms that warn when environmental conditions are getting out of range.		
Equip all heating and cooling systems with air filters to remove airborne dust.		
Humidity controls installed shall provide an alarm if fluctuations, potentially harmful to personnel or equipment operation, are detected; adjustments to humidifier/de-humidifier systems may be made manually. (DoDI 8500.2 IA Control Number: PEHC-1)		
Temperature controls installed shall provide an alarm when temperature fluctuations potentially harmful to personnel or equipment operation are detected; adjustments to heating or cooling systems may be made manually. (DoDI 8500.2 IA Control Number: PETC-1)		
Employees shall receive initial and periodic training in the operation of environmental controls. (DoDI 8500.2 IA Control Number: PETN-1)		
Provide protection from water damage such as flooding from rain or ice buildup outside, toilet or sink overflow inside, or water from sprinklers used to fight a fire. Consider plastic sheeting to protect the equipment if the sprinklers go off.		
Avoid locating computer rooms in a basement, especially when drainage is a problem.		
Install uninterruptible power supply (UPS) units.		
Install anti-static flooring in the computer facility.		
Where no UPS is installed, install a line filter on the computer's power supply; a voltage spike can destroy a computer's power supply.		
Install a master power switch or emergency cut-off switch to IT equipment and locate it near the main entrance of the IT area. Ensure that it is labeled and protected by a cover to prevent accidental shut-off. (DoDI 8500.2 IA Control Number: PEMS-1)		
Install voltage regulators or ensure that similar automatic voltage control is implemented for key IT assets. (DoDI 8500.2 IA Control Number: PEVR-1)		

Major focus areas are broken into numbered sub-items and further designated as either required or addressable.

An addressable sub-item is defined as an area where risk may be mitigated by alternative measures.

A required sub-item is defined as an area where risk must be mitigated utilizing one of the strategies listed.

"Implement Requirement" in the Mitigation Strategy Column depicts a firm requirement - no alternative mitigations are authorized. Mitigation options are suggestions only. Other possible solutions that may eliminate the risk associated with the finding may exist.

Purple colored text indicate additions to the matrix required by DoDI 8500.2

"R" designates an item as "Required"

"A" designates an item as "Addressable"

"D" designates the requirement applies to the "Data Center"

"F" designates the requirement applies to the "Facility"

All requirements are baseline requirements for MAC III systems; **MAC II requirements, if different, are identified in blue text.**

An "X" listed in the box marked "IATO" indicates the item is required to be mitigated for an Interim Approval to Operate (IATO).

An "X" listed in the box marked "ATO" indicates the item is required to be mitigated for an Approval to Operate (ATO).

MHS Physical Security Assessment Matrix

NR	Requirement	Description	R/A	D/F	Mitigation Strategies	Findings	Site Mitigation Plan of Action	Mitigation Completion Date	IATO	ATO
1.0	Documentation									
1.1	Security Policy	The policy outlines the requirements and guidelines for the proper physical security of information assets. Procedures are implemented to ensure the proper handling and storage of information, such as end-of-day security checks, unannounced security checks, and, where appropriate, the imposition of a two-person rule within the computing facility.	R	D/F	Implement Requirement				X	X

1.2	Incident Response Plan	The Incident Response Plan establishes procedures to address cyber attacks against an organization's IT system(s). These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware, software, or data (e.g., malicious logic, such as a virus, worm, or Trojan horse).	R	D/F	Implement Requirement				X	X
1.3	Disaster Recovery Plan (DRP) including natural disasters (flood, hurricane, earthquake, fire, etc.)	A plan maintained for emergency response, backup operations, and post-disaster recovery for an information system (IS), to ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. A disaster plan exists that provides for the partial resumption of mission essential functions within 5 days of activation. Disaster recovery procedures include business recovery plans, system contingency plans, and facility disaster recovery plans. For MAC II systems, the disaster plan provides for the resumption of mission or business essential functions within 24 hours.	R	D/F	Implement Requirement				X	X
1.4	Access Control Documentation	A means of restricting access based on the identity and need-to-know of users and/or groups should be documented. Only authorized personnel with a need-to-know are granted physical access to computing facilities that process sensitive information (SI) or unclassified information that has not been cleared for release.	R	D/F	Implement Requirement				X	X

1.5	Backup Plan	A backup plan establishes plans, procedures and technical measures that can enable a system to be recovered quickly and effectively following a service disruption. A backup plan provides a means of recovery without loss of data in the event of a malicious act, natural disaster or human error.	R	D	Implement Requirement					X	X
1.6	Key control is logged, maintained, and reviewed	Administrative procedures for the control and accounting of keys shall be established. The level of protection provided such keys shall be equivalent to that afforded the classification of the information being protected. A procedure must be established for initiation, modification and/or removal of an individual's authorization to enter the area.	R	D/F	Implement Requirement					X	X
2.0 Physical Access											
2.1	Picture Identification is present and visible	<p>A means of physically establishing positive identification of personnel authorized to enter and exit the controlled area should be present.</p> <p>Facilities that do not use picture ID systems must control access through the use of receptionists/clerks with authorization lists, log-in/out systems, and limited entry and exit points.</p> <p>For small data centers that have a limited number of authorized users (less than 30) with access to the computer room, there may not be a requirement for a badge system; however, their access must be controlled via receptionist/clerk, log in and out system, plus an access authorization list. The decision concerning whether data center personnel require a badge system shall be determined by the facility manager/commander after a risk assessment has been completed.</p>	R	D/F	To control access to facilities and data centers, managers may use: Option 1: Receptionists with authorization lists, and sign-in/out logs Option 2: Use ID Cards, or Facility badges Option3: Use Biometrics					X	X

2.2	Badge is present and visible	Authentication of individuals entering a controlled area shall be accomplished by ID badge/card or by personal identity verification.	R	D/F	Option 1: Facilities that do not use picture ID systems must control access through the use of receptionists/clerks with authorization lists, log in and out systems, and limited entry and exit points. Option 2: For data centers that have a limited number of authorized users with access to the computer room, there may not be a requirement for a badge system (determination for the requirement will be determined by the data center's Information Assurance Officer (IAO) in coordination with the DAA), however, during duty hours, their access must be controlled via receptionist/clerk with an access authorization list, or log.				X	X
2.3	Visitors Sign In/Out Log	<p>Each facility shall have procedures for identification and control of visitors. A log of all visitors shall be maintained. Current signed procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the computing facility.</p> <p>For both facilities and data centers, a record must be maintained that identifies visitors who enter the facility and data center. At a minimum, the record shall identify the visitor by name, the date and time of their arrival and departure.</p>	R	D/F	Implement Requirement				X	X

2.4	Badge control policies in place	<p>Procedures regarding the distribution and maintenance of ID badges, PINs, level of access, personnel clearance and similar system related records shall be maintained.</p> <p>For facilities and data centers, policies and procedures must be in place that control access to the facilities (e.g. key control, swipe card, or cipher lock). The underlying theme is to insure that access mechanisms are maintained.</p>	R	D/F	Implement Requirement					X	X
2.5	Badge logs are audited	<p>Records shall be maintained reflecting active assignment of access to controlled facilities. Records concerning personnel removed from the system shall be retained for 90 days. Badge logs should be audited semi-annually by the IAO or his/her representative. At a minimum, logs shall include the first and last name of the individual, time and date of authorization to access the facility/data center, time and date of loss of authorization, and name of authorizing official.</p>	R	D/F	Implement Requirement					X	X
2.6	Access card or token swiped are presented at automated reader for building/secure area entry, or presentation of access card to security personnel required for building/secure area entry	<p>Data center controls include: key control, swipe card, or cipher lock access systems. Secure computing areas should be protected by appropriate entry controls to ensure only authorized personnel are allowed access.</p> <p>At facilities where there are a number of access points, and personnel do not pass through a sentry point (receptionist), there must be a process for controlling access to the data center.</p>	R	D	Implement Requirement					X	X
2.7	Authorized personnel access list is available inside the Data Center (DC)	<p>An access roster listing all authorized personnel shall be maintained.</p>	R	D	Implement Requirement					X	X

2.8	Data backup tapes are securely stored on-site until moved to an off-site facility	The backup tapes and documents should be stored in a locked, fireproof container until they are removed from the facility to an off-site storage location.	R	D	Implement Requirement					X	X
2.9	Data backup tapes are securely stored off-site	The backup tapes shall be removed from the facility to an authorized off-site storage.	R	D	Implement Requirement					X	X
2.10	Deposits and withdrawals of tapes and other storage media from the data backup library are authorized and logged	All access to the tape library should be logged for proper accountability. The log must record logistical transactions in the library (additions and withdrawals). Logs shall be reviewed by the IAO annually.	R	D	Implement Requirement					X	X
2.11	Password protected screen saver is set to turn on automatically after 15 minutes of inactivity	Implement electronic procedures that lock the computer keyboard after a predetermined time (15 minutes). Once the workstation screen-lock is activated, access to the workstation requires the knowledge of a unique authenticator, for example, a userid and password.	R	D/F	Implement Requirement					X	X
2.12	Implement security procedures to ensure each workstation is protection by allowing only authorized personnel to log on.	Implement security procedures to ensure each workstation is protected from allowing unauthorized user access.	R								
3.0	Facilities										
3.1	Windows and glass walls are protected by Intrusion Detection Systems (IDS) if less than 18 feet from ground or roof level	Windows should be constructed from or covered with materials which will provide protection from forced entry. Windows not consisting of these materials should be protected by an Intrusion Detection System. The IDS alerts a response service that responds within 15 minutes.	A	D/F	Option 1: Data centers and facilities may use roving guards, or duty personnel Option 2: Remove windows, enclose space Option 3: Install Closed Circuit Television						X

3.2	Openings over 96 square inches covered by material the same as the wall or by iron bars, or 18 gauge wire mesh	Expanded metal, wire mesh or rigid metal bars are not required if an IDS is used as supplemental protection.	A	D/F	Openings, which allow undetected access to the facility, are blocked by: Option1: Grills or bars Option 2: Alarmed with a response system that alerts a response service. This requirement covers vents, ducts, and similar openings in excess of 96 square inches.						X
3.3	Individual personnel that have access to restricted areas, must not allow piggybacking or entry to unauthorized individuals	Unauthorized personnel shall not be allowed access to a restricted area based on another person's authorization. Each person that accesses the area must use their own authentication to gain access.	R	D/F	Implement Requirement					X	X
3.4	Entrance doors must be constructed of solid wood, metal, metal clad, or bullet-proof glass	Acceptable types of doors include: Solid wood core door that is a minimum of 1-3/4 inches thick; sixteen gauge metal cladding over wood or composition materials that is a minimum of 1-3/4 inches thick; or metal fire or acoustical protection door that is a minimum of 1-3/4 inches thick.	R	D	Implement Requirement						X
3.5	Emergency doors will be void of all devices on the outside thereby allowing exit but no entry (Subject to life safety codes)	There should be no door handles or devices on the outside of the door that allow entry. Door handles cannot not be operational from the outside. For facilities where the data center is very small, there may be only one entry and exit point. If that is the case, the door must have an emergency exit capability (breaker bar) and the door must be locked (from the outside) at all times.	R	D/F	Implement Requirement						X

3.6	Emergency doors will be equipped with emergency bar openers on the inside with a deadbolt throw of at least ½ inch (Subject to life safety codes)	Doors will be secured with deadlocking panic hardware on the inside and have no exterior hardware. Door equipment will have the capability to allow expeditious exit.	R	D/F	Implement Requirement						X
3.7	Doors have hinges on the inside. If door hinges are on the outside, the hinges must be peened, welded or equipped with setscrew fastener	If doors are equipped with hinge pins located on the exterior side of the door where it opens into an uncontrolled area outside of the controlled area, the hinges will be treated to prevent removal of the door (e.g. welded, set screws, etc.).	R	D/F	Implement Requirement						X
3.8	Intrusion Detection System should be placed on the protected side of doors, windows, or other moveable openings greater than 96 square inches to protect against movement	Data Centers must use simple magnetic alarm to detect unauthorized penetration.	R	D/F	Facilities may use: Option 1: Roving guards to guard against/identify unauthorized penetration Option 2: Duty personnel to guard against/identify unauthorized penetration					X	X
3.9	Walls solid and contained from true floor to next floor or roof	Walls shall be constructed of materials such as plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other materials offering resistance to, and evidence of unauthorized entry into the area. False ceilings should be avoided.	A	D	Develop cost-effective security controls over all physical access points and address significant threats to sensitive areas. Mitigations include: Option 1: Install an IDS (Motion detectors, etc.) above or below the false ceiling. Alarms should sound at a point where a response force can respond within 15 minutes. Option 2: Reinforce false ceilings with wire mesh, and roving guards check inside the facility on a routine basis during non-working hours.						X

3.10	True Floor to ceiling walls constructed of a material that would provide detection of surreptitious entry	The ceiling and walls shall be constructed of plaster, gypsum, wallboard material, hardware or other acceptable material.	R	D	For small facilities or facilities that have been housed in rooms that do not have a true ceiling; Option 1: An IDS may be installed to detect entry through the ceiling, and may be installed above or below the false ceiling. Option 2: Motion detectors installed in a way that allows maximum coverage of the room, and install wire mesh to reinforce the ceiling. Option 3: Roving guards check inside the facility on a routine basis during non-working hours.					X
3.11	Secure areas are protected with true ceilings and true floors	The data center must be constructed of solid permanent construction materials (plaster, gypsum wallboard, metal panels, hardboard, wood, plywood), or materials that will deter and detect unauthorized penetration.	A	D	For small data centers or data centers that are housed in rooms that do not have a true ceiling: Option1: An IDS may be installed below the false ceiling to detect entry through the ceiling. Option 2: Motion detectors installed in a way that allows maximum coverage of the room, andinstall wire mesh to reinforce the ceiling. Option 3: Roving guards check inside the facility on a routine basis during non-working hours.					X

3.12	Closed Circuit TV (CCTV) in use	The perimeter entrance should be under visual control at all times during non-working hours to prevent entry by unauthorized personnel.	A	D	<p>1. Protective measures should appear formidable enough to prevent or deter criminal attempts. Option 1: Warning notices/signs on doors Option 2: Security checkpoint sign-off sheets for roving guards</p> <p>2. Mutually supporting protective measures include: Option 1: Guard posted within visual range of the data center. Option 2: Simple magnetic alarm on data center doors/windows that sound in response force area; response force is capable of reacting within 15 minutes, and install an IDS.</p>					X
3.13	Roving guard	Roving guards' coverage will consist of, but not be limited to, physical checks of the window or door access points, classified containers, and improperly secured documents or spaces. Every physical access point to facilities housing workstations that process or display SI or unclassified information, that has not been cleared for release, is controlled during working hours and guarded or locked during non-work hours. Roving guards check the data center.	A	F	<p>After normal working hours, On non military installations: A contracted response service may respond within 15 minutes, an IDS must be in place to alert the response service.</p> <p>On military installations: Alarm sounds in duty officer area, and in the military police area, and response is available within 15 minutes.</p>				X	X

3.14	Main building access managed by security personnel	Visual monitoring shall be maintained at all times during working hours.	A	F	Building access must be managed. 1. MTFs/clinics/leased facilities: A central point of access is most desirable; however, this may not be reasonable due to the number of entry points. Receptionist, clinic clerks, and other receiving personnel may act as the visual monitor to sensitive area access. Personnel must receive security training.2. Business facilities. A central point of access is required unless:Option 1: Swipe cards are usedOption 2: Cipher locks are used					X	X
3.15	Security lighting for all exterior doors	The lighting shall be of sufficient intensity to allow detection of unauthorized activity. For MAC II systems, an automatic emergency lighting system is installed that covers all areas necessary to maintain mission or business essential functions, to include emergency exits and evacuation routes.	R	F	Implement Requirement						X
4.0	Environmental										X
4.1	Appropriate fire extinguishers (levels A, B, C) are present with current inspection information (Subject to life safety codes)	Facilities must undergo periodic fire marshal inspections. Deficiencies discovered should be promptly resolved. Handheld fire extinguishers or fixed fire hoses are available.	R	F	Implement Requirement					X	X

4.2	Data center should not contain wet pipe	Building plumbing lines should not endanger the computer facility or, at a minimum, shut-off valves and procedures exist and are known.	A	D	Appropriate and adequate controls will vary depending on individual system requirements. This is not intended to imply that all ADP facilities must have a dry pipe system, but a mitigation plan must be in place to reduce damage. The following three items must be in place. 1. Plastic sheeting must be available to cover hardware 2. Personnel must know the location of shut-off valves and their operation 3. Procedures for alerting facility engineers/fire department are prominently displayed					X	X	
4.3	Identify wet and dry pipes in the data center	Wet and dry pipes should be identified in the facility so that actions may be taken in case of rupture of extinguisher discharge. Shut-off valves and shut-off procedures should be known.	R	D	Implement Requirement						X	X
4.4	Heat Ventilation Air Conditioning (HVAC) is present and working	Resources supporting business essential functions have been implemented.	R	D/F	Implement Requirement					X	X	X

4.5	Backup air conditioning is present and in working condition	Redundancy exists in the air-cooling system.	A	D	Temperature monitors should be in place to alert employees when the room temperature is too high. Systems should be shut down to mitigate system damage. Option 1: Cut off the comfort air conditioning to the remaining office space in the building and redirect to the data center, and lighting and unnecessary equipment should be turned off Option 2: Floor fans may be used to expel computer exhaust outside the data center						X
4.6	Heat and smoke sensors are present and in working condition	Fire suppression devices have been installed and are in working order (e.g., smoke detectors, fire extinguishers, sprinkler systems, etc.). Battery-operated or electric stand-alone smoke detectors are installed in the facility. For MAC II systems, a servicing fire department receives an automatic notification of any activation of the smoke detection or fire suppression system.	R	D	Implement Requirement					X	X
4.7	Uninterrupted Power Supply (UPS) is present and in working condition	Critical devices are attached to UPSs to ensure against network and system disruption during power outages. For MAC II systems, a master power switch or emergency cut-off switch to IT equipment is present. It is located near the main entrance of the IT area and it is labeled and protected by a cover to prevent accidental shut-off.	R	D	Implement Requirement					X	X

4.8	24 hour temperature monitor/alarm is present and working	Temperature controls should be installed that provide an alarm when temperature fluctuation is potentially harmful to equipment; adjustments to heating or cooling systems may be made manually.	R	D	Implement Requirement						X
4.9	Moisture control devices are present and working	Humidity controls should be installed to provide an alarm if fluctuations occur that are potentially harmful to equipment; adjustments to humidifier/de-humidifier systems may be made manually. For MAC II systems, automatic humidity controls are installed to prevent humidity fluctuations.	A	D	Install portable de-humidifiers and check equipment operation daily.						X
4.10	Emergency Lighting	An automatic emergency lighting system is installed that covers emergency exits and evacuation routes. For MAC II systems, the emergency lighting system is installed that covers all areas necessary to maintain mission or business essential functions.	R	F	Implement Requirement						X
4.11	Voltage Regulators	Automatic voltage control is implemented for key IT assets.	R	D	Implement Requirement						X
4.12	Clearing and Sanitizing	All documents, equipment, and machine-readable media containing sensitive data are cleared and sanitized before being released outside of the Department of Defense.	R	D	Implement Requirement				X		X
4.13	Environmental Control Training	For MAC II systems, employees receive initial and periodic training in the operation of environmental controls.	A	D	Implement Requirement - Required for MAC II systems only.						
4.14	Fire Suppression System (Subject to life safety codes)	Handheld fire extinguishers or fixed hoses are available should an alarm be sounded or fire detected. For MAC II systems, a fully automatic fire suppression system is installed that automatically activates when it detects heat, smoke or particles.	R	D	Implement Requirement					X	X

5.0	Human Threat									
5.1	Intentional and unintentional internal threat policies/procedures in place	As part of the continuity of operation plan, an internal threat policy shall be designed to ensure the procedures are in place. A set of rules that clearly delineate IA responsibilities and expected behavior of all employees are in place. The rules include the consequences of inconsistent behavior or non-compliance. Signed acknowledgement of the rules is a condition of access.	R	D/F	Implement Requirement				X	X
5.2	Intentional and unintentional external threat policies/procedures in place	As part of the continuity of operation plan, an external threat policy shall be designed to ensure the procedures are in place. Drills should be executed annually or when significant changes occur.	R	D/F	Implement Requirement				X	X
5.3	Power Outage policies/procedures in place	Staff are aware of the locations of regular and auxiliary electrical power switches.	R	F	Implement Requirement				X	X
6.0	Mobile Computing Devices									
6.1	Unattended portable and wireless devices are secured and locked	Wireless devices containing SI shall be physically safeguarded to prevent unauthorized access. Laptops, PDAs and other wireless devices when left unattended, should be protected in such a way as to discourage theft. 1. Laptops that are used during the day as a workstation should be positioned on desks not convenient to casual traffic. If not used as a workstation - they should be stored in a locked container (locker, locking file cabinet). 2. As with laptops, PDAs and other handheld devices should also be mounted in areas that are not convenient to casual traffic and easy theft.	R	F	Implement Requirement				X	X

6.2	Unattended removable media containing SI are secured and locked	Unattended removable media containing SI shall be physically safeguarded to prevent unauthorized access. Hard drives, disks, magnetic tapes, CD ROMs, etc., must be stored in an area that is not convenient to casual traffic. 1. Locked inside desks, cabinets or file cabinets 2. Removed from the tops of desks, work areas, team and conference rooms, or other accessible work areas	R	F	Implement Requirement					X	X
7.0	Hard Copy Output Access										
7.1	Hard copy sensitive information that is no longer required is shredded or destroyed	All documents containing SI shall be shredded.	R	D/F	Implement Requirement					X	X
7.2	All sensitive hard copy output is immediately removed from output devices	Policies and practices shall be put in place to require the immediate pick-up of SI from printers or other sources of hard copy output. SI in hard copy form shall be protected at all times.	R	D/F	Implement Requirement					X	X
7.3	All sensitive hard copy output is secured and locked	All documents containing sensitive data should be secured and locked when not in use. SI, when left unattended, should be stored in a container (drawer, etc.). When an office is left unattended, either the container is locked or the office is locked.	R	F	Implement Requirement					X	X
7.4	Data Interception	Devices that display or output classified or SI in human-readable form are positioned to deter unauthorized individuals from reading the information. Computer screens should be positioned so that casual passersby cannot read the data on the screen. Printers, faxes and copiers should be positioned in areas that are not available to casual traffic.	R	F	Implement Requirement					X	X

8.0 Marking										
8.1	Sensitive data is marked with the appropriate security label	Appropriate labels and markings must appear on media (tapes, hard copy output) to inform personnel that the information is sensitive.	R	D/F	Implement Requirement				X	X
9.0 Incident Response										
9.1	Incident Response Plan/Procedures	All auditable administrative functions relating to information security should be reviewed. This should include specific security "post-mortems" on contingency plan testing, program assessments, and risk analyses. Review and documentation gives upper management the opportunity to impose reasonable countermeasures to detected vulnerabilities. Part of the program should require formal review of incidents as well as mock exercises for system-wide failures.	R	D/F	Implement Requirement				X	X
9.2	Computer Emergency Response Team	All attacks by viruses, Trojan Horses, etc. within the data center and user workstations shall be reported to the Computer Emergency Response Team.	R	D/F	Implement Requirement				X	X