UNITED STATES MARINE CORPS
MARINE CORPS AIR STATION
BEAUFORT, SOUTH CAROLINA 29904-5001

IN REPLY REFER TO:
5239.1A
S-6
AUG 20 2020

AIR STATION ORDER 5239.1A

From: Commanding Officer
To: Distribution List

Subj: CYBER SECURITY PROGRAM

Ref: (a) MCO 5239.2B
(b) MCO 5400.52
(c) USMC ECSM 001
(d) USMC ECSM 004
(e) USMC ECSM 005
(f) USMC ECSM 006
(g) USMC ECSM 008
(h) USMC ECSM 010
(i) USMC ECSM 011
(j) USMC ECSM 017
(k) USMC ECSM 020
(l) USMC ECSM 024
(m) DoD 8570.01-M
(n) DoDD 8140.01
(o) CJCS Manual 6510.01B
(p) SECNAVINST 5239.19
(q) DoDI 8500.01
(r) SECNAVINST 5211.5F
(s) CJCS Instruction 6510.01F
(t) SECNAVINST 5239.3C
(u) SECNAV M-5239.2
(v) SECNAVINST 1543.2
(w) SECNAV M-5239.1
(x) DoDM 5200.01, Volume 3
(y) DoDM 5200.01, Volume 4
(z) DoDM 5200.01, Volume 2
(aa) DoD 5500.7-R
(ab) DoDI 8520.03
(ac) DoDM 5205.02
(ad) MARADMIN 258/16
(ae) CG, MCIEAST Policy Letter 10-19
(af) USCYBERCOM TASKORD 13-0651
(ag) USCYBERCOM TASKORD 14-0185

Encl: (1) Cyber Security Program

1. Situation. This Order and all references provide requirements and guidance for Commanding Officers (COs), department heads, Officers in Charge (OICs), supervisors, managers, and Marine Corps Air Station (MCAS) Beaufort Cyber Security professionals to identify and manage cyber risks and meet mission requirements.

2. Cancellation. ASO 5239.1.

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

3. Mission

a. To communicate Department of Defense (DoD) Cyber Security orders and directives to provide guidance to mitigate Cyber Security incidents aboard MCAS Beaufort and ensure mission accomplishment.

b. This Order has been revised and should be reviewed in its entirety.

4. Execution. COs, department heads, OICs, supervisors, and managers shall ensure all military, federal civilians, and contract personnel comply with and implement the references as it pertains to their requirements and in the conduct of operations relating to all Cyber Security functions.

4. Administration and Logistics. Any conflicts regarding the contents of this Order shall be forwarded to the S-6 department or Cyber Security Division.

5. Command and Signal

a. Command. This Order is applicable to all personnel aboard MCAS Beaufort.

b. Signal. This Order is effective the date signed.

K. R. ARBOGAST

DISTRIBUTION: A

TABLE OF CONTENTS

Chapter 1

Introduction

1. General. This order provides the security requirements and technical/ operational controls for information systems (IS) aboard MCAS Beaufort. This order represents the Command's plan to manage risks, implement safeguards, audit, report, and document information to ensure physical and personal security.

2. Background. Reference (a) formally establishes the responsibilities for protecting Marine Corps IS as well as delineates DoD directives, DoD instructions, and guidance governing cyber security. Per reference (b), detailed cyber security practices and procedures supporting the Marine Corps Cyber Security Program have been published by the Headquarters Marine Corps (HQMC) Deputy Commandant for Information (DCI) Command, Control, Communications, and Computers (IC4) through supplemental cyber security guidance, updates, or revisions to Enterprise Cyber Security Manuals (references (c) through (l)).

3. Purpose. This Order establishes the Command's policies for maintaining compliance with the DoD, Department of the Navy (DON), and Marine Corps orders, directives, and other governing documents (references (m) through (ag)) for the secure use and safeguarding of IS.

4. Applicability and Scope

a. Applicability. This Order applies to all personnel assigned to, or operating in support of, MCAS Beaufort who access Marine Corps IS. This includes any networks that process Marine Corps data whether stand alone, contractor provided, or directly connected to the Marine Corps Enterprise Network (MCEN).

b. Scope. All DoD owned or controlled IS that receive, process, store, display, or transmit information, regardless of mission assurance category, classification, or sensitivity are applicable. This includes but is not limited to:

(1) Stand-alone IS.

(2) Mobile computing devices such as laptops, tablets, handhelds, and smartphones operating in a wired or wireless capacity and other information technologies that may be developed.

(3) Contracted third parties who use commercial devices, services, networks, and technologies.

c. Cyber Security Policy. This section mandates the actions of all administrators and users who develop, access, and maintain IS.

Chapter 2

Roles and Responsibilities

1. Commanding Officer. The CO's responsibilities, as derived from reference (a), are listed below with additional responsibilities for special programs or functions as noted:

a. Appoint in writing an Information Systems Security Manager (ISSM) for the MCEN. Ensure the ISSM receives applicable certifications per reference (m) and can perform required duties.

b. Ensure that all applicable U.S. Cyber Command Tasking Orders are applied to the portion of the MCEN that falls under their area of responsibility per references(c), (h), and (e).

c. Take responsibility for incident reporting, unauthorized disclosure, and wireless networks according to references (c), (h), and (e).

d. Assign manpower, personnel, and training responsibilities to local human resources, administrative, and training officers to carry out the Cyber Security Workforce Improvement Plan (CWIP).

2. ISSM. ISSMs are privileged users, or individuals with access to system control, monitoring, or administrative functions. Individuals having privileged access require training and certification to Information Assurance (IA) technical levels I, II, or III depending on the functions they perform. They should be a U.S citizen and must hold local access approvals commensurate with the level of information processed on the system, network, or enclave. They must have an IT-I security designation and a Tier Three (T3) and/or an initiated Tier Five (T5) background investigation per reference (u). The ISSM functions as the command focal point and principal advisor for all cyber security matters on behalf of the CO. The ISSM reports to the CO or an appointed representative and implements the overall cyber security program within their area of responsibility (AOR). The ISSM is appointed in writing by the CO and endorsed by the Authorizing Official (AO). ISSM responsibilities as derived from reference (a) are listed below with additional responsibilities for special programs or functions as noted:

a. Establish and manage the cyber security program within the command, site, system, or enclave per DoD, DON, and Marine Corps cyber security guidance and policies.

b. Manage the command, site, system, or enclave Risk Management Framework process to ensure that IS within their purview are approved, operated, and maintained throughout their life cycles per the IS accreditation package.

c. Serve as the principle advisor to the CO for site, system, or enclave cyber security matters on behalf of the Marine Corps AO per reference (q).

d. Assess the cyber security program effectiveness and mitigate deficiencies per references (b), (q), (t), and (w).

e. Assess IS for compliance with the Information Assurance Vulnerability Management (IAVM) Program and all applicable Security Technical Implementation Guide (STIG) in addition to ensuring accurate compliance information reporting per references (q) and (s).

f. Ensure cyber security workforce (CSWF) personnel receive all required security training commensurate with their security duties per reference (n).

g. Report all issues/concerns regarding programs of record to the appropriate Marine Corps System Command program office or the Marine Corps Cyberspace Operations Group (MCCOG) Vulnerability Management Team (VMT).

h. Ensure security incidents (malicious code, attacks intrusions, violations, spillages, etc.) are reported to the MCCOG Defensive Cyber Operations Section (DCOS) and the responsible parent command in a timely manner per references (p), (s), and (x).

i. Ensure MCCOG DCOS directed protective/corrective actions are implemented for security incident remediation or mitigation in accordance with the timelines provided, regardless of overtime costs or issues per references (o), (p), and (r).

j. Monitor compliance with cyber security policy, as appropriate, and review the results of such monitoring.

k. Ensure implementation of IS security measures and procedures, including the reporting of incidents to the AO and appropriate reporting chains and coordinating system-level responses to unauthorized disclosures per reference (x) for classified information or per reference (y) for Controlled Unclassified Information (CUI).

l. Responsibilities listed with regard to remote access systems per reference (d) are:

(1) Establish and manage the cyber security program within a command, site, system, or enclave in accordance with DoD, DON, and Marine Corps cyber security guidance and policies.

(2) Verify that personnel requesting access to Marine Corps Information Technology (IT) have completed all required Marine Corps Cyber Awareness training for active duty and reserve DoD service members and civilian cyber awareness training for DoD civilians, contractors, and others with unclassified MCEN accounts, and meet all DoD personnel security requirements.

(3) Validate that all DD Form 2875, System Authorization Access Requests (SAAR), are completed in their entirety and retained per current directive retention policies.

(4) Verify that remote access users have a valid telework agreement.

m. Secure Data Transfer. Ensure unit/organizational personnel follow the guidelines, process, and procedures outlined in reference (g) when manually transferring data between security domains.

n. Responsibilities listed with regard to unauthorized disclosures per reference (h) are:

(1) Serve as the first level in the reporting process for unauthorized disclosure or electronic spillage.

(2) Report all unauthorized disclosures or electronic spillages to Marine Corps IT Service Center (MITSC) East.

(3) Notify the MCCOG Battle Captain of any action taken on an unauthorized disclosure or spillage.

(4) Support the Naval Criminal Investigative Service (NCIS) in the investigation of any unauthorized disclosure or spillage.

(5) Ensure local network and technical support personnel assist NCIS in the investigation as needed.

(6) Coordinate the removal and troubleshooting of devices involved in the unauthorized disclosure or spillage with local personnel.

(7) Coordinate with the Security Manager to send classified materials (e.g., a classified hard drive) to the MCCOG in support of any investigations.

o. Responsibilities listed with regard to Personally Identifiable Information (PII) per reference (i) are:

(1) Report all breaches of PII and make notifications to affected individuals in accordance.

(2) Advocate for PII policies and procedures.

(3) Initiate and coordinate collaborative efforts within the command for actions required following the initial PII breach report.

p. Responsibilities listed with regard to the IAVM program per reference (k) are:

(1) Monitor vulnerability management notification operation directives and ensure reporting compliance with the MCCOG VMT.

(2) Coordinate with system administrators (SA) on issues regarding vulnerabilities on Marine Corps systems in their AOR.

3. Information System Security Officer (ISSO). ISSOs are privileged users with access to system controls, monitoring, or administrative functions. Individuals having privileged access require training and certification to IA technical levels I, II, or III, depending on the functions they perform. They must also be trained and certified on the operating system (OS) or computing environment they are required to maintain. They should be a U.S. citizen and must hold local access approvals commensurate with the level of information processed on the system, network, or enclave. They must have an IT-I security designation and a T3 and/or an initiated T5 back ground investigation per reference (u). ISSOs are appointed in writing by the ISSM and their responsibilities as derived from references (a) and (q) are listed below with additional responsibilities for special programs or functions as noted:

a. Provide direct support to the ISSM for all cyber security matters.

b. Ensure system-level cyber security controls in accordance with the proper program and policy guidance per references (b), (n), (q), (t), and (w).

c. Evaluate risks, threats, and vulnerabilities to determine if additional safeguards are needed to protect the command, site, system, or enclave.

d. Develop and issue any additional specific cyber security policies, guidance, and instructions as needed.

e. Assist the ISSM in monitoring, reporting, and enforcing the command, site, system, or enclave IAVM monitoring.

f. Ensure that all users have the requisite security clearances and access authorization, and are aware of their cyber security responsibilities for DoD IS and IT under their purview before being granted access to those systems.

g. In coordination with the ISSM, initiate protective or corrective measures when a cyber security incident or vulnerability is discovered. Ensure that a process is in place for authorized users to report all cyber security related events and potential threats and vulnerabilities to the ISSO.

h. Assist the ISSM in all aspects regarding unauthorized disclosure per reference (h).

4. Cyber IT/CSWF Program Manager (PM). Cyberspace IT/CSWF PMs are personnel appointed in writing who are responsible for serving as the technical Cyber IT/CSWF advisor. Responsibilities listed with regard to the CWIP per reference (l) are:

a. Identify all positions performing IS management, specialized, or privileged access cyber security functions by category, specialty, and level as described in reference (n). This applies to all positions with cyber security duties, whether performed as primary or additional/embedded duties. This requirement applies to military and civilian positions.

b. Identify all cyber security function requirements to be performed by contractors in their statement of work/contract. Ensure contractors are appropriately certified and have the appropriate background investigation to perform those cyber security functions per reference (m).

c. Train, certify, and obtain the proper background investigation for all military and civilian personnel identified as part of the CSWF to accomplish their cyber security duties per reference (m).

d. Ensure cyber security personnel performing cyber security functions obtain/maintain a commercial certification corresponding to the highest level functions required by their position per reference (m).

e. Obtain the appropriate background investigation, per reference (m), prior to granting unsupervised privileged access or management responsibilities to any DoD system.

f. Identify, track, and monitor cyber security personnel performing IA functions, per reference (m), to ensure that cyber security positions are staffed with trained and commercially certified personnel.

g. Ensure that all CSWF personnel within their command understand and comply with requirements directed in reference (a), (b), (m), (n), and (t) through (v) by establishing awareness of individual commercial certification requirements for the position assigned and developing individual training and certification compliance requirements.

h. Track all CSWF personnel, training, and certifications within the command and report compliance.

i. Submit requests in writing to HQMC DCI IC4 Cyber for all CSWF personnel requiring certification waivers via the chain of command per references (l) through (n).

5. Privileged Users. Privileged users (system and network administrators) are individuals with access to system controls, monitoring, or administrative functions. Individuals with privileged access require training and certification to IA technical levels I, II, or III, depending on the functions they perform. They must also be trained and certified on the OS or computing environment they are required to maintain. They should be a U.S. citizen and must hold local access approvals commensurate with the level of information processed on that system, network, or enclave. They must have an IT-I security designation and a T3 and/or an initiated T5 background investigation per reference (u). Privileged users are appointed in writing by the ISSM and their responsibilities, derived from references (a) and (q), are to:

a. Monitor user account activity and establish procedures to investigate, deactivate, and delete accounts that do not show activity over time and report these actions and findings to the ISSM.

b. Provide cyber security safeguards and assurances to the data under their control as well as their personal authentication and authorization mechanisms, reporting all incidents to the ISSM.

c. Analyze patterns of noncompliance or unauthorized activity and take appropriate administrative or programmatic actions to minimize security risks and insider threats, reporting all incidents to the ISSM.

d. Recognize potential security violations, report the incident as required by regulation, and remediate or mitigate any adverse impact.

e. Implement applicable patches and critical security updates in a timely manner to avoid potential compromise or loss of functionality.

f. Manage accounts, network rights, and access to information systems and equipment.

g. Configure, optimize, and test hosts (servers and workstations, etc.) and network devices (hubs, routers, and switches, etc.) to ensure compliance with security policy, procedures, and technical requirements.

h. Install, test, maintain, and upgrade OSs, software, and hardware to comply with prescribed cyber security requirements.

i. Ensure that hardware, software, data, and facility resources are archived, sanitized, or disposed of in a timely manner compliant with system security plans, requirements, and regulations.

j. Perform audit log review on network, systems, and applications in accordance with the applicable STIGs.

6. Authorized Users. Authorized users (information owners and system/data users) are military, government civilians, or contractors with authorized access to the MCEN or Marine Corps IT resources. Authorized user responsibilities as derived from references (a) and (q) are listed below with additional responsibilities for special programs or functions as noted:

a. Obtain a favorable background investigation and hold a security clearance or access approvals commensurate with the level of information processed or available on the system.

b. Comply with the guidelines established in reference (a) and submit a SAAR for access to government owned IS. A separate SAAR is required for Non-Classified Internet Protocol Router (NIPR) access and Secret Internet Protocol Router (SIPR) access.

c. Receive initial and annual cyber security training per references (m) and (n). Training is to be taken via MarineNet or the Total Workforce Management System (TWMS) only.

d. Mark, label, and safeguard all media, devices, peripherals, and IS at the security level for which they are intended in accordance with DoD, DON, and Marine Corps policies and procedures. Dissemination shall only be made to individuals with a valid need to know and clearance level at or above the classification level of the shared media, device, or peripheral per reference (z).

e. Protect all media, devices, peripherals, and IS located in their respective area of responsibility per physical security and data protection requirements.

f. Practice safe internet and intranet operating principles and take no actions that threaten the integrity of the system or network per references (a), (f), and (aa).

g. Report incidents or suspicious events regarding suspected intrusions or unauthorized access, circumvention of security procedures, presence of suspicious files or programs, receipt of suspicious email attachments, files, or links, spillage incidents, and malicious logic (viruses, trojan horses, worm spamming, phishing, chain letters, etc.) to the ISSM, ISSO, or SA per references (a) and (p).

h. Report the receipt or discover of unfamiliar or unauthorized removable media (CD-ROMs, floppy disks, thumb drives, external hard drives, etc.) to the ISSM, SA, or network administrator per applicable directives.

i. Use antivirus (AV) protection on all files, attachments, and media before opening or introducing them into the IS.

j. Report suspicious, erratic, or anomalous IS operations; missing or added files; and non-approved services or programs to the SA or network administrator in accordance with local policy and cease operations on the affected IS until authorized to start operations again by a higher authority per references (a) and (p).

k. Comply with cryptographic login requirements and password or passphrase policy directives and protect IS from unauthorized access per references (a) and (p).

l. Logoff and secure the IS and work environment (secure For Official Use Only (FOUO)/CUI media, remove Common Access Card (CAC), etc.) at the end of every workday or when out of the immediate area per references (a) and (y).

m. Access only data, controlled information, software, hardware, and firmware for which they are authorized access and have a need to know. Assume only authorized roles and privileges.

n. Install and update of authorized government-provided products (AV, Virtual Private Networks (VPNs), personal firewalls, etc.) is encouraged on personal systems as required by the AO for approved remote access.

o. Digitally sign and encrypt all sensitive information on external media or in email exchanges using Federal Information Process Standard 140-2 validated encryption (DoD CAC, DoD Alternate token). Such information includes items marked FOUO/CUI, financial data, contract related information, health information, PII, network or technical diagrams with identifiable labels (internet protocol addresses), or other information that may have an operational security impact if compromised.

p. Protect authenticators commensurate with the classification or sensitivity of the information accessed and report any compromise or suspected compromise of an authenticator to the appropriate ISSO.

q. Inform the help desk when access to a particular DoD IS or IT is no longer required.

r. Observe policies and procedures governing the secure operation and authorized use of DoD IT, including operations security per reference (ac).

s. Use DoD IT/IS only for official or authorized purposes.

t. Notify the help desk if they are unable to log into their account(s) in excess of 30 days due to deployment, temporary assigned duty, or any other valid reason to prevent them from being disabled or deleted.

u. Report any breach of PII to the ISSM.

v. Responsibilities listed with regard to remote access systems per reference (d) are:

(1) Ensure only authorized programs or applications are used in the performance of official duties.

(2) Restrict the use of Marine Corps IT to official use or authorized purposes only.

(3) Report any misuse, abuse, or other prohibited actions on Marine Corps IT systems through their chain of command.

(4) Have a signed copy of their user telework agreement on file.

w. Responsibilities listed with regard to IT resource access per reference (l) are:

(1) Restrict use of Marine Corps IS and equipment (including computers, electronic mail, and Internet systems) for official use or authorized purposes only.

(2) Report any misuse, as defined in reference (l), of Marine Corps systems to their CO or supervisor.

x. Responsibilities listed with regard to secure data transfers per reference (g) are:

(1) Follow the guidelines, processes, and procedures outlined in reference (g) when transferring data from different security domains.

(2) Ensure proper classification markings and proper handling of classified material.

(3) Act as a reliable human reviewer.

Chapter 3

Cyber Security Policy

1. General. This chapter defines the security polices for the Command's IS and IT assets. It addresses all directed requirements and local policies to ensure the secure use and safeguarding of IS throughout MCAS Beaufort.

2. System Management. Reference (ad) provides guidance on the OS authorized for use on the MCEN. The following additional policies are applicable to MCAS Beaufort:

a. MCEN assets will be disabled if not utilized for more than 90 days based off the last logon time stamp. Systems requesting to be enabled after this time will require a reimage with the current MCEN baseline image before they can access the MCEN again.

b. Systems will be maintained by MCAS Beaufort, MITSC East, and the MCCOG to meet STIG and IAVM program requirements.

c. Once added to the network, group policy will be applied to configure additional security settings (if required).

d. Contractor provided IS are authorized for use on the NIPR MCEN with the current approved MCEN image. Once the IS are no longer required to be on the MCEN, the IS will be reimaged to wipe all potential government information.

3. Public Key Infrastructure (PKI). PKI and Public Key Enablement (PKE) are implemented and enforced across the MCEN. Any requests to waive this policy shall be made in writing by the ISSM to the Marine Corps AO. The ISSM will validate such requests and keep a list of any account that is approved for exemption. The following additional policies are applicable for MCAS Beaufort:

a. All alternate token and certificate requests are processed by local Trusted Agents (TA). These are utilized for privileged users, functional accounts, and SIPRNet accounts.

b. Token and certificates are provided by the MCCOG. Distribution, tracking, and accounting are provided by the local TA.

4. Account Management. Account management controls and policies shall be implemented per reference (q) as updated by the most recent OS, application, or database STIGs. Under the supervision of the ISSM, the following additional account policies will be implemented:

a. Maintaining. NIPR SAARs are to be maintained by the Cyber Division on every account associated with MCAS Beaufort. SIPR SAARS are maintained by the SIPR Network Operations section. Each SAAR will be verified and signed by the ISSO to ensure accuracy and completeness. Once the SAAR is signed by the ISSO, it will be filed alphabetically in the SAAR database folder located on the S-6 sharedrive. Only personnel with a need to know and administrators have access to this folder.

b. Destruction. SAARs are to be kept on file for one year after the departure of the individual. SAARs will be pulled from the active folders and placed in the destruction folder, separated by month. At the one year mark the SAARs are to be permanently destroyed.

c. Authorized User Accounts

(1) Prior to accessing any system, the required IA Awareness and PII training must be completed. Derivative classification training is required for SIPR access. Certificates of completion dated within 365 days will accompany the completed SAAR form.

(2) The Security Manager must validate that a T3 or T5 background investigation has been conducted for all user account requests.

(3) One hundred percent verification of credentials and need to know is required prior to the ISSM granting access.

(4) In situations where a single sign-on PKE and PKI cannot be used, strong passwords of at least 15 characters will be used containing at least two special characters, numbers, uppercase, and lowercase letters. Application/service account passwords must be at least 15 characters meet complexity requirements, and passwords manually generated and entered by a SA must be changed at least annually or whenever a SA has knowledge that the password left the organization.

(5) Users who execute a permanent change of station will be deactivated after 60 days if a logical move does not occur (verified through Active Directory). Users that have retired, reached their end of active service date, or are no longer employed aboard MCAS Beaufort will have their accounts deactivated when they check out with the helpdesk.

(6) Management of inactive authorized user accounts will be as follows:

(a) Accounts that have been inactive for more than 90 days based off their last logon time stamp attribute will be disabled and that action will be annotated in their description field. Accounts will be moved from their Organizational Unit (OU) to the Deletion OU.

(b) The owner of the disabled account is required to contact the help desk to have the account re-enabled, at which time, validation of current documentation will occur.

(c) Guidance on account deletion and mailbox retention will be directed by HQMC. Situations for exemption include extended leave due to illness, contractors or civilians activated on reserve duty, or individuals in a temporary duty status such as an Individual Augment billet. The latter situations require prior notification to prevent deletion of the account.

(7) Any account through which unauthorized user activity has been detected will be disabled immediately and appropriate disciplinary actions taken.

d. Privileged Accounts

(1) Users requesting a privileged access account will be screened to ensure a T5 background investigation is complete and favorable.

(2) All privileged accounts will have a privileged user agreement form on file that shall be updated annually.

(3) Requests for privileged access will be processed by the ISM and approved prior to submission for creation via Remedy.

(4) The ISSM shall maintain a list of privileged users, their roles, and assigned administrative access.

(5) Accounts are audited continuously for activity by the MCCOG and disabled for inactivity.

(6) Management of inactive privileged accounts will be as follows:

(a) Accounts that have been inactive for more than 30 days based of the last logon time stamp attribute shall be disabled and that action shall be annotated in the description field.

(b) Accounts that have been disabled for longer than 30 days shall be deleted

(c) Once an account has been deleted, the privileged user must complete the request process as a new user in order to regain access.

e. Functional Accounts. Accounts that require multiple users to log in (e.g. watch standers) may have a functional account created. The following requirements must be met:

(1) Complete a SAAR, which includes the computer name in the justification.

(2) The account must have a sponsor and an ISSO assigned to it.

(3) An alternate token will be requested by the local TA and issued to the sponsor of the functional account for access to the MCEN.

5. Wireless Controls. Wireless technologies have specific controls per the references.

a. Per reference (e), wireless peripherals are not authorized for use within the Marine Corps. This includes but is not limited to mice, keyboards, headsets, printers, or other devices capable of operating on a radio frequency (RF) or utilizing Wireless Personal Area Network 802.15 protocols (Bluetooth, Infrared Data Association, Ultra-wideband, Z-Wave, Zigbee, etc.).

b. All wireless local area networks (WLAN) operated by MCAS Beaufort organizations must be approved by the MCEN AO and MCAS Beaufort S-6 prior to activation and operation.

c. All WLANs must meet the technical, administrative, and physical security requirements specified in reference (e). All waivers of the requirements must be approved by the MCEN AO via the MCAS Beaufort S-6.

d. As directed by reference (e), an authorization to operate and an authorization to connect must be granted prior to installation of any commercial wireless technologies.

6. Remote Access. Remote access is an essential means for authorized users located outside the physically secured MCEN boundary to access internal MCEN resources via secure remote connectivity. Reference (d) establishes remote access policies for the MCEN.

a. Remote Access Devices. The following are approved remote connection methods:

(1) Government issued cellular devices (hotspot) with a government issued laptop/tablet.

(2) Government issued cell phones.

(3) Wired connection to a government issued laptop.

(4) Personally owned computers may be used to access NIPRNet email via Outlook Web Access using a CAC.

b. Remote Access Controls

(1) Authorized users will request Wi-Fi capabilities through the help desk.

(2) Government devices used for remote access will be safeguarded at all times while connected to MCEN resources.

(3) Remote access devices will only be enabled while in use.

(4) Laptops may connect to the MCEN through Wi-Fi hotspots in homes, hotels, travel conference sites, and airports (domestic and international) when utilizing the Pulse Secure VPN.

(5) Laptops may not be used to connect to the internet for any purpose other than connecting to the MCEN.

(6) Personal or government issued wireless/cellular hotspots are not authorized in areas that are processing or discussing classified information.

(7) Wireless/cellular hotspots are not to be used to send, receive, store, or process classified information.

(8) All internet browsing will be done after connecting via Pulse Secure.

(9) Personal or non-MCEN connection approved contractor owned laptops/desktops are not authorized for remote access.

7. Portable Electronic Devices (PEDs). Reference (c) is the governing directive for implementation of PED policies within the Marine Corps. A PED is defined as any non-stationary electronic apparatus with singular or multiple capabilities of recording, storing, or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, tablets, MP3 players, cellular telephones, video cameras, external hard drives, and pagers. PEDs present a higher risk for compromise to their portability outside of the traditional physical security of the command. The following controls are directed for the safeguard and accountability of PEDs:

a. Smartphone Controls

(1) Prior to use, a user must complete the smartphone user agreement.

(2) Reference (e) contains the processing areas where PEDs are not authorized within MCAS Beaufort spaces.

(3) Only government owned and issued PEDs that are certified and accredited are authorized to connect to the MCEN. Contractor imaged and privately owned PEDs are not authorized to connect to the MCEN.

(4) At no time will government owned PEDs, to include hard drives, be connected to personally owned computers.

(5) If classified military information is found on a smartphone, the device must be reported to the ISSM for incident handling and whipped when authorized by the ISSM.

(6) Smartphones shall be wiped prior to disposal or transfer by the Telephone and Information Services Department (TISD).

(7) Theft, loss, or compromise of a smartphone will be reported immediately to TISD.

(8) Until official guidance is published on what is deemed an authorized application, ask yourself whether it is necessary to perform your duties and if there might be security concerns.

(8) Smartphones must be provisioned with DoD PKI digital certificates so users can digitally sign and encrypt email notifications or other email messages required by DoD policy via Purebred.

b. Laptop and Tablet Controls

(1) Laptops shall not contain any information of a personal nature (Privacy Act (PA), PII, etc.) and shall be encrypted with BitLocker.

(2) All sensitive, PII or FOUO information sent vial email shall, at a minimum:

(a) Be transmitted encrypted and digitally signed.

(b) Have a subject line stating "FOUO."

(c) Contain in the body of the email the following warning: "FOR OFFICAL USE ONLY - PRIVACY ACT SENSITIVE: Any misuse or unauthorized disclosure of this information may result in both criminal and civil penalties."

(3) Data-at-Rest encryption must be enabled per reference (c).

(4) Theft, loss, or compromise of a laptop shall be immediately reported to the ISSM.

(5) Laptops shall be properly labeled in accordance with the classification of the information they process.

(6) Only approved software installed through the software center is authorized.

(7) AV software must be enabled and updated in accordance with reference (w).

(8) RF capabilities and the microphone must be disabled prior to entry in or around the storage, discussion, or processing of sensitive information. The internal microphone and Bluetooth capabilities shall be disabled at all times via the basic input/output system.

8. Removable External Storage Devices. Removable secondary storage media devises are addressed in reference (ae). Reference (g) is the current Marine Corps directive for the secure transfer of data. Per these references, the following guidelines shall be strictly adhered to when procuring, installing, and/or using a removable external storage device:

a. Prior to use, users must complete a Removable External Storage Device User Agreement.

b. All new hard drives and those transferred from prior commands require initial approval, scanning, and tracking by the Cyber Security Division.

c. Unclassified removable external storage media is authorized up to FOUO. They shall be encrypted with BitLocker and shall not contain any information of a personal nature.

d. Removable external storage devices must be government owned and procured. Personal or contractor owned external storage devices are not authorized for connection to government information technology assets.

e. All removable storage devices connecting to classified networks shall be treated as controlled items and handled according to local command physical security policy.

f. Government owned removable external storage devices shall never be connected to personal or contractor owned computers.

g. Flash media is not authorized for use in any system that connects to the MCEN. Flash media may be use on standalone systems running current AV software and definitions. Data can then be scanned with AV software and moved to a CD/DVD for air gapping to a MCEN system.

h. Storage devices that are disguised to look like common items such as pens or bracelets are not authorized in MCAS Beaufort spaces.

i. Theft, loss, or compromise of a removable external storage device shall be reported immediately to the ISSM.

j. Removable external storage devices shall be properly marked and labeled in accordance with the classification of the information it processes.

k. Destruction of classified storage devices is handled by the Command Security Manager.

1. Destruction of unclassified storage devices is handled by the Cyber Security Division. Specific policy on destruction is available from the ISSM.

9. Insider Threat Mitigation. References (af) and (ag) direct DoD components to implement a number of technical and procedural safeguards to prevent, deter, and detect insider threats. They are only applicable to the SIPRNet with the following controls:

a. Ensure all devices are capable of installing the data loss prevention component of the host based security system or have an alternate means to disable data transfer activity (DTA).

b. Ensure all users that require DTA are approved in writing by the unit CO.

c. Ensure the procedures to identify, report, and investigate violations of DTA are documented in the Command's incident handling program.

d. Ensure acceptable use and approval processes for use of removable media devices is included in the Command's user training program.

e. Ensure all approved DTA users maintain data transfer records for all data removed from a SIPRNet machine.

f. Conduct quarterly reviews of privileged users in accordance with reference (ag) to ensure a continuing need for their capabilities and access.

10. Information Operations Condition (INFOCON). Reference (j) addresses the implementation of INFOCON in the Marine Corps.

a. Implementation. Meeting INFOCON requirements is the responsibility of the network and security association, with validation audits conducted by cyber security professionals. This implies that INFOCON measures should be, to the greatest extent possible, transparent to users. Maintaining a baseline configuration, running appropriate comparisons, and restoring systems to a known good baseline are parts of the process required to ensure networks are free of malicious activity.

b. Responsibility. The ISSM is responsible for the notification and subsequent compliance with INFOCON procedures as well as the return to normal network activity. The ISSM will periodically check the integrity of the Command INFOCON elevation plan to ensure a smooth transition into an elevated security posture. These responsibilities shall be managed by MITSC East and coordinated with MCAS Beaufort personnel for any actions that may be required.

11. Disaster Recovery/Contingency Plan. In the event of an outage, emergency, or disaster, the S-6 shall provide continuity of communication services to support various contingencies with the aid of MITSC East.

12. Incident Handling. Reference (c) provides the techniques and procedures for the proper response to computer security incidents within the Marine Corps. Reference (h) is the governing directive for classified spillage handling, and reference (i) addresses the disclosure of PII.

a. Types of Incidents or Events. Reference (c) defines the types of computer security incidents or events and their categories as established by the Chairman of the Joint Chiefs of Staff, the National Institute of Standards and Technology, and the DON.

b. Response. Users of the Command's IS are required to report incidents, suspicious activity, or possible incidents to the Cyber Security Division within 15 minutes through the quickest means possible.

c. Reporting Procedures. The Command's incident handling procedures shall provide specific guidance on reporting:

(1) Computer security incidents of events.

(2) Classified spillages.

(3) PII spillages.

d. Incident Report Storage and Analysis. All incident reports and related data must be preserved by the ISSM for three years from the resolution of the incident to enable possible criminal proceedings. Storage of incident reports and related information shall be properly safeguarded to prevent unauthorized exposure and to preserve its integrity as evidence.

13. Protected Distribution System. The Protected Distribution System (PDS) is used to transmit unencrypted national security information in lieu of a National Security Agency (NSA) approved Type One cryptographic device through an area controlled at a lesser classification level. As required by DoD regulations, the PDS must provide adequate electrical, electromagnetic, and physical safeguards to deter exploitation. Per reference (ac), the Cyber Security Division shall:

a. Maintain accreditation documents for all MCAS Beaufort PDSs.

b. Ensure daily visual inspections of the PDS are conducted by the respective unit and report any evidence of tampering, penetration, or unauthorized interception to the PDS certification authority for assessment and to the Command Security Manager for review and investigation initiation.

c. Supervise PDS modifications to ensure changes adhere to the guidelines in reference (ac).

14. Privacy Act and Personally Identifiable Information. Reference (r) provides current policy concerning PA compliance and establishes policy and procedures for safeguarding PII. The following provides MCAS Beaufort procedures and responsibilities for implementing Marine Corps policy concerning the storage and disposal of documents and media containing PII.

a. No part of a social security number shall be included as part of printed documents, computer document files in any format, computer databases, personnel reports, rosters, award certificates, correspondence, or local forms.

b. No PA data shall be resident or accessible via publically accessible websites.

c. All PA data on internal Marine Corps websites must be secured using Secure Socket Layer and PKI protocols.

d. All files and documents containing PA data shall be marked FOUO.

e. Any printed documents containing PA data shall be covered with a PA data cover sheet (DD Form 2923).

f. All printed forms of PA data shall be shredded using a NSA approved cross cut shredder, which produces particles that are one by five millimeters in size.

15. Secure Data Transfer. The transfer of data from one system to another system of a different classification or release level shall be conducted in accordance with reference (g). Failure to follow those procedures is an offense punishable under Article 92 of the Uniform Code of Military Justice and will be reported as a security incident through the Defense Information System for Security.

a. Unauthorized Dissemination of Classified Information. Electronic spillage is defined as the inadvertent or accidental contamination of electronic storage media by information classified above the accredited level of the device. If a secure data transfer results in a spillage, it must be reported and handled per reference (h)

b. Inspections and Audits. A command representative shall conduct random inspections of data transfer procedures and logs per reference (ag). A system audit will be conducted to verify documented data transfers and identify any unauthorized activity or activity that exceeds the designated threshold for that agent or asset.

16. Cyberspace IT/CSWF. Per reference (a) commands are required to develop a CWIP that compels both training managers and the ISSM to meet shared CSWF training, training, certification, and reporting requirements. The MCAS Beaufort CWIP details the procedures and responsibilities of the involved units aboard the installation in order to comply with HQMC guidance.

a. Certification

(1) Per reference (a), all CSWF personnel must obtain and maintain the certification that satisfies the requirements of their designated level. The CSWF PM shall ensure that individuals are assigned the proper level accoarding to duties and are following the guidelines of the reference.

(2) It is the responsibility of the individual to ensure that any fees and/or continuing education credits required to retain certification are maintained. Individuals who allow a certification to expire and do not make an effort to re-certify are subject to removal of privileges.

b. Training

(1) The CSWF PM is responsible for determining individuals' CSWF levels as detailed in reference (a). Upon determination of the level, the CSWF PM shall ensure the appropriate certification training and testing is completed.

(2) The CSWF PM shall ensure personnel who are designated as part of the CSWF are registered within the Defense Manpower Center and accounted for in TWMS.

c. Tracking. The CWSF PM will maintain electronic records on all personnel assigned to the CSWF. These records shall be maintained for the duration of the individual's employment and/or while the individual maintains a CSWF level status. Personnel shall be tracked via a local compliancy spreadsheet and documented in TWMS.

d. Reporting. The CSWF PM is responsible for reporting compliancy and annual training to higher headquarters. The CSWF PM shall utilize training offices that maintain records in accordance with this policy. Requests for training and certification records may come with little notice, so it is imperative that records are properly maintained.

17. Prohibited Activities. The following activities are strictly prohibited, per reference (a). Users shall not:

a. Use official government IS for commercial gain or to conduct illegal activities.

b. Use IS in any manner that interferes with official duties, undermines readiness, reflects poorly on the Marine Corps, or violates standards of ethical conduct.

c. Intentionally send, store, or propagate sexually explicit, threatening, harassing, prohibited, partisan, political, or unofficial public communications.

d. Participate in online gambling or other activities inconsistent with public service.

e. Participate in, install, configure, or use unauthorized peer-to-peer technologies.

f. Release, disclose, or alter information without consent of the data owner, the original classification authority the individual's supervisory chain of command, Freedom of Information Act official, Communication Strategy and Operations Officer, or the disclosure officer's approval.

g. Attempt to strain, test, circumvent, or bypass security mechanisms; perform network line monitoring; or perform keystroke monitoring per reference (q). If cyber security mechanisms must be bypassed, users with coordinate the procedure with the ISSO and receive written approval from the ISSM.

i. Introduce or use software, firmware, or hardware that has not been approved by the Marine Corps AO per reference (q).

j. Share personal accounts and passwords or allow remote access to non-privileged users.

k. Alter, circumvent, disable, or remove government provided and installed cyber security products, protective software, or mechanisms on Marine Corps IS.

l. Acquire commercial or unauthorized internet service provider (ISP) network access into Marine Corps operational facilities without approval from the Marine Corps AO.

m. Implement commercial wireless components (access points, base stations, clients, etc.) without approval from the Marine Corps AO.

n. Use wireless technologies for storing, processing, and transmitting unclassified information in areas where classified information is discussed, stored, processed, or transmitted without the written permission of the Marine Corps AO.

o. Automatically forward email from government accounts to commercial ISP email services, engage in the creation or forwarding of chain mail, or open email attachments or internet links from unknown sources.

p. Attempt to access files or data or use OS programs except those specifically designed or authorized for performance of official duties.

APPENDIX A

ACRONYMS

Antivirus	AV
Area of Responsibility	AOR
Authorizing Official	AO
Command, Control, Communications, and Computers	IC4
Commanding Officer	CO
Common Access Card	CAC
Controlled Unclassified Information	CUI
Cyber Security Workforce	CSWF
Cyber Security Workforce Improvement Plan	CWIP
Department of Defense	DoD
Department of the Navy	DON
Deputy Commandant for Information	DCI
For Official Use Only	FOUO
Headquarters Marine Corps	HQMC
Information Assurance	IA
Information Assurance Vulnerability Management	IAVM
Information Operations Condition	INFOCON
Internet Service Provider	ISP
Information System	IS
Information System Security Officer	ISSO
Information System Security Manager	ISSM
Information Technology	IT
Marine Corps Air Station	MCAS
Marine Corps Cyberspace Operations Group	MCCOG
Marine Corps Enterprise Network	MCEN
Marine Corps Information Technology Service Center	MITSC
National Security Agency	NSA
Naval Criminal Investigative Service	NCIS
Non-Classified Internet Protocol Router	NIPR
Officer in Charge	OIC
Operating System	OS
Organizational Unit	OU
Personally Identifiable Information	PII
Portable Electronic Device	PED
Privacy Act	PA
Program Manager	PM
Protected Distribution System	PDS
Public Key Enablement	PKE
Public Key Infrastructure	PKI
Radio Frequency	RF
Secret Internet Protocol Router	SIPR
Security Technical Implementation Guideline	STIG
System Administrator	SA
System Authorization Access Request	SAAR
Telephone and Information Services Department	TISD
Tier 3	T3
Tier 5	T5
Total Workforce Management System	TWMS
Trusted Agent	TA
Virtual Private Network	VPN
Vulnerability Management Team	VMT
Wireless Local Area Network	WLAN