



UNITED STATES MARINE CORPS
MARINE CORPS INSTALLATIONS COMMAND
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

IN REPLY REFER TO:

7500
G-6
5 May 15

MARINE CORPS INSTALLATIONS COMMAND POLICY LETTER 5-15

From: Commander, Marine Corps Installations Command
To: Distribution List

Subj: ROLE IDENTIFICATION, PERMISSIONS, AND PRIVILEGED USER ACCOUNT
DISTRIBUTION FOR ADMINISTRATION OF THE MARINE CORPS ENTERPRISE
NETWORK-NIPRNET AND SIPRNET (MCEN-N/S)

Ref: (a) Information Resource Manual (IRM) 5231-01 (Enterprise
Service Roles, Responsibilities, and Permissions
Guide), dtd 28 Jun 12
(b) IRM 2300-14 (Enterprise Information Technology Service
Management Identity and Access Management Process Guide)
(c) IRM 5231-01 Implementation Guide (DRAFT), dtd 5 Dec 14

Encl: (1) MCICOM MCEN-N/S Information Technology Services Management
(ITSM) Roles and Permissions Map
(2) Privileged Access Agreement Form, dtd 15 Jan 2013

1. Purpose. To publish policy regarding the assignment of Information Technology Service Management (ITSM) roles, and the distribution and delegation of privileged user accounts necessary to effectively execute permissions-based Incident Management (IcM) and Request Fulfillment (RqF) tasks across the Regions and Base/Post/Station (B/P/S) levels of support, and to facilitate decentralizing service desks to the Major Subordinate Commands (MSCs) (i.e. Marine Expeditionary Force (MEF), Division, Logistics Group, Wing, and lower.)

2. Background. The current MCEN-N/S permission identification strategy outlined in references (a) through (c), do not adequately identify ITSM framework and Network Operations roles and responsibilities for executing permission-based tasks. The lack of clear roles and responsibilities has led to a delay in IcM and RqF actions. System administration and end user service professionals must understand their roles and responsibilities and must be in possession of the appropriate type of privileged user accounts necessary to execute and complete permissions-based tasks.

3. Policy. Enclosure (1) outlines roles, permissions, and privileged user accounts that can be established to support Organizational Unit-aligned IcM and RqF permissions-based task accomplishment. Per enclosure (1), Regional G-6's will authorize the creation of privileged user accounts at the B/P/S and tenant supported command

Subj: ROLE IDENTIFICATION, PERMISSIONS, AND PRIVILEGED USER ACCOUNT DISTRIBUTION FOR ADMINISTRATION OF THE MARINE CORPS ENTERPRISE NETWORK-NIPRNET AND SIPRNET (MCEN-N/S)

permission levels required to support local unit service desk functions.

4. Tasks.

a. Marine Corps Installations Command (MCICOM) Regional G-6's are directed to authorize the establishment of MSC Service Desks at the MEF, Division, Logistics Group, and Wing level and to their subordinate commands as required. MCICOM Regional G-6's will facilitate decentralizing support to service desks at all MSC's. Each subordinate service desk will be staffed and supported by MSC G-6 personnel, with direction, guidance, and advice that is provided via their chain of command. MSC G-6's will have the authority to distribute permissions to organization S-6's. Each MSC G-6 and subordinate unit S-6 will be held accountable for the number of personnel to whom they assign permissions.

b. Each B/P/S, MEF, and MSC G-6/S-6 will complete the following actions:

(1) Request creation of privileged user accounts per reference (b).

(2) Identify and recommend changes to enclosure (1) to address changes in B/P/S G-6/S-6 mission requirements.

(3) Thoroughly vet each privileged user to determine if this Marine, civilian, contractor should be placed in such a high position of trust within the organization.

c. Each Regional G-6 will complete the following actions:

(1) As required, publish regional account creation RqF updates modifying processes outlined in reference (b) to meet regional ITSM models/frameworks.

(2) Ensure privileged user account creation requests from the B/P/S's and MSC's for completion at the Regional level (.bps and .tsc accounts) are fulfilled in a timely manner.

(3) Ensure privileged user accounts are assigned the correct role-based permissions per reference (c) and enclosure (1).

(4) Properly maintain security groups in accordance with reference (c) ensuring B/P/S G-6/S-6's and MSC G-6/S-6's have adequate permissions to accomplish assigned tasks while minimizing the privileged user's ability to adversely affect other units/organizational units' networks and user population.

Subj: ROLE IDENTIFICATION, PERMISSIONS, AND PRIVILEGED USER ACCOUNT
DISTRIBUTION FOR ADMINISTRATION OF THE MARINE CORPS ENTERPRISE
NETWORK-NIPRNET AND SIPRNET (MCEN-N/S)

5. Restrictions and Disciplinary Actions. Privileged user account requestors are responsible per reference (b) for completing enclosure (2), before account creation is implemented. Enclosure (1) identifies roles and permissions-based task alignments across regional and B/P/S levels of support. Failure of privileged user account holders to comply with guidance contained in the previously mentioned reference and enclosure will result in suspension of privileged user access or other disciplinary action as recommended by the Regional G-6 per enclosure (2).

6. Cancellation. This policy is in effect until amended or rescinded.

7. Applicability. This policy applies to both MCICOM and Training and Education Command commanded installations.


D. L. STANESZEWSKI
By direction

DISTRIBUTION: C

Copy to:
Commander, MARFORCYBER
CG, TECOM



MCICOM Roles and Permissions Map (4.0)

Date: 7 May 2015

The following identifies roles, permissions (functions/actions), and types of privileged user account access required to perform/support each.

OU	Object Type	Role	Permission (Action/Function/Task)	Type of MCEN-N Privileged Account Required	Notes	
MITSC: MITSC East (MCB CAMLEJ) MITSC MidPAC (MCBH) MITSC NCR (MCBQ) MITSC West (MCB CAMPEN) MITSC WestPAC (MCBJ)	User	System Administrator <i>or</i> Regional Service Desk Support <i>or</i> Regional Customer Service Center Support	Create new user objects	s.mit		
	Command Server Administrator		Delete user objects	s.mit		
			Fully control existing user objects, except Exchange-related attributes	s.mit		
			Create new command server computer objects	s.mit		
			Delete command server computer objects	s.mit		
			Create print queues	s.mit		
			Delete print queues	s.mit		
	Group		Fully control existing computer objects	s.mit		
			Fully control existing print queue objects	s.mit		
			Create new group objects	s.mit		
			Delete group objects	s.mit		
			Fully control existing group objects, except Exchange-related attributes	s.mit		
			Create new workstation computer objects	s.mit		
		Delete workstation computer objects	s.mit			
	Workstation	End User/Field Service Technician	Fully control existing workstation computer objects, except Exchange-related attributes	s.mit		
			Local Workstation - Local Admin rights on all computer objects within OU	w.mit	If a machine is off the network (not currently connected to the domain) or has never been connected, a local admin account (xAdmin) and password will be required to log in.	
			Manually Install Software	w.mit		
		Registry Changes	w.mit			
		System Administrator <i>or</i> Regional Service Desk Support <i>or</i> Regional Customer Service Center Support	Adding workstation to the domain		s.mit	End User Service (EUS) technicians will need to be on-site in order to add the machine to the domain.
			End User/Field Service Technician	Add/delete peripherals	w.mit	
Local Troubleshooting				w.mit		
Remote Desktop Connection (RDC)				w.mit		
Reset Local Admin Credentials				w.mit		
Event Logs				w.mit		
Staging OU	User		System Administrator <i>or</i> Regional Service Desk Support <i>or</i> Regional Customer Service Center Support	Create user objects	s.mit	
		Delete user objects	s.mit			

<i>OU</i>	<i>Object Type</i>	<i>Role</i>	<i>Permission (Action/Function/Task)</i>	<i>Type of MCEN-N Privileged Account Required</i>	<i>Notes</i>	
BPS: MCLB ALBANY MCAS BEAUFORT BLOUNT ISLAND CHERRY POINT LEJEUNE MARFORCOM PARRIS ISLAND MARFORPAC MCB HAWAII CBIRF MCDC MCSC QUANTICO 29PALMS BARSTOW BRIDGEPORT MIRAMAR PENDLETON MCAS PENDLETON SAN DIEGO YUMA FUJI IWAKUNI MARFORK OKINAWA * OTHERS AS REQUIRED	Command Server Administrator	System Administrator	Create new command server computer objects	s.bps		
			Delete command server computer objects	s.bps		
			Create print queues	s.bps	For those BPS'/Installations that maintain and manage print servers/services objects within their own OU.	
			Delete print queues	s.bps	For those BPS'/Installations that maintain and manage print servers/services objects within their own OU.	
			Fully control existing computer objects	s.bps		
	Fully control existing print queue objects		s.bps	For those BPS'/Installations that maintain and manage print servers/services objects within their own OU.		
	Group		Create new group objects	s.bps		
			Delete group objects	s.bps		
			Fully control existing group objects, except Exchange-related attributes	s.bps		
			Create new workstation computer objects	s.bps		
			Delete workstation computer objects	s.bps		
	Workstation		Fully control existing workstation computer objects, except Exchange-related attributes	s.bps		
			End User/Field Service Technician	Local Workstation - Local Admin rights on all computer objects within OU	w.bps	If a machine is off the network (not currently connected to the domain) or has never been connected, a local admin account (xAdmin) and password will be required to log in.
				Manually Install Software	w.bps	
				Registry Changes	w.bps	
		System Administrator	Adding workstation to the domain	s.bps	End User Service (EUS) technicians will need to be on-site in order to add the machine to the domain.	
		End User/Field Service Technician	Add/delete peripherals	w.bps		
			Local Troubleshooting	w.bps		
			Remote Desktop Connection (RDC)	w.bps		
			Reset Local Admin Credentials	w.bps		
Event Logs			w.bps			

<i>OU</i>	<i>Object Type</i>	<i>Role</i>	<i>Permission (Action/Function/Task)</i>	<i>Type of MCEN-N Privileged Account Required</i>	<i>Notes</i>
TENANT: MEF MLG DIVISION WING TECOM * OTHERS AS REQUIRED	Command Server Administrator	System Administrator	Create new command server computer objects	s.tsc	
			Delete command server computer objects	s.tsc	
			Create print queues	s.tsc	For those Tenants that maintain and manage print servers/services objects within their own OU.
			Delete print queues	s.tsc	For those Tenants that maintain and manage print servers/services objects within their own OU.
			Fully control existing computer objects	s.tsc	
	Fully control existing print queue objects		s.tsc	For those Tenants that maintain and manage print servers/services objects within their own OU.	
	Group		Create new group objects	s.tsc	
			Delete group objects	s.tsc	
			Fully control existing group objects, except Exchange-related attributes	s.tsc	
	Workstation		End User/Field Service Technician	Create new workstation computer objects	s.tsc
		Delete workstation computer objects		s.tsc	
		Fully control existing workstation computer objects, except Exchange-related attributes		s.tsc	
		System Administrator	Local Workstation - Local Admin rights on all computer objects within OU	w.tsc	If a machine is off the network (not currently connected to the domain) or has never been connected, a local admin account (xAdmin) and password will be required to log in.
			Manually Install Software	w.tsc	
			Registry Changes	w.tsc	
		Adding workstation to the domain	s.tsc	End User Service (EUS) technicians will need to be on-site in order to add the machine to the domain.	
		End User/Field Service Technician	Add/delete peripherals	w.tsc	
Local Troubleshooting			w.tsc		
Remote Desktop Connection (RDC)			w.tsc		
Reset Local Admin Credentials	w.tsc				
Event Logs	w.tsc				

PRIVILEGED-LEVEL ACCESS AGREEMENT ACCEPTABLE USE POLICY (AUP)

PRIVILEGED-LEVEL ACCESS AGREEMENT (PAA) & ACKNOWLEDGEMENT OF RESPONSIBILITIES

___ (INITIALS) I understand that I have access to *classified and unclassified network* Department of Defense (DoD) Information System (IS), and that I have and will maintain the necessary clearances and authorizations for privileged-level access to (*specify what IS privileges are being granted*).

As a privileged-level user,

___ (INITIALS) I will protect the **root, administrator, or superuser** account(s) and authenticator(s) to the highest level of data or resource it secures.

___ (INITIALS) I will **NOT** share the **root, administrator, or superuser** account(s) and authenticator(s) entrusted for my use.

___ (INITIALS) I am responsible for all actions taken under my account and understand that the exploitation of this account would have catastrophic effects to all networks for which I have access. I will **ONLY** use the special access or privileges granted to me to perform authorized tasks or mission related functions. I will only use my privileged account for official administrative actions.

___ (INITIALS) I will not attempt to "hack" the network or connected ISs, subvert data protection schemes, gain, access, share, or elevate permissions to data or ISs for which I am not authorized.

___ (INITIALS) I will protect and label all output generated under my account to include printed materials, magnetic tapes, external media, system disks, and downloaded files.

___ (INITIALS) I will immediately report any indication of computer network intrusion, unexplained degradation or interruption of system or network services, illegal or improper possession of content or files, or the actual or possible compromise of data, files, access controls, or systems to the Information Systems Security Manager (ISSM).

___ (INITIALS) I will **NOT** install, modify, or remove any hardware or software (i.e. freeware/shareware, security tools, etc.) without permission and approval from ISSM.

___ (INITIALS) I will not install unauthorized or malicious code, backdoors, software (e.g. games, entertainment software, instant messaging, collaborative applications, etc) or hardware.

___ (INITIALS) I am prohibited from obtaining, installing, copying, pasting, modifying, transferring or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade-secret, or license agreements.

___ (INITIALS) I will not create or elevate access rights of others; share permissions to ISs for which they are not authorized; nor allow others access to IS or networks under my privileged account.

___ (INITIALS) I am prohibited from casual or unofficial web browsing and use of email while using the privileged-level account. This account will NOT be used for day-to-day network communications.

___ (INITIALS) I am prohibited from accessing, storing, processing, displaying, distributing, transmitting and viewing material that is; pornographic, racist, defamatory, vulgar, hate-crime related, subversive in nature, or involves chain letters, spam, or similarly related criminal offenses such as encouragement of criminal activity, or violation of State, Federal, national, or international law.

___ (INITIALS) I am prohibited from storing, accessing, processing, sharing, removing, or distributing Classified, Proprietary, Sensitive, Privacy Act, and other protected or privileged information that violates established security and information release policies.

___ (INITIALS) I am prohibited from promoting partisan political activity, disseminating religious materials outside an established command religious program, and distributing fund raising information on activities, either for profit or non-profit, unless the activity is specifically approved by the command (e.g. command social-event fund raisers, charitable fund raisers, etc).

___ (INITIALS) I am prohibited from using, or allowing others to use, Marine Corps resources for personal use or gain such as posting, editing, or maintaining personal or unofficial home pages, web-blogs, or blogging sites, advertising or solicitation of services or sale of personal property (e.g. eBay) or stock trading.

___ (INITIALS) I am prohibited from employing, using, or distributing personal encryption capabilities for official electronic communications. I will contact the Cyber Security Office if I am in doubt as to any of my roles, responsibilities, or authorities.

___ (INITIALS) I understand that all information processed on ISs is subject to monitoring. This includes E-mail and Web Browsing.

___ (INITIALS) I will obtain and maintain required certification(s) in accordance with Marine Corps policy to retain privileged level access.

___ (INITIALS) I understand that failure to comply with the above requirements is a violation of the trust extended to me for the privileged access roles and may result in any of the following actions:

- a. Chain of command revoking IS privileged access and/or user privileges.
- b. Counseling.
- c. Adverse actions under the UCMJ and/or criminal prosecution.
- d. Discharge or Loss of Employment.
- e. Revocation of Security Clearance.

User Acknowledgement

Name: _____

CAC DoD EDI Personal Identifier (EDIPI) (10 digit #): _____

Signature: _____ Date: _____

Cyber Security Endorsement

ISSM Name: _____

ISSM Signature: _____

**PRIVILEGED-LEVEL ACCESS AGREEMENT
ACCEPTABLE USE POLICY (AUP)
CERTIFICATE OF NON-DISCLOSURE**

DISCLOSURE OF PROTECTED OR PRIVILEGED INFORMATION

Whoever, being an officer, employee or agent of the United States or of any department, agency or contractor thereof, publishes, divulges, discloses or makes known in any manner or to any extent not authorized by law, any information coming to him/her in the course of their employment or official duties, which information concerns or relates to the trade secrets or proprietary information of a non-Federal government entity; any information protected by the Privacy Act; any information subject to protection under the Freedom of Information Act; other law, regulation, or policy (including all privileged communications such as doctor-patient, attorney-client, etc.); any information protected under the classification system set forth in DoDI 5239.1; or any other information protected by law or regulation (i.e. IG, AAA, CID); shall, in addition to any penalty imposed by said law or regulation, be subject to UCMJ, administrative, or contract remedy enforcement.

CERTIFICATION

I have read the provisions herein and I understand my responsibility not to disclose any matters connected with or pertaining to these provisions as they pertain to the (INSERT NETWORK) except to persons theretofore listed as having a need to know.

Signature: _____

CAC DOD EDI Personal Identifier (EDIPI) (10 digit #)

Name: _____

Date: _____