NAVY REGION JAPAN FRONTLINE USER ACCOUNT REQUEST

TYPE OF REQUEST	DATE
☐ CREATION ☐ MODIFICATION ☐ DEACTIVATION ☐ REACTIVATION	

SYSTEM	LOCATION

PART 1. REQUEST FOR ACCESS (*To be completed by Requester)*

1. USER NAME	2. JOB TITLE
3. DEPARTMENT	4. PHONE

5. TRAINING REQUIREMENTS

5a. CYBER AWARENESS	5b. OPSEC AWARENESS	5c. ID AND SAFEGUARD PII	5d. PCI-DSS

USER AGREEMENT AND RESPONSIBILITIES

By signing this document, I agree that as a user I am responsible for access to and entries made in the systems under my User ID and fully accept the responsibilities of those actions. I will

- Access only the information and data required to perform day-to-day duties;
- Follow all Standard Operating Procedures and guidance applicable to perform my duties and utilize the system;
- Not provide any unauthorized person or organization access to departmental information or systems;
- Follow all applicable rules for passwords, including but not limited to:
  - Not storing passwords on or near workstations,
  - Creating passwords that follow length and complexity requirements,
  - Choosing passwords that cannot be easily guessed,
  - Not disclosing passwords to any other person or organization, and
  - Resetting/changing passwords as required.

6. USER SIGNATURE	7. DATE

PART 2. ENDORSEMENT OF ACCESS (*To be completed by Information Owner, User Supervisor, or Government Sponsor)*

8. ENDORSER NAME	9. JOB TITLE
10. EMAIL	11. PHONE

12. DETAIL OF AND JUSTIFICATION FOR ACCESS

ENDORSER AGREEMENT AND RESPONSIBILITIES

By signing this document, I certify and authorize the user identified above for access to the system as requested. I will

- Ensure the user is only given access necessary to perform their duties;
- Ensure the user has been properly trained on the system and procedures;
- Ensure separation of duties, where required and possible, is not compromised;
- Immediately notify the IT Department to remove access if the user no longer needs it to perform their duties;
- Immediately notify the IT Department to remove access if the user has separated from the organization.

13. ENDORSER SIGNATURE	14. DATE

Part 3. IT DEPARTMENT USE ONLY

15. USER ID(S) ASSIGNED		16. ROLE(S) ASSIGNED	
17. DATE PROCESSED		18. PROCESSED BY	

RESET

v3.0

Instructions

A. TYPE OF REQUEST: The requestor must indicate if this request is for creation of a new user account; or a modification, deactivation, or reactivation of an existing user account.

B. DATE: The date the form is started.

C. SYSTEM: The requestor must indicate for which system(s) the user account is being requested. The requestor can select multiple systems by holding down the CTRL button during selection.

D. LOCATION: The location where the user account will be used to access the system.

E. PART 1: The following information is provided by the user when establishing or modifying their user account.

(1) Name. The last name, first name, and middle initial of the user.

(2) Job Title. The civilian job title (Example: Front Desk Clerk) of the user.

.

(3) Department. The user's department or organization.

(4) Phone. The Defense Switching Network (DSN) phone number of the user. If DSN in unavailable, indicate commercial number.

(5) Training Requirements. The user must declare the date of their annual

(5a) Cyber Awareness,
(5b) OPSEC Awareness,
(5c) Identifying and Safeguarding PII, and
(5d) PCI-DSS

trainings and attach the completion certificates to this form at submission.

(6) User Signature. The user must sign the form with the understanding that they are responsible and accountable for their password(s) and access to system(s) as described in the User Agreement and Responsibilities.

(7) Date. The date the user signs the form.

F. PART 2: The request requires endorsement from the user's Supervisor or the Government Sponsor. Alternatively, the Information Owner or functional appointee of the office responsible for approving access to the system being requested can endorse.

(8) Endorser Name. The last name, first name, and middle initial of the approver.

(9) Job Title. The civilian job title (Example: Theater Manager) of the endorser.

(10) Email. The endorser's official email address.

(11) Phone. The DSN phone number of the endorser. If DSN is unavailable, indicate commercial number.

(12) Detail of and Justification for Access. A brief statement to explain access details and justify establishment of an initial user account, or appropriate information if the user account or access to the current user account is modified.

(13) Endorser Signature. The endorser must sign the form with the understanding that they are responsible and accountable for ensuring the appropriateness of the user's access and are authorizing the same as described in the Endorser Agreement and Responsibilities.

(14) Date. The date the endorser signs the form.

G. PART 3: The following information is provided by the IT Department to record and specifically identify the user account and access permissions provided to the user.

(15) User ID(s) Assigned. The USER ID(s) in the requested system(s) assigned to the user.

(16) Role(s) Assigned. The role(s) and/or permission(s) in the requested system(s) assigned to the USER ID(s) assigned to the user.

(17) Date Processed. The date the IT staff processed the form.

(18) Processed by. The IT staff who processed the form must sign to attest completion of the access request process.