Appointment Letter Template (Technical I - III)

Date (MM/DD/YYYY)

Major Command

Office Symbol

Sub Organization

MEMORANDUM FOR RECORD

SUBJECT: Designation of Cybersecurity (CS) Support Personnel

1. References: AR 25-2 Chapter 3 and DoD 8570.01-M.

2. Effective immediately, the below individual is appointed to perform Cybersecurity duties and functions for the category and level below.

Full name

Duty position/role

AKO or EE mail address

Civilian series/ MOS

Personnel Category

IT Position Category

Supervisor AKO/EE mail address/phone number

Contract #/Expiration date

IT Support Services

CYBERSECURITY CATEGORY AND LEVEL

Primary Duty

Additional/Embedded

3. Purpose: To perform Cybersecurity functions and duties IAW the DoD 8570.01M category and level listed above.

4. Period: Until officially relieved or released from appointment, or upon transfer, termination, reassignment, retirement or discharge.

5. Special instructions:

a. Register in the Army Training and Certification Tracking System (https://atc.us.army.mil).

b. Complete required IA training and certification for category/level. Review the IA Training and Certification BBP.

c. Complete and sign Privileged Access Agreement (PAA)/Non-Disclosure Agreement and Acceptable Use Policy then upload in ATCTS.

d. Ensure the DD 2875 is signed in part IV by the servicing Network Enterprise Center/Service Provider noting elevated privileges are approved/denied.

6. Soldiers annotated as 25B/25U w/supervised access will sign a PAA and work under the direct supervision of an IATI or higher baseline certified DA civilian or military individual. They will be designated as 25B/25U w/ supervised access in ATCTS and meet the Computing Environment certification or certificate of training requirement per DoD 8570.01-M. Personnel in this category are not authorized certification vouchers from Army CIO/G6 voucher program.

Name of commander or designee signing letter

Position/Role

Grade

Signature

Functions/responsibilities-Check all that apply

- ☐ Install perimeter defense systems including intrusion detection systems, firewalls, grid sensors, etc., and enhance rule sets to block sources of malicious traffic.
- ☐ Write and maintain scripts for the NE.
- ☐ Recommend, schedule, and/or implement IA related repairs within the enclave environment
- ☐ Coordinate and/or provide support for all enclave applications and operations.
- ☐ Lead teams and/or support actions to quickly resolve or mitigate IA problems for the enclave environment.
- ☐ Support the installation of new or modified hardware, operating systems, and software applications ensuring integration with IA security requirements for the enclave
- ☐ Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action.
- ☐ Direct and/or implement operational structures and processes to ensure an effective enclave IA security program including boundary defense, incident detection and response, and key management.
- ☐ Evaluate functional operation and performance in light of test results and make recommendations regarding C&A.
- ☐ Examine enclave vulnerabilities and determine actions to mitigate them.
- ☐ Monitor and evaluate the effectiveness of enclave IA security procedures and safeguards.
- ☐ Establish enclave logging procedures to include: important enclave events, services and proxies, log archiving facility.
- ☐ Implement and maintain perimeter defense systems including, but not limited to, intrusion detection systems, firewalls, grid sensors
- ☐ Other

- ☐ Examine potential security violations to determine if the NE policy has been breached, assess the impact, and preserve evidence.
- ☐ Recognize a potential security violation, take appropriate action to report the incident as required by regulation, and mitigate any adverse impact.
- ☐ Provide end user IA support for all CE/NE or Enclave operating systems, peripherals, and applications.
- ☐ Support, monitor, test, and troubleshoot hardware and software IA problems pertaining to their CE or NE
- ☐ Apply CE specific IA program requirements to identify areas of weakness. Apply appropriate CE access controls.
- ☐ Install and operate the IT systems in a test configuration manner that does not alter the program code or compromise security safeguards.
- ☐ Conduct tests of IA safeguards in accordance with established test plans and procedures. Implement and monitor IA safeguards for CE system(s) in accordance with implementation plans and standard operating procedures.
- ☐ Comply with system termination procedures and incident reporting requirements related to potential CE security incidents or actual breaches.
- ☐ Implement online warnings to inform users of access rules for CE systems.
- ☐ Implement applicable patches including IA vulnerability alerts (IAVA), IA vulnerability bulletins (IAVB), and technical advisories (TA) for the CE or NE or Enclave operating system(s).
- ☐ Install, test, maintain, and upgrade CE operating systems software and hardware to comply with IA requirements.
- ☐ Implement DoD and DoD Component password policy.
- ☐ Perform IA related customer support functions including installation, configuration, troubleshooting, customer assistance, and/or training, in response to customer requirements for the NE.
- ☐ Analyze patterns of non-compliance and take appropriate administrative or programmatic actions to minimize security risks and insider threats.
- ☐ Manage accounts, network rights, and access to NE systems and equipment.
- ☐ Identify IA vulnerabilities resulting from a departure from the implementation plan or that were not apparent during testing.
- ☐ Configure, optimize, and test network servers, hubs, routers, and switches to ensure they comply with security policy, procedures, and technical requirements.
- ☐ Ensure that hardware, software, data, and facility resources are archived, sanitized, or disposed of in a manner consistent with system security plans and requirements.
- ☐ Develop and implement access control lists on routers, firewalls, and other network devices.
- ☐ Other

ADDITIONAL DETAILS FOR FUNCTIONS