Appointment letter template: Cyber Information Technology (IT) (IATI-III)

Reset Form

Date (MM/DD/YYYY)

Major Command

Office Symbol

Sub Organization

MEMORANDUM FOR RECORD

SUBJECT: Designation of Cyber IT Support Personnel

1. References: AR 25-2, DoDD 8140.01 and DOD 8570.01-M.

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

Full name

Duty position/role

EE mail address

Civilian series/ MOS

Personnel Category

IT Position Category

Supervisor EE mail address/phone number

Contract #/Expiration date

IT Support Services

Proficiency Level

CYBERSECURITY IT Category and Level

Primary Duty

Additional/Embedded

3. Purpose: To perform Cybersecurity functions and duties IAW the DOD 8570.01M category and level and DoD Cyberspace workforce Framework task 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 CS training and certification for category/level. Review the IA Training and Certification BBP/DA PAM when signed.

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

d. Complete and sign privileged access agreement (PAA) and Acceptable Use Policy then upload in ATCTS.

6. Soldiers annotated as 25B/25U with 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 DCWF as a General User. They must 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 the 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.
- ☐ Provide recommendations on data structures and databases that ensure correct and quality production of reports/management information.
- ☐ Develops and administers databases and/or data management systems that allow for the storage, query, protection, and utilization of data.
- ☐ Troubleshoot hardware/software interface and interoperability problems.
- ☐ Manage accounts, network rights, and access to systems and equipment.
- ☐ Plan, execute, and verify data redundancy and system recovery procedures.
- ☐ Addresses problems; installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support). Typically provides initial incident information to the Incident Response (IR) Specialty
- ☐ Install, update, and troubleshoot systems/servers.
- ☐ Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.
- ☐ Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
- ☐ Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.
- ☐ Design, build, implement, and maintain a knowledge management framework that provides end-users access to the organization's intellectual Capital.
- ☐ Test and maintain network infrastructure including software and hardware devices.
- ☐ Provide end user IA support for all CE/NE or Enclave operating systems, peripherals, and applications.
- ☐ Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.
- ☐ Performs configuration management, problem management, capacity management, and financial management for databases and data management systems.
- ☐ Ability to manage Communications Security (COMSEC) material accounting, control and use procedure.
- ☐ Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.
- ☐ Studies an organization's current computer systems and procedures, and designs information systems solutions to help the organization operate more securely, efficiently, and effectively. Brings business and information technology (IT) together by understanding the needs and limitations of both.
- ☐ Perform backup and recovery of databases to ensure data integrity.
- ☐ Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).
- ☐ Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.
- ☐ Administer accounts, network rights, and access to systems and equipment.
- ☐ Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration
- ☐ Analyze patterns of non-compliance and take appropriate administrative or programmatic actions to minimize security risks and insider threats.
- ☐ Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.
- ☐ Diagnose and resolve customer reported system incidents, problems, and events.
- ☐ Configure, optimize, and test network servers, hubs, routers, and switches to ensure they comply with security policy, procedures, and technical requirements.
- ☐ Recognize a possible security violation and take appropriate action to report the incident, as required.

ADDITIONAL DETAILS FOR FUNCTIONS