# Personnel Security Procedure

|  |  |  |  |
| --- | --- | --- | --- |
| Procedure Owner |  |  | |
| Procedure Approver(s) |  |
| Effective Date |  | Next Review Date |  |

# Purpose

The purpose of this procedure is to define a consistent approach to manage Personnel Security of the IT environment at Applied Information Sciences.

# Scope

This procedure is consistent with CMMC and covers all personnel security procedures within Applied Information Sciences environment. This procedure will be followed by all employees of Applied Information Sciences. The CMMC System Security Plan (SSP) will be updated to reflect any significant modifications made to this procedure.

# Definitions

**Employees**: All individuals belonging to one or many groups defined below:

1. All individuals associated with Applied Information Sciences through an employee – employer relationship or contract between Applied Information Sciences and their employer or Applied Information Sciences and individual.
2. All individuals possessing equipment issued by Applied Information Sciences
3. All individuals working on the premises of Applied Information Sciences and/or utilizing the Internet services provided by Applied Information Sciences.

# Governing Laws, Regulations, and Policies

* NIST SP 800-171, 3.9.1 - 3.9.2
* CMMC PS.L2-3.9.1 – PS.L2-3.9.2
* Applied Information Sciences – PS – 3.9 - Personnel Security Policy

# Procedure Statements

**PS.L2-3.9.1 – Screen individuals prior to authorizing access to organizational systems containing CUI:**

1. Personnel security screening (vetting) activities involve the evaluation/assessment of individual’s conduct, integrity, judgment, loyalty, reliability, and stability (i.e., the trustworthiness of the individual) prior to authorizing access to organizational systems containing Controlled Unclassified Information (CUI). The screening activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and specific criteria established for the level of access required for assigned positions.
   * + - Applied Information Sciences has an established personnel security program to ensure compliance with all DoD personnel security requirements for access to Controlled Unclassified Information (CUI). Employees who need access to CUI undergo the following screening before being granted access:
         * Prior to employment:
   1. Criminal check
   2. Employment and Education check
   3. Drug Screening
   4. Citizenship check
   5. Social Security Check
      * + Applied Information Sciences has an established personnel security program to ensure compliance with all DoD personnel security requirements for access to Controlled Unclassified Information (CUI). Employees who need access to CUI undergo the following screening before being granted access:
          - A System Authorized Access Request (SAAR) form is completed indicating the user’s position and authorized access
          - A Non-Disclosure Agreement (NDA) is completed by the user to protect confidential and proprietary information
        + The SAAR and NDA are the access documents signed by all personnel before being granted access to the IS. The SAAR and appointment letter are reviewed annually and at the time any personnel are transferred laterally to an organization that requires different authorized access to the IS. Individuals requiring access to organizational information and IS re-sign access agreements to maintain access to organizational information systems when access agreements have been updated.

**PS.L2-3.9.2** **– Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers:**

1. Upon termination of individual employment, Applied Information Sciences retains access to information and information systems formerly controlled by the terminated individual. the following actions taken by appropriate designated staff are required within the 24 hour timeline:
   * Conduct exit interview to remind employee of responsibilities as documented in the SAAR, NDA, and CUI protection obligations
   * Revoke employee authorization immediately
   * Retrieve all hardware, software, and documentation, including government equipment used at home
   * Retrieve Physical Access instruments such as keys, smart cards, tokens, badges, etc.
   * Remove all access permissions to critical/sensitive areas, such as telephone closets, computer rooms, and areas containing CUI
   * Delete the employee’s account and password from all systems and networks; to include any external communication User IDs
2. Applied Information Sciences manages all personnel onboarding / out-processing processes through Human Resources. Applied Information Sciences reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned, terminated, or transferred to other positions within the organization.

* The SAAR is reviewed annually and when any personnel are transferred laterally within the organization requiring different authorized access to the IS. The SAAR is the vehicle that is utilized to grant/revoke/modify access to the IS that are applicable to the transfer. <role> is notified immediately when individuals are transferred or reassigned to other positions within the organization. <role> or designee of, will modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer. Applied Information Sciences does not manage transfers to outside organizations. This type of transfer would be considered a termination.

1. Applied Information Sciences ensures that organizational systems containing CUI are protected during and after personnel actions such as transfers.

* Employee access to CUI is removed or modified when they transfer to a new department. When employment or program access is changed for any reason, the following actions are required within the 24 hour timeline.
* All company IT equipment (e.g., laptops, cell phones, storage devices) are returned or modified
* All identification, access cards, and keys are returned or modified
* An exit interview is conducted to remind the employee of their obligations to not discuss CUI, even after employment or transfer to a new position
* Remove access to all accounts granting access to CUI or modify access to CUI as appropriate for a new work role
* Disable or modify employee accounts If applicable
* Limit access to physical spaces with CUI for departing employees or those who transition to a work role that does not require access to CUI
* The <role> or Data Owner is notified of the change in access authorization

# Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| **Role** | **Responsibilities** | **Contact Information** |
|  |  |  |
|  |  |  |
|  |  |  |

# Non-Compliance

Violations of this policy will be treated like other allegations of wrongdoing at Applied Information Sciences. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable Applied Information Sciences policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
| V.01 | 11/21/2022 | Securestrux | Initial draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |