Organizational Security Awareness

Table of Contents

- **Getting Started** | **Overview** | **Resources** | **Standards**
- **Prior to Employment**
- **During Employment**
- **Termination and Change of Employment**

Getting Started

As cited in a variety of sources, people are often described as the weakest link in any security system. It is important to build security into the entire Human Resource (HR) process, from pre-employment, during employment, and through termination, to ensure that policies and procedures are in place to address security issues. Consistent training throughout the entire process ensures that employees and contractors are fully aware of their roles and responsibilities and understand the criticality of their actions in protecting and securing both information and facilities.

In collaboration with Human Resources staff, evaluate HR department policies and procedures to verify whether institutional supervisors and employees:

1. **Review and acknowledge** understanding (documented) of your institution's Acceptable Use policy.
2. **Require** contractors, part-time staff, and student workers to review and comply with the Acceptable Use Policy and sign NDA's or confidentiality agreements if appropriate given their levels of access to institutional information.
3. **Understand** the HR disciplinary process for policy violations.
4. **Comply** with HR requirements for new hire background checks.
5. **Develop** job descriptions which include information security responsibilities and adequate separation of duties where applicable.
6. **Provide** ongoing information security awareness training opportunities for staff, faculty, and students.
7. **Provide** HR and IT with the most current status of staff, faculty, student workers, and part-time staff employed by the institution to assist with account provisioning and terminations.
8. **Return** institutional assets as required by HR policies/procedures when terminating employment.

Top of page

Overview

Employees handling personal data in an organization need to receive appropriate awareness training and regular updates in an effort to safeguard the data entrusted to them. Appropriate roles and responsibilities assigned for each job description need to be defined and documented in alignment with the organization's security policy. The institution's data must be protected from unauthorized access, disclosure, modification, destruction or interference. The management of human resources security and privacy risks is necessary during all phases of employment association with the organization. Training to enhance awareness is intended to educate individuals to prevent data disclosure, recognize information security problems and incidents, and respond according to the needs of their work role.

Safeguards include the following:

- Job descriptions and screening,
- user awareness and training,
- a disciplinary process, and
- an orderly exit process must exist to equip employees to operate securely and use information appropriately, and ensure that access privileges change when a user's relationship with the University changes.

The objective of Human Resources Security is to ensure that all employees (including contractors and any user of sensitive data) are qualified for and understand their roles and responsibilities of their job duties and that access is removed once employment is terminated. The three areas of Human Resources Security are:

- **Prior to Employment:** This topic includes defining roles and responsibilities of the job, defining appropriate access to sensitive information for the job, and determining depth of candidate's screening levels - all in accordance with the company's information security policy. During the phase, contract terms should also be established.
- **During Employment:** Employees with access to sensitive information in an organization should receive periodic reminders of their responsibilities and receive ongoing, updated security awareness training to ensure their understanding of current threats and corresponding security practices to mitigate such threats.
- **Termination and Change of Employment:** To prevent unauthorized access to sensitive information, access must be revoked immediate upon termination/separation of an employee with access to such information. This also includes the return of any assets of the organization that was held by the employee.

Top of page

Prior to Employment

Objective: To develop a comprehensive process that includes identification of job roles and responsibilities, identify the corresponding candidate screening level for those roles and responsibilities and establish terms and conditions of employment.

Prior to hiring or contracting employees or companies, security roles and responsibilities should be clearly articulated in job descriptions or well defined in contract terms and conditions. These roles and responsibilities should be defined in accordance with the institution's security policies.

Careful attention should be paid to validation of references and the appropriate level of background checks as determined by the security roles and responsibilities of the position or contract. Consideration should be given that the receipt of affirmative references and the successful completion of a background check at a level commensurate with the position's roles and responsibilities be a condition of hire.

- Virginia Tech Policy and Procedures for Conviction and Driving Record Investigation

Top of page

During Employment

Objective: To ensure that employees are aware of and understand their roles and responsibilities; to ensure that they understand information security threats and; to ensure they have the necessary knowledge to mitigate those threats.

- Employee Orientation for new employees: All new employees should participate in new employee orientation workshops or be provided with pertinent information including security policies and procedures and potential disciplinary process/actions for any security breaches. Additionally, new employees should be required to sign an acknowledgement indicating that they read and understand the institution's acceptable use policy, the institution's security policies and any non-disclosures (if applicable). All managers and supervisors should be expected to emphasize the importance of security to their employees. This is one example of an institution's Supervisor's Guide to Information & Security Policy.
- Ongoing Education and Awareness Training: Institutions should provide relevant information security information delivered on a defined schedule (annually, bi-annually, etc.) appropriate to the employee's job roles and responsibilities. All employees should be required to take a general training on basic information security practices and/or acknowledge their basic understanding of the institution's security policies and procedures.
- A process for official disciplinary actions for security breaches should be established and promulgated to the institution's employees.

Top of page

Termination and Change of Employment

Objective: To develop an orderly exit process to ensure that access is removed and assets returned in an expedited time frame.

Responsibilities for performing employee terminations must be clearly defined and assigned to ensure actions are taken as quickly as possible. A checklist listing actions to be taken and the person responsible for the execution of that action allows for quick identification of any missed steps. (CSO offers this brief checklist for a secure employee departure.)

Specifically, there should be a process that validates that all the institution's assets are returned at termination.

Additionally, there should be a process that ensures access to information assets are removed at the time of termination.

Top of page

Resources

EDUCAUSE Resources

EDUCAUSE Resource Center Pages

- Acceptable and Responsible Use Policies
- Certification, Education, Training, and Tutorials
- Executive Security Awareness
- Security Awareness
- Training
- User Training

HEISC Toolkits/Guidelines

- CISO Job Description Template
- Collaborating with Faculty
- Cybersecurity Awareness Resource Library
- National Cyber Security Awareness Month (NCSAM) Resource Kit
- Top Information Security Concerns for HR Leaders & Process Participants – Protecting Your HR Assets
- Top Information Security Concerns for Researchers
- Top Information Security Concerns for Campus Executives & Data Stewards

Initiatives, Collaborations, & Other Resources

- Mitigating Top EDU Human Risks (video - 47 min.)
- ThinkingCIO blog: Recognizing and Handling Safety Issues (October 2015)
- Virginia Tech Policy and Procedures for Conviction and Driving Record Investigation

Top of page

Standards

ISO	NIST	COBIT	PCI DSS	2014 Cybersecurity Framework	HIPAA Security
27002:2013 Information Security Management **Chapter 7**: Human Resources Security	**800-12**: An Introduction to Computer Security - The NIST Handbook Chapter 3 - Roles and Responsibilities Chapter 10 - Personnel/Users Issues Chapter 13 - Awareness, Training and Education **800-100**: Information Security Handbook: A Guide for Managers **800-50**: Building an Information Technology Security Awareness and Training Program **800-14**: Generally Accepted Principles and Practices for Securing Information Technology Systems	**APO01.06** **APO07.01** **APO07.02** **APO07.03** **APO07.04** **APO07.05** **APO13.12** **BAI05.07** **DSS06.03**	**Req 6** **Req 12**	**ID.GV-2** **PR.AT-1** **PR.AT-2** **PR.AT-3** **PR.AT-4** **PR.AT-5** **PR.DS-5** **PR.IP-11**	**45 CFR 164.308(a)(3)**

Top of page

Questions or comments? Contact us.

Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0).