13.1.2 Personnel Policy Facts

This lesson covers the following topics:

- Vulnerabilities
- Pre-employment policies
- Onboarding policies
- Security awareness training
- Daily operational policies
- Offboarding policies

Vulnerabilities

Employees can present a high-level security risk. The following table defines common employee-related security vulnerabilities.

Vulnerability	Description
Fraud	*Fraud* is the use of deception to divert company assets or profits to an employee. An example of a situation in which fraud is possible is where the same employee both issues a product and takes payment for the product. Separation of duties is the most effective method for preventing fraud. Mandatory vacations are one way to help detect fraud. An organization can compare if the activity ceases to happen only when a specific employee is away.
Collusion	*Collusion* is a situation in which multiple employees conspire to commit fraud or theft. Collusion is designed to overcome the separation of duties countermeasures. The following example demonstrates how collusion would be required for theft of company assets: ▪ An employee is responsible for ordering equipment. ▪ A second employee is responsible for approving purchase orders for the equipment. ▪ A third employee is responsible for taking possession of equipment. ▪ A fourth employee is responsible for inventorying equipment. In the case of collusion, all four employees would have to be involved for the equipment to be stolen. Possible methods for collusion protection are: ▪ Separation of duties. ▪ Two-man control. ▪ Principle of least privilege. ▪ Mandatory vacations (which allow problems to surface and gives you time to audit the system while the employee is away).

Pre-employment Policies

To ensure that a prospective employee is a low-security risk, an organization should perform pre-employment processing. A pre-employment processing checklist should include the following activities:

- Perform a background check of the prospective employee. These checks may include criminal records, credit reports, drug testing, identity verification, previous employers, social security verification, driving records, and reference checks.
- Perform a background check of the prospective employee's references.

- Verify the prospective employee's educational declaration.
- Verify the prospective employee's job history.
- Conduct a criminal background check.
- Obtain a credit history (if appropriate).
- Perform a social media analysis to gather information on a potential employee's online presence.

Onboarding Policies

Onboarding is the process followed when setting up a partnership with a new employee. While this process primarily involves a lot of HR paperwork, it also involves setting up a work environment for the employee. There are a few onboarding procedures that security professionals should understand. Consider the following documentation when onboarding an employee:

Documentation	Description
Non-disclosure agreement (NDA)	An NDA is a contract in which both parties agree not to share proprietary or confidential information gathered during the business relationship.
Non-compete agreement	A non-compete agreement states that an employee will not work for or work with a competing organization for a set period during or after employment with your organization.
Acceptable use policy (AUP)	The AUP defines how users should use information and network resources in the organization. For example, it might identify the employees' rights to use company property, such as internet access and computer equipment, for personal use.

Security Awareness Training

To enforce security policy measures, implement appropriate technical and procedural controls that adequately protect systems and data. However, even the best control can fail if users are not properly informed or trained. It is important that each employee who uses, relies on, or manages some aspect of your organization's information systems understands the specific information security responsibilities.

The goals of a security awareness training program include making employees aware of:

- The security policy.
- Threats to the company's assets.
- Laws, regulations, and guidelines that employees are required to follow.
- Sensitive information and how to protect it.
- Identification and reporting of events, such as social engineering, theft, and other violations of the security policy.

Consider the following concepts when designing training for your new and existing employees:

Concept	Description
Gamification	Gamification involves using games to help teach, practice, and retain information.
Phishing simulations	A phishing simulation can be used to provide employee awareness and can help to reduce the effectiveness of potential phishing attacks.

Computer-based training (CBT)	CBT is delivered through a computer. It could be through a software application or it could be provided over the internet
Role-based training	Training on the standards, procedures, and baselines that apply to the employee's specific job.

Daily Operational Policies

Here are some organizational policies to consider for the day-to-day employee operations within your organization.

Policy	Description
Job rotation	A requirement for job rotation cross-trains individuals and rotates users between positions on a regular basis. Job rotation helps to catch irregularities that could arise when one person is unsupervised over an area of responsibility.
Mandatory vacation	A requirement for mandatory vacations requires employees to take vacations of a specified length. These vacations can be used to audit actions taken by the employee and provide a passage of time during which problems caused by misconduct could become evident.
Separation of duties	Separation of duties restricts the amount of access or influence an employee has, thereby removing single points of failure within the organization
Least privilege	The concept of least privilege ensures that a user has access only to the information and resources needed to effectively do the employee's job.
Clean desk space	A clean desk policy requires employees to clear their desks when they are away. All notes and documents should be properly stored or disposed of and should not be left laying on an employee’s desk.

Offboarding

Offboarding is the process followed when ending a relationship with an employee or other third party. This termination process identifies the tasks an organization takes when an employee voluntarily or involuntarily leaves the organization. This is a key area in which the proper processes can ensure the protection of company assets. Always use a checklist to ensure that you have completed all the appropriate tasks. Items on the checklist should include:

- Disable the user account, including physical access, electronic access, and telephone access.
- Perform an exit interview. The exit interview may help to reduce the number of frivolous lawsuits related to employee termination. During the exit interview, the employee should always sign a statement indicating agreement with the reason for termination. When an employee has been terminated for violation of the security policy, a signature agreeing to the reason for termination is especially important because:
  - The signature can be used as evidence that the employee violated a security policy.
  - The employee recognizes the violation.
  - The employee also recognizes that it was grounds for termination.

Copyright © 2022 TestOut Corporation All rights reserved.