3.7.2 Employee Management Facts

Employee management is the implementation of processes to ensure that employees play a major role in protecting company assets. An organization should hire and develop professionals who are right for the jobs needed. Employees are human beings, so they function better when they are being paid fairly, can enjoy offered benefits and incentives, and are heard by their employer. Communication between employee and organization is very important and can lead to better attitude and performance. Three important principles that should be part of every employee management decision are:

- The principle of *least privilege*, which specifies that an employee is granted the minimum privileges required to perform duties of the position. If an employee has too much access, they could intentionally or unintentionally compromise security.
- The principle of *separation of duties*, which specifies that for any task in which vulnerabilities exist, steps within the tasks are assigned to different positions with different management. This is usually done by dividing a project into different teams responsible for different steps.
- The principle of *two-man control*, which specifies that certain tasks should be dual-custody in nature to prevent a security breach.

The following table defines common employee-related security vulnerabilities:

Vulnerability	Definition
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 only ceases to happen 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 countermeasure. 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 in order 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).

Employee security should start before an employee starts work and continue after the employee leaves. The following table lists recommendations for each employment stage.

Employment Process	Description
Pre-Employment	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 job history. - Verify the prospective employee's educational declaration. - Conduct a criminal background check. - Obtain a credit history (if appropriate).
Employment	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 that uses, relies on, or manages some aspect of your organization's information systems understands their specific information security responsibilities. The goals of a security awareness training program include making employees aware of: - The security policy. - The standards, procedures, and baselines that apply to the employee's specific job. This is referred to as *role-based training*. - Threats to the company's assets. - Laws, regulations, and guidelines 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.

	In addition to formal security awareness training, implement security policy reminders as reinforcement, such as: - Banners posted throughout the organization, especially the places in which employees gather. - Inclusion of a security section in newsletters. - Reminders of security policy and currently relevant topics, such as virus protection or disaster recovery. Many organizations use continuous background checks to ensure that they are aware of any criminal activity on the part of an employee. This can only be done, however, with the authorization and consent of the employee.
Termination	The *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. - Remind the employee of any agreements related to non-disclosure and non-compete. - Collect all company assets, including: - Hardware, such as laptops and cell phones. - Software issued to the employee. - Identification badges, such as smart cards, swipe cards, security keys, etc. - Printed documents that the employee may possess. - Passwords used for user accounts. This simplifies the recovery of encrypted documents that might be stored on their workstations. - Archive email and voice mail. - Clean out the employee's workspace for them and supply the employee-owned materials at the exit interview. - Escort the employee off of the premises.

Security awareness increases the security of an organization by training employees on security procedures. Security awareness should include:

- Security training, including:
  - How to recognize security breaches and exploits when they occur
  - What to do in the event of a security breach
  - Sample scenarios and recommended responses
- Security retraining to train employees on new security issues and refresh them on issues in previous training.
- Random security audits to identify how well employees are implementing security policies.