

Personnel Security *(Security Awareness)*

COBIT

Communication of IT Security Awareness

An IT security awareness program should communicate the IT security policy to each IT user and assure a complete understanding of the importance of IT security. It should convey the message that IT security is to the benefit of the organization, all its employees, and that everybody is responsible for it. The IT security awareness program should be supported by, and represent, the view of management.

Roles and Responsibilities

Management should clearly define roles and responsibilities for personnel, including the requirement to adhere to management policies and procedures, the code of ethics and professional practices. The terms and conditions of employment should stress the employee's responsibility for information security and internal control.

Personnel Training

Management should ensure that employees are provided with orientation upon hiring and with on going training to maintain their knowledge, skills, abilities and security awareness to the level required to perform effectively. Education and training programs conducted to effectively raise the technical and management skill levels of personnel should be reviewed regularly.

Cross-Training or Staff Back-up

Management should provide for sufficient cross training or back-up of identified key personnel to address unavailability. Management should establish succession plans for all key functions and positions. Personnel in sensitive positions should be required to take uninterrupted holidays of sufficient length to exercise the organization's ability to cope with unavailability and to prevent and detect fraudulent activity.

Personnel Clearance Procedures

IT management should ensure that their personnel are subjected to security clearance before they are hired, transferred or promoted, depending on the sensitivity of the position. An employee, who was not subjected to such a clearance when first hired, should not be placed in a sensitive position until a security clearance has been obtained.

Job Change and Termination

Management should ensure that appropriate and timely actions are taken regarding job changes and job terminations so that internal controls and security are not impaired by such occurrences.

Security Principles and Awareness Training

All personnel must be trained and educated in system security principles, including periodic updates with special focus on security awareness and incident handling.

Management should provide an education and training program that includes: ethical conduct of the IT function, security practices to protect against harm from failures affecting availability, confidentiality, integrity, and performance of duties in a secure manner.

Personnel Health and Safety

Health and safety practices should be put in place and maintained in conformance with applicable international, national, regional, state and local laws and regulations.

HIPAA

Personnel security

All personnel who have access to any sensitive information have the required authorities as well as all appropriate clearances that includes all of the following implementation features:

Assuring supervision of maintenance personnel by an authorized, knowledgeable person.

These procedures are documented formal procedures and instructions for the oversight of maintenance personnel when the personnel are near health information pertaining to an individual.

Maintaining a record of access authorizations

Ongoing documentation and review of the levels of access granted to a user, program, or procedure accessing health information.

Assuring that operating and maintenance personnel have proper access authorization

Formal documented policies and procedures for determining the access level to be granted to individuals working on, or near, health information.

Establishing personnel clearance procedures

A protective measure applied to determine that an individual's access to sensitive unclassified automated information is admissible.

Establishing and maintaining personnel security policies and procedures

Formal, documentation of procedures to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances.

Assuring that system users, including maintenance personnel, receive security awareness training.

Security incident procedures

Formal documented instructions for reporting security breaches that include all of the following implementation features:

Report procedures

Documented formal mechanism employed to document security incidents.

Response procedures

Documented formal rules or instructions for actions to be taken as a result of the receipt of a security incident report.

Sanction policies and procedures

Statements regarding disciplinary actions that are communicated to all employees, agents, and contractors; for example, verbal warning, notice of disciplinary action placed in personnel files, removal of system privileges, termination of employment, and contract penalties). They must include employee, agent, and contractor notice of civil or criminal penalties for misuse or misappropriation of health information and must make employees, agents, and contractors aware that violations may result in notification to law enforcement officials and regulatory, accreditation, and licensure organizations.

Termination procedures

Formal documented instructions, which include appropriate security measures, for the ending of an employee's employment or an internal/external user's access that include procedures for all of the following implementation features:

Changing locks

A documented procedure for changing combinations of locking mechanisms, both on a recurring basis and when personnel knowledgeable of combinations no longer have a need to know or require access to the protected facility or system.

Removal from access lists

Physical eradication of an entity's access privileges.

Removal of user account(s)

Termination or deletion of an individual's access privileges to the information, services, and resources for which they currently have clearance, authorization, and need-to-know when such clearance, authorization and need-to-know no longer exists.

Turning in of keys, tokens, or cards that allow access

Formal, documented procedure to ensure all physical items that allow a terminated employee to access a property, building, or equipment are retrieved from that employee, preferably before termination.

Training

Education concerning the vulnerabilities of the health information in an entity's possession and ways to ensure the protection of that information that includes all of the following implementation features:

Awareness training for all personnel, including management personnel
In security awareness, including, but not limited to, password maintenance, incident reporting, and viruses and other forms of malicious software.

Periodic security reminders

Employees, agents, and contractors are made aware of security concerns on an ongoing basis.

User education concerning virus protection

Training relative to user awareness of the potential harm that can be caused by a virus, how to prevent the introduction of a virus to a computer system, and what to do if a virus is detected.

User education in importance of monitoring log-in success or failure and how to report discrepancies

Training in the user's responsibility to ensure the security of health care information.

User education in password management

Type of user training in the rules to be followed in creating and changing passwords and the need to keep them confidential.

Security awareness training

Information security awareness training programs in which all employees, agents, and contractors must participate, including, based on job responsibilities, customized education programs that focus on issues regarding use of health information and responsibilities regarding confidentiality and security.