Yukon

SAFEGUARDING INFORMATION ASSETS

Guidance on Safeguarding Information Assets

Purpose

This document is intended to assist government employees to develop processes that will ensure the security of information assets stored in information systems. This document's main intent is to develop an awareness of the fact that ensuring adequate safeguards are in place is a requirement of all privacy legislation. Generally, safeguards fall into three categories: physical, technical and administrative.

NOTE: The information below is not exhaustive and employees should consult with their information & technology branch or an information security specialist before applying specific safeguards. Safeguards need to be properly tailored to the sensitivity of the information.

Physical Safeguards

Physical safeguards involve protecting the actual computer hardware, software, data and information from physical damage or loss due to natural, human, or environmental threats. Specific issues related to physical security are: assigned security responsibility, media controls, physical access controls and workstation security.

1. **Assigned Security Responsibility**

   - Identify an employee as being responsible for security.

2. **Media Controls**

   - Develop policies and procedures that govern the receipt and removal of hardware, software, disks, tapes, etc., into and out of the organization.

3. **Physical Access Controls**

   - Limit access to information systems to individuals authorised to see the information. o Controls that can be employed are: equipment control; a facility security plan; procedures that verify user identity before allowing access to an area; a procedure for maintaining records of repairs and modifications to hardware, software, and physical facilities; antitheft devices; and a visitor sign-in procedure.

4. **Workstation Security**

- Ensure workstations that allow access to sensitive data are placed in secure or constantly monitored areas.
    - Controls that can be employed are: secure workstation policy and situate workstations so visitors cannot read screens.

Technical Safeguards

Technical safeguards secure the information system and the networks on which data and information reside. Specific issues related to technical security are: access control, entity authentication, audit trails, data encryption, firewall protection and virus checking.

1. **Access Control**

- Only individuals with a need to know should have access to data. Controls over access may involve any of the following methods: user-based access, role-based access, and context-based access.
    - User-based access: An individual has access to data based on who he or she is.
    - Role-based access: An individual has access to data based on his or her role within the organisation.
    - Context-based access: An individual has access to data based on where and when he or she is accessing the data. Context-based access also incorporates user-based and/or role-based access to authenticate the user.

2. **Entity Authentication**

- Corroboration that a person is the one claimed.
- Two-factor authentication is the recommended standard. It can include any two of the three accepted methods for authentication:
    - Something the individual knows; a password or PIN, for example.
    - Something the individual has; a swipe card or token, for example.
    - Something the individual is; a fingerprint, voice scan or retinal scan, for example.

3. Audit Trails

- A record showing who has had access to the information system and what operations were performed during a period of time.
  - Audit trails have multiple uses, including: individual accountability; reconstructing electronic events; problem monitoring; and intrusion detection.

4. Data Encryption

- Ensures that data transferred from one location on a network to another are secure against anyone eavesdropping or seeking to intercept them. Encryption is recommended for the following:
  - Back-up media that must leave the facility
  - Emails containing sensitive information
  - Laptops or mobile devices containing sensitive information
  - Internet sessions involving sensitive information
  - Any remote access sessions involving sensitive information

5. Firewall Protection

- A system or combination of systems, that supports an access control policy between two networks. Basic types of firewalls include packet filter (or network level) and proxy servers (or application level).

6. Virus Checking

- Have antivirus software installed and ensure the virus catalogue is updated frequently.

Administrative Safeguards

Administrative safeguards: cover a wide range of organisational activities and are generally intended to control human behaviour through clearly written policies and procedures. Issues that policies and procedures should cover include, but are not limited to: security management functions; assigned security responsibility; workforce security; information access management; security awareness and training; security incident reporting; contingency plan; evaluation; and third party service providers.

1. **Security Management Functions**

    - Risk assessments of the vulnerability of the information system.
    - Sanction policy for employees who do not comply with the policies and procedures.
    - Information system security review procedures to ensure records of system activity are reviewed (review of audit logs, access reports, and security incident tracking reports, for example).

2. **Assigned Security Responsibility**

    - An individual within the organisation needs to be assigned responsibility for overseeing the development of policies and procedures.

3. **Workforce Security**

    - Policies and procedures need to be in place to prevent employees from having unauthorised access to data.
        - Workforce clearance procedures and termination procedures are examples.

4. **Information Access Management**

    - Policies and procedures need to be in place to authorise employees' access to data.

5. **Security Awareness and Training**

    - Awareness training needs to be in place to inform employees of legislated and corporate requirements and expectations.

6. **Security Incident Reporting**

    - Policies and procedures need to be in place to address a security or privacy breach.

7. **Contingency Plan**

    - Policies and procedures need to encompass the following: data backup plan; disaster recovery plan; and emergency mode operation plan.

8. **Evaluation**

    - Regularly scheduled evaluation processes need to be encompassed within existing policies and procedures.

9. **Third Party Service Providers**

    - Policies and procedures need to ensure formal agreements between third party service providers and clients are in place, and that these agreements fulfill the requirements of the governing privacy legislation.

Acknowledgements

This guidance document was developed from material created by the following reference:

Wager, K. et al.. (2013). Chapter 11: Security of Health Information Systems. In Health Care Information Systems (pp. 351-392). Jossey-Bass.