Security Principles for Information Systems Development/Deployment

Information security is concerned with the confidentiality, integrity, and availability of information. From these three "pillars", the following principles must be applied when implementing and maintaining an information system:

- Accountability
- Trust
- Data Management
- Isolation
- Change
- Compliance

These security principles must be applied and managed throughout the entire systems development lifecycle.

Accountability

Regardless of who is implementing an information system for the University of Waterloo, roles must be assigned to appropriate permanent university staff. Policy 8 defines the roles of information steward (e.g. the business owner) and information custodian (e.g. the technologist), along with their respective responsibilities.

Within the information system itself, controls must be implemented to maintain the appropriate level of information security. In most cases, the system must authenticate users, and record an appropriate level of system activity for audit purposes.

Trust

It must be assumed that any information system will be under attack via a number of vectors. A variety of safeguards are required for all system components to maintain system security and the security of the information being processed and stored.

Internal threats must also be considered. For example, implementing least privilege in a business process, and through authorization mechanisms, will lower the risk of a successful exploitation of trust by a trusted system user.

Data Management

Data Classification

Information may be classified in a number of different ways, reflecting its importance to the university. Information must be classified in terms of confidentiality (see Policy 8), records management (see Policy 12), and importance to the institution for the purposes of Business Continuity Planning.

Data Minimization

The collection and use of information must be restricted to that which is required to support the business processes implemented by the information system. Data minimization reduces the exposure in the event of a breach. For example, do not collect personal information such as Social Insurance Numbers or dates of birth unless absolutely required.

Data Protection

The appropriate level of physical and logical security controls must be implemented to protect data when transmitted, processed, and stored. Some examples:

- Use Transport Layer Security (TLS) to maintain the confidentiality and integrity of information in transit on the network.
- Use encryption to protect the confidentiality and integrity of information stored on mobile devices.
- Use locked doors, surveillance cameras, and motion detectors to maintain the physical security of data centers.

Isolation

Highly sensitive information, such as information classified as Highly Restricted, should be isolated from more public systems. Isolation:

- Reduces the exposure to attack.
- Allows for greater security controls to be applied on a smaller scale, helping with the control of costs.
- Helps with managing the flow of information between independent systems.
- Can be used as an access control technique within an information system.

Change

When not managed properly, change can have a negative impact on the confidentiality, integrity, and availability of information. Untested or unplanned changes could introduce vulnerabilities that, when exploited, lead to a breach. The changes could also introduce bugs that may compromise the integrity of information. The discovery of any of these kinds of issues after-the-fact often requires unplanned outages to resolve, which has a negative impact on availability.

Compliance

The University of Waterloo is subject to an increasing number of compliance requirements. Some examples:

- The Freedom of Information and Protection of Privacy Act (FIPPA) contains disclosure requirements in the event of a breach.
- The Payment Card Industry Data Security Standard (PCI DSS) prescribes how credit card holder data is to be handled and secured.
- The Food and Drug Administration (FDA) in the USA has security requirements with respect to the handling of contact lens research data.
- The Federal Information Security Management Act (FISMA) in the USA could impact the university when it comes to working with health-related research data from that country.

Compliance requirements must be identified early in the planning stages of an information system development or deployment project.