Royal Roads University Policy

First implemented:
October 22, 2014
Amended:
October 22, 2014

Preamble

This document (the IT-Services Security Policy Framework) represents a formalised organisational structure for Information Technology policies, standards and processes. The document, also known as an Information Security Management System (ISMS), provides a risk-based architecture for consistent IT security practices that govern the entire University. The document provides a summary context, scope, components and linkages to specific enterprise IT security policies and supporting references.

This and all other related policies, standards and procedures are in support of Royal Roads University Board policy # D-1140 titled “Information Security Policy”.

Definition and Purpose

This IT Security Policy describes the approach taken by University management for administering information technology security, and reflects management’s commitment to a visible and clear set of responsibilities for ensuring IT security is coordinated across the organization.

The Policy goals include: sustaining a cost-effective secure computing environment for the protection of confidential or sensitive information; maintaining personal information privacy; and preventing disruptions that impact the use of the Royal Roads University computing facilities.

The policy specifies the over-arching model and components for providing appropriate levels of protection for the University’s information technology assets, including business applications, technology infrastructure services and information data stores.
Information Technology (IT) Security ensures that:

- Information systems are available and usable when required, and can appropriately resist attacks and recover from failures (availability)
- Information is observed by or disclosed to only those who have the right to know (confidentiality)
- Information is protected against unauthorized modification or errors so that accuracy, completeness and validity are maintained (integrity)

Ownership and Maintenance

This IT Security Policy Framework is subject to the approval of the University Executive. Responsibility for on-going maintenance, sponsorship and coordination of IT policies rests with the IT-Services Director (ITSD). This document will be periodically reviewed and supported by the University’s IT-Services Management Group (ITMG).

All institutional IT security policies, standards and guidelines will be referenced and accessible from this policy document. Drafting, revision, approval, and periodic review will be documented as an Appendix to this document.

Scope and Statement of Applicability

The scope of this IT Security Policy Framework includes the entire University enterprise, including remote offices, all administrative, academic, research and ancillary units, and the entire University networking environment (including remote and mobile users). The Policy is intended to guide cost-effective protection of all systems infrastructure, applications, services, databases and computing accounts (i.e. information assets).

The Policy references guidance of the international ‘code of practice’ for information security contained in ISO/IEC 27002:2005.

Security Policy Components

This document utilizes the organizational structure of the ISO 27002 standard, with each of the eleven categories referenced in the standard included in this document as individual components.

The eleven components introduce focus areas of security practice and control. Components include: allocation of information security responsibilities, access control, physical, network and environmental security, security incident management, and systems development and maintenance.

As new policies are developed, this document will include hyper-text links to individual policy documents (both draft and approved) mapped to the appropriate component within the Policy.

The ISO standard also includes guidance (not included in this document) on the essential first step of information security risk management, enabling a holistic approach to IT security based on management’s risk assessment, security requirements and prioritized security controls (i.e. risk mitigation).

[header = pagebreak]

Component #1: IT-Services Security Policy

This IT-Services Security Policy represents the university's over-arching IT security policy document. In accordance with recommended practice, this enterprise-level policy will be reviewed annually. Approval and revision history will be recorded in Appendix I within this document.
The IT-Services Security Policy establishes requirements to ensure that information security policies remain current as business needs evolve and technology changes. This policy must be published and communicated to employees and relevant external parties.

IT-Services Security Policy

The IT-Services Security Policy contains operational policies, standards, guidelines and metrics intended to establish minimum requirements for the secure delivery of university services. Secure service delivery requires the assurance of confidentiality, integrity, availability and privacy of university information assets through:

- Management and business processes that include and enable security processes;
- Ongoing personnel awareness of security issues;
- Physical security requirements for information systems;
- Governance processes for information technology;
- Reporting information security events and weaknesses;
- Creating and maintaining business continuity plans; and,
- Monitoring for compliance.

The IT-Services Department recognizes that information security is a process, which to be effective, requires management commitment, the active participation of all personnel and ongoing awareness programs.

IT-Services Security Policy review

The IT-Services Director (ITSD) is responsible for reviewing information security policies, standards and guidelines on an annual basis.

[header = pagebreak]

Component #2: Organization of Information Security

Coordination of information security and allocation of information security responsibilities are specified in the following policy statement:

Roles and Responsibilities for Information Technology Security

Policy Statement

The IT-Services Director (ITSD) is responsible for sponsoring, developing, and implementing a comprehensive information technology security strategy and policy framework which reflects the asset value of information and includes the entire technology infrastructure of the University. This Policy specifies the groups and individuals responsible and accountable for various elements of IT Security practice.

Vice President Academic and Provost

The Vice President has overall responsibility for approving the University's strategy and administrative structure for managing information technology assets and infrastructure. The Vice President approves the information technology security policy framework and delegates responsibility for administration and compliance to the University's IT-Services Director.

IT-Services Director

The IT-Services Director (ITSD) is responsible for overall strategy, policy administration, risk management, and compliance of the University's information technology, information services and information resources. Reporting to the Provost and Vice President (Academic), the ITSD will:

- Be accountable for the development and use of information systems (IS) and information technology (IT) to further the academic mission and to support the administrative requirements of the University.
- Establish standards for use of information and technology on campus.
- Escalate security incidents to the appropriate executive level.
- Coordinate IT disaster recovery and emergency response planning.
- Monitor IT compliance to meet legislative requirements.
- Analyze and manage institutional information technology risks.
- Investigate IT security incidents and coordinate their resolution as defined in the Royal Roads University Acceptable Use Policy.
- Develop and implement an enterprise information security awareness program.
- Liaise with other University agencies on information security issues and initiatives.
- Collaborate with law enforcement agencies, physical resources, external agencies, audit services, and University administration on IT security issues.
- Coordinate investigation and responses to external and internal IT security threats or compromises.

Individual Responsibilities

Every member of the university community is responsible for protecting the security of university information and IT systems by adhering to the objectives and requirements stated within published university-level information technology and IT security policies. In addition, individuals are required to comply with the additional security policies, procedures, and practices established by their respective schools, departments or other units.
Specific responsibilities for all individuals employed at the University include the following:

- Maintain awareness of and abide by the conditions set out in the University's Acceptable Use Policy (AUP) and any other existing IT-Services policy set out by the University as applicable.
- Maintain computing accounts, application access and individual computing devices in a secure manner.
- Report any security incidents or privacy breaches to the appropriate area.

Exceptions

Any exceptions to this policy should be submitted to the ITSD for review and possible approval.

[header = pagebreak]

Component #3: Asset Management

Information and information systems services constitute valuable university resources. The asset management chapter establishes the blueprint to identify the rules of acceptable use and the rules for protection: what assets to protect, who protects them and how much protection is adequate.

Asset Management – Responsibility for assets

Documenting and maintaining asset inventories

Information Owners and Information Custodians must maintain an inventory of assets under their control. This inventory should record sufficient information to facilitate system planning, asset lease management and asset recovery in the event of loss or destruction.

Loss, theft or misappropriation of assets

The loss, theft or misappropriation of assets must be reported immediately. Where the loss, theft or misappropriation involves information the Security Incident Response Program must be followed.

Acceptable use of university IT resources

All users of the university's information systems must take responsibility for, and accept the duty to actively protect the university's information and technology assets.

The Royal Roads IT-Services Acceptable Use Policy document defines acceptable uses and breaches of acceptable use of Information Technology Resources at Royal Roads University.

[header = pagebreak]

Component #4: Human Resources Security

This chapter identifies the information security requirements for personnel that have an employment relationship with Royal Roads University. To reduce information security risks, the terms and conditions of employment must establish expectations for the protection of university assets, information and services.

Management and personnel have different security responsibilities and liabilities that apply prior, during, and at the time of termination of employment. Prior to employment, emphasis is on the awareness of the expected roles and responsibilities, the screening of prospects and the existence of agreements. During employment, policies establish management responsibilities, education, training and formal processes to handle problematic security situations. This chapter also establishes rules to ensure a secure transition when employment is ended or changed.

Human Resources Security – Prior to employment

To ensure personnel are informed of their information security roles and responsibilities, security roles and responsibilities for personnel must be documented.

Security roles and responsibilities

Information Owners and Information Custodians must:

- Document information security roles and responsibilities for personnel in job descriptions, standing offers, contracts, and information use agreements; and,
- Review and update information security roles and responsibilities when conducting staffing or contracting activities.

Terms of Employment

The terms and conditions of employment must document the responsibility of personnel for information and information systems security. Managers must ensure terms and conditions of employment are agreed to by personnel prior to employment or provision of services.

Human Resources Security – During Employment

Management Responsibilities

Managers must support the implementation of information security policies and practices by:

- Ensuring personnel are informed of information security roles and responsibilities prior to being granted access to information or information systems;
- Supporting and encouraging personnel to adhere to information security policies; and,
- Requiring that personnel conform to the terms and conditions of employment, including information security policies.

Orientation for New Personnel

Managers must include an information security awareness component in orientation processes that personnel must complete prior to accessing information or information systems.

Ongoing Information Security Awareness Training

Managers must provide ongoing information security awareness, education and training, addressing topics including:

- Protection of information;
- Legal responsibilities;
- Information security policies and directives;
- Procedures for reporting information security events to the ITSD;
- Appropriate use of University resources;

Reviewing Security Breaches and Policy Violations

Upon receipt of information identifying personnel responsible for a security breach or policy violation, managers are responsible for:

- Ensuring the IT–Services Director has been informed of the potential security breach or policy violation;
- Assisting in an investigation and verifying the details of the security breach or policy violation;
- Determining if disciplinary action is warranted for employees;
- Determining if disciplinary action is warranted for non-employees; and,
- Arranging for permanent or temporary removal of access privileges when appropriate.

Human Resources Security – Termination or Change of Employment

Return of assets

Managers must document the return of university assets in the possession of personnel upon termination of their employment using standard processes.

Change of employment status

To ensure physical and logical access rights to information systems and information processing facilities are managed in relation to the security responsibilities of the job requirements, the access rights of personnel to information systems must be removed upon termination of employment and reviewed upon change of employment.

Managers must review access to information systems and information processing facilities when personnel change employment.

Action upon termination or change of employment

Managers must ensure access to information systems and information processing facilities is removed upon termination of employment or reviewed upon change of employment.

Reduction of access rights

Managers must ensure access to information systems and information processing facilities is reduced or removed before the employment terminates or changes.

IT Security Awareness

Raising the level of awareness of security issues in the community is an important component of IT security management. It is also important that the community is aware of Security Policies and their responsibilities. The IT-Services Director is responsible for communicating IT security issues to the community, and developing IT security education and training.

This Security Program will also be published through a web page accessible from the Computer Services web-site, and kept current.

http://computerservices.royalroads.ca/knowledge-base-section/security [1]

Computer Services provides regular communication via a security web page, periodic articles in the campus newspapers, meetings and targeted emails.

[header = pagebreak]

Component #5: Physical and Environment Security

This chapter identifies requirements for the protection from environmental and man-made threats to personnel and property in information processing facilities. Safety measures for equipment installations are also described.

Requirements for the installation, operation, protection and maintenance of computer equipment are identified to preserve the confidentiality, integrity and availability of University information and information systems.

Equipment must be protected when off-site

Equipment Security controls

Information Owners and Information Custodians must ensure that university equipment being used off-site is protected commensurate with the sensitivity of the information it contains and the value of the equipment.

Information Custodians must ensure that:

- Sensitive data is encrypted;
- Equipment is protected from unauthorized access by the use of a logical or physical access control mechanism (e.g., password, USB key or smart card);
- Equipment is protected from loss with a physical locking, restraint or security mechanism when appropriate; and,
- Personnel are familiar with operation of the protection technologies in use.

To provide further protection personnel must:

- Not leave university equipment unattended in a public place;
- Ensure that equipment is under their direct control at all times when travelling;
- Use the physical locking, restraint or security mechanisms provided whenever possible;
- Take measures to prevent viewing of sensitive information other than by authorized persons;
- Not permit other persons to use the equipment; and,
- Report loss of equipment immediately to Campus Security.

Reassignment of hardware and media

Information, records and software must be protected against unauthorized disclosure when hardware and media are reassigned or destroyed. Information Owners must consider the value and sensitivity of the information stored on hardware or media when determining whether it will be reassigned or destroyed.
Prior to reassignment of hardware or media within the university Information Owners and Information Custodians must ensure:

- That the integrity of university records is maintained by adhering to Records Management policies;
- Information and software is erased using methods and standards approved by IT-Services;

Where information is erased by third parties there must be contractual and audit procedures to ensure complete destruction of the information. Third parties must certify that destruction has occurred.

[header = pagebreak]

Component #6: Communications and Operations

This chapter establishes a framework to support the integration of information security in the services provided by Royal Roads University information processing facilities.
Planning and management of the day-to-day activities is required to ensure the availability and capacity of the resources that provide services. Services can be delivered by external parties and by computer networks and by all services that exchange information. This framework identifies requirements to control and monitor operations for service delivery and to manage changes as the operations evolve.
Controls for operations include documented processes, staff duties and formal methods to implement changes to facilities. This includes: methods to protect information, create copies for back-up and to manage the media where those copies are stored. Network protection requirements from threats such as viruses or unauthorized disclosure are also described.

Operational procedures and responsibilities

Documented operating procedures

To ensure correct operations of information systems and information processing facilities, operating procedures and responsibilities for information systems and information processing facilities must be authorized, documented, and maintained.
Information Custodians must ensure that approved operating procedures and standards are:

- Documented;
- Consistent with university policies;
- Reviewed and updated annually

Operations documentation could contain instructions regarding:

- Information processing and handling;
- System re-start and recovery;
- Back-up and recovery, including on-site and off-site storage;
- Exceptions handling, including a log of exceptions;
- Output and media handling, including secure disposal or destruction;
- Audit and system log management;
- Change management including scheduled maintenance and interdependencies;
- Computer room management and safety;
- Information Incident Management Process;
- Disaster recovery;
- Business continuity; and,
- Operations, technical, emergency and business contacts.

Change management

To ensure changes to information systems and facilities are applied correctly and do not compromise the security of information and information systems changes to information systems and information processing facilities must be controlled.

Change management process

Information Owners and Information Custodians must document and implement a change management process to control changes by:

- Identifying and recording significant changes;
- Assessing the potential impact, including the security impact, of the change;
- Obtaining approval of changes from the manager(s) responsible for the information system;
- Planning and testing changes including documenting fallback procedures;
- Communicating change details to relevant personnel; and,
- Evaluating that planned changes were performed as intended.

System planning and acceptance

Capacity management

The risk of system failures and unacceptable performance levels can be reduced by monitoring and optimizing resources to meet current and future information system capacity requirements. To achieve this, the use of information system resources must be monitored, optimized and projections made of future capacity requirements.

Resource capacity management

Information Custodians are responsible for implementing capacity management processes by:

- Including capacity requirements in service agreements;
- Monitoring and optimizing information systems to detect impending capacity limits; and,
- Projecting future capacity requirements based on:
  - New business and information systems requirements,
  - Statistical or historical capacity requirement information, and,
  - Current and expected trends in information processing capabilities (e.g., introduction of more efficient hardware or software).

System acceptance

Security certification

The Information Owners and Information Custodians should receive assurance that a new or updated information system meets minimum security acceptance criteria.

Protection against malicious code

To protect the integrity of information systems and software, security awareness, prevention and detection controls must be utilized.

Prevention and detection controls

Information Custodians must protect university information systems from malicious code (e.g., viruses, worms) by undertaking such activities as:

- Installing, updating and consistently using software (e.g., anti-virus or anti-spyware software) designed to scan for, detect and provide protection from malicious code;
- Checking files, including electronic mail attachments and file downloads for malicious code before use; and,
- Maintaining business continuity plans to recover from malicious code incidents.

User awareness

The IT-Services Director is responsible for developing user awareness programs for malicious code countermeasures.

Back-up

To enable the timely recovery of information and information systems, information and information systems must be backed up and the recovery process tested regularly.

Defining requirements

Information Owners and Information Custodians must define and document backup and recovery processes that reflect the security classification and availability requirements of information and information systems including:

- Confirming that the backup and recovery strategy complies with:
    - Business continuity plans,
    - Policy, legislative, regulatory and other legal obligations, and,
    - Records management requirements and,
- Documenting the backup and recovery processes including:
    - Types of information to be backed up,
    - Schedules for the backup of information and information systems,
    - Backup media management (e.g., retention period, pattern of backup cycles),
    - Methods for performing, validating and labelling backups, and,
    - Methods for validating recovery of the information and information system.

Safeguarding backup facilities and media

Information Custodians must identify safeguards for backup facilities and media that are commensurate with the value and sensitivity of the information and information systems.

Safeguards can include:

- Using encryption to protect the backed up information;
- Physical and environmental security;
- Access controls;
- Methods of transit to and from offsite locations (e.g., by authorized couriers, by encrypted electronic transfer);
- Storage of media adhering to manufacturer recommendations for storage conditions and maximum shelf-life; and,
- Remote storage of backup media at a sufficient distance to escape any damage from a disaster at the main site.

Information Custodians must regularly test backup and recovery processes.

Network Security Management

Network security controls and network security management practices are implemented and documented to protect the network infrastructure, information traversing the network, and network-attached information systems.

Network controls

Information Custodians must implement network infrastructure security controls and security management systems for networks to ensure the protection of information and attached information systems.

Configuration control

To maintain the integrity of networks, Information Custodians must manage and control changes to network device configuration information such as configuration data, access control definitions, routing information and passwords.
Network device configuration data must be protected from unauthorized access, modification, misuse or loss by the use of controls such as:

- Encryption;
- Access controls and multi-factor authentication;
- Monitoring of access;
- Configuration change logs;
- Configuration baselines protected by cryptographic checksums; and,
- Regular backups.

Where required by information classification, legislation or industry standards / best practices, information must only be transmitted using a secured path.

Logging, monitoring and detection

To facilitate monitoring, response and investigation, logging to a centralized log management service should be enabled.
Logs must be continuously monitored to enable detection and response to security events and intrusions (e.g., automation of log monitoring and event alerting).
Sensors enabling on-demand capture of network traffic must be implemented at network security boundaries and within networks housing sensitive information or information.

Media Handling

All removable computer media must be managed with controls appropriate for the sensitivity of the data contained on the media, to ensure that the risks to information introduced by portable storage devices are sufficiently managed.

Use of portable storage devices

The use of portable storage devices to store or transport information increases the risk of information compromise. Portable storage devices are typically small, portable and are easily lost, stolen or damaged, particularly when transported in public environments.
Information Owners, Information Custodians and Managers must:

- Ensure that use of portable storage devices is managed and controlled to mitigate risks;
- Ensure personnel using portable storage devices protect information and information technology assets in their custody or control.

Human factors

Information Owners, Information Custodians and Managers must ensure personnel using portable storage devices are:

- Aware of the additional risks and responsibilities inherent with portable storage devices;
- Familiar with operation of the required protection technologies and when they must be used; and,
- Familiar with security event and loss reporting procedures.

Mandatory controls

Minimum information protection safeguards for the use of portable storage devices include:

- Not storing the only version of a document on portable storage devices;
- Encryption of stored data;

- Contractual requirements for external parties that transport, handle or store portable storage devices;
- Adherence to manufacturer specifications for media storage environment;

Electronic Messaging

To enable secure and trustworthy electronic messaging Information transmitted by electronic messaging must be appropriately protected.

General requirements

Electronic messaging services must be managed to protect the integrity of university messages by:

- Protecting messages from unauthorized access, modification or denial of service;
- Ensuring correct addressing and transportation of messages;
- Providing reliable and available messaging infrastructure; and,
- Conforming to university, regulatory and policy requirements.

The IT-Services Director must approve implementation of, and significant modification to, electronic messaging systems.

Custody of electronic messages

Electronic messages created, compiled on, sent or received on university information systems are records of the university. These records:

- Are the property of Royal Roads University; and,
- Are subject to the access and the protection of privacy provisions of the Freedom of Information and Protection of Privacy Act.

Electronic commerce services

To enable secure electronic commerce for the delivery of university services, information in electronic commerce information systems must be protected from fraudulent activity, contract dispute, unauthorized disclosure and modification.

Electronic commerce

Prior to initiating or implementing electronic commerce information systems Information Owners and Information Custodians must:

- Ensure that a PCI-DSS Assessment is conducted and addresses threats and risks related

to electronic commerce;
- Confirm that a Privacy Impact Assessment has been conducted and approved;
- Ensure that the user notification and acceptance of terms and conditions of use complies with university policies and standards;
- Ensure multi factor authentication is used commensurate with the sensitivity and value of the information;

On-line transaction security

Information Owners and Information Custodians are responsible for ensuring information systems containing on-line transactions implement security controls commensurate with the value and sensitivity of the information.
Security controls must be implemented to prevent incomplete transmission, misrouting, repudiation of transaction, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication and replay. Security controls include:

- Validating and verifying user credentials;
- Using cryptography to protect data and information;
- Establishing secure communications protocols; and,
- Storing on-line transaction details on servers within the appropriate network security zone.

Information Owners and Information Custodians are responsible for ensuring that information systems used for processing payment card transactions or connected to payment card transaction processing systems comply with the Payment Card Industry Data Security Standard.

Monitoring

Audit logs recording user activities, exceptions and information security events must be produced and kept to assist in access control monitoring and future investigations.

Audit logging

Information Owners and Information Custodians must ensure that audit logs are used to record user and system activities, exceptions and information security and operational events including information about activity on networks, applications and systems. Information Owners and Information Custodians will determine the degree of detail to be logged based on the value and sensitivity of information assets, the criticality of the system and the resources required to review and analyze the audit logs.

Audit logs may contain confidential data and access must be restricted to personnel with ‘need-to-know’ privileged access and be protected accordingly.

[header = pagebreak]

Component #7: Accounts and Access Controls

This chapter identifies the mechanisms that restrict access to university information and information assets. Access restrictions protect organizations from security threats such as internal and external intrusions. The restrictions are guided by legislation that protects particular types of information and by business requirements.

Access management procedures provide the blueprint for the management of user access, authorizations and control mechanisms for computer networks, operating systems, applications and information. This chapter identifies security best practices and responsibilities for administrators and personnel.

Business requirement for access control

Access management procedures

Access to information systems and services must be consistent with business needs and be based on security requirements, to ensure that information and information systems are available for authorized use and protected from unauthorized use.

Access management procedures must:

- Consider both physical and logical access to assets;
- Apply the “need to know” and “least privilege” principles;
- Require access by unique user identifiers or system process identifiers to ensure that all access actions are auditable;

The access management procedure must be communicated to personnel as part of awareness training.

User access management

To ensure that all access actions are traceable to an identifiable individual or process, there must be a formal user registration and de-registration process for granting access to all information systems. User access will be configured in accordance with university user access management procedures which will, at a minimum, provide for:

- User registration processes
- Privilege management
- User password management
- Review of user access rights

User responsibilities

To maintain the integrity of the unique identifier (user id) users must follow good security practices in the selection and use of passwords. The RRU IT-Services Electronic Credential & Authentication Standard provides guidance on password / pass phrase creation and usage.

[header = pagebreak]

Component #8: Systems Acquisition and Development

This chapter establishes requirements for incorporating security measures into the life cycle of an information system. Security controls must be identified as part of the business requirements for new information systems or enhancements to existing information systems.

Information security is integrated into the creation, modification, implementation and expansion by ongoing security practices such as the management of vulnerable points and securing system files. For applications, information security can be applied to the validation of data input and output and by encoding information using electronic keys.

Security requirements for information systems

Identifying Security Controls

IT-Services must conduct a Security Threat and Risk Assessment during the requirements phase when developing, implementing major changes to, or acquiring an information system, to:

- Identify the security requirements necessary to protect the information system; and,
- Assign a security classification to the information and information system.

IT-Services must ensure that information system development or acquisition activities are done in accordance with documented requirements, standards and procedures which include:

- Testing the information system to verify that it functions as intended;
- All default accounts being disabled or removed prior to deployment on the network;
- Enforcing change control processes to identify and document modifications or changes which may compromise security controls or introduce security weaknesses; and,
- Using common university processes and services (e.g., authentication, access control, financial management).

Cryptographic Controls

To manage the use of cryptography for protecting the confidentiality and integrity of electronic information the use of cryptographic controls must be based on the risk of unauthorized access and the classification of the information or information system that is to be protected.

Acceptable use of cryptography

The type and quality of cryptographic controls used in information systems should include consideration of:

- Confidentiality requirements, in accordance with information classification, labelling and handling requirements;
- Integrity requirements (e.g., for financial payment instructions in excess of a specified dollar amount);
- Non-repudiation requirements (e.g., for proof of the occurrence or non-occurrence of an event);
- Authentication requirements (e.g., proof of identity);
- Other security measures (e.g., for proof of origin, receipt, or ownership);
- Legislation, regulations or policies requiring the use of cryptography;
- Restrictions on the export or use of cryptographic products; and,
- Risks relating to the long-term storage of electronic information (e.g., recovery of encrypted data, long-term key maintenance).

Vulnerability management

In order to mitigate damage to university operations resulting from exploitation of published vulnerabilities, systems and software must be patched regularly and kept up to date with current releases.

Vulnerability response processes

Vulnerabilities which impact university information systems must be addressed in a timely manner to mitigate or minimize the impact on university operations. Information Custodians must establish processes to identify assess and respond to vulnerabilities that may impact information systems by:

- Monitoring external sources of information on published vulnerabilities;
- Testing and evaluating options to mitigate or minimize the impact of vulnerabilities;
- Applying corrective measures to address the vulnerabilities.

[header = pagebreak]

Component #9: Security Incident Handling

The purpose of information security incident response is to:

- mitigate the effects caused by such an incident,
- protect the information resources of the University from future unauthorized access, use or

damage, and
- ensure that Royal Roads University fulfills all of its obligations under University policy, federal and provincial laws and regulations with respect to such incident.

Royal Roads University recognizes the need to follow established procedures to address situations that could indicate the security of the University's information assets may have been compromised. Such procedures include ensuring the appropriate level of University management becomes involved in the determination of actions implemented in response to an information technology security incident.

A standard University-wide approach to information security is important in order to protect the security of Royal Roads University's intellectual capital and to ensure that Information Security Incidents are handled properly, effectively and in a manner that minimizes the adverse impact to the University. Every user of any of Royal Roads University's information resources has responsibility toward the protection of the University's information assets; certain offices and individuals have very specific responsibilities.

Definitions

Security Incident - For the purposes of this document, a security incident is an incident involving one or more of the following:

- An *information security breach*, as defined below, involving electronic information.
- Activity originating from a university computer system or network that violates Canadian anti-spam legislation. Such activity includes, but is not limited to:
    - Spam
    - Malware (includes any "attack" designed to exploit a software vulnerability)
    - Botnet traffic
- Any other activity on a university computer system or network considered malicious, including a Denial of Service attack.

Security Event - For the purposes of this document, a security event is defined as one of the following:

- A notification from an IT Services Manager advising of a security-related issue.
- A report to Royal Roads University Computer Help Desk containing evidence of a security incident.
- Observed user, system or network behaviour that is suggestive of a security incident.

Responder - A responder is a technical staff member, designated by an IT-Services Manager or the Director, responsible for investigating a security event and security incidents involving a particular network, system, and/or service. Ideally, several technical staff, with complementary skills spanning the relevant technology stack, would be involved in a response to a security event or incident. A responder is an information custodian for electronic information.

Use of information - means any access to, collection, storage, transmission, processing, or destruction of information.

Custody of information - means the keeping, care, watch, preservation, or security of information for a legitimate business purpose.

Control of information - means the power or authority to make a decision about the use or disclosure of information in university records.

Information Security Breach - involves one or more of: a circumvention of information security controls; the unauthorized use of information; the unintended exposure of information.

Response to Security Events

A member of the University Community who becomes aware of an Information Security Incident should immediately:

- Disconnect the compromised system and equipment from RRU's network.
- Avoid making any updates or other modifications to software, data, or equipment involved or suspected of involvement with an Information Security Incident until after IT-Services has completed its investigation and authorizes such activity.
- Contact the University's Computer Help Desk by calling (250) 391-2659.

Investigation

When an Information Security Incident is reported, the University’s IT-Services Director (ITSD) or designate, will do the following:

- The ITSD, or designate, will investigate the Information Security Incident in accordance with the procedures detailed in the University’s Information Security Incident Response Program. In order to minimize the impact of the Information Security Incident on the University and in order to complete a proper investigation, the ITSD has the authority to restrict information system access or operations to protect against unauthorized information disclosures. In order to complete the investigation, the ITSD may convene a preliminary fact-finding working group comprised of relevant business and technical personnel.
- If the ITSD concludes that applicable federal or provincial laws or regulations may have been violated, the ITSD will notify a member of the university executive, which will, in turn, notify law enforcement agencies if appropriate.

[header = pagebreak]

Component #10: Business Continuity Management

This chapter provides direction from a security focus for planning the resumption of business or services where a man-made or natural disaster has occurred. Royal Roads University is required to be prepared and to re-establish business or services as swiftly and smoothly as possible.

The Royal Roads University disaster recovery plan is located in a document titled "Royal Roads University Disaster Recovery Plan", located on the main file server.

Component #11: Compliance

The chapter describes requirements for verifying that information systems comply with relevant statutory, regulatory, and information security contractual clauses. Compliance policies identify what to do to ensure that the University is in compliance with applicable laws and policies. Processes to monitor the extent in which information systems follow policies include conducting security reviews, assessments and the systematic analysis of logged information.

Relevant Legislation, Regulations, Standards and Policies

- Freedom of Information and Protection of Privacy Act
- Canadian Anti-Spam Legislation
- Payment Card Industry Data Security Standards
- Royal Roads Privacy Policy [2]

Compliance with Legal Requirements

Intellectual property

Information Owners and Information Custodians must protect intellectual property by:

- Ensuring that information and software is only acquired from reputable vendors;
- Maintaining proof or evidence of ownership or right to use;
- Adhering to the terms and conditions of use associated with intellectual property;
- Ensuring the maximum number of users permitted is not exceeded;
- Requiring the removal of unlicensed information and software from university information systems;
- Informing personnel of university policies including those pertaining to appropriate use of university resources;
- Ensuring licensed intellectual property is securely removed from electronic media prior to media disposition; and,
- Complying with terms and conditions for information and software obtained from public networks (e.g., "free for personal use only", open source).

Data and personal information protection

Security controls must be applied to protect data and personal information in accordance with relevant legislation.

The Freedom of Information and Protection of Privacy Act requires personal information to be protected using ‘reasonable security measures’.

Policy requirements for protecting data and personal information are found in the Freedom of Information and Protection of Privacy Act Policy and Procedures Manual. [3]

Deter misuse of information systems

Controls and safeguards must be in place to ensure personnel do not create security exposures through unauthorized or inappropriate use of information systems.

Information Owners and Information Custodians must monitor information system usage to prevent, detect and respond to unauthorized or inappropriate use by:

- Ensuring audit logs contain sufficient detail to detect and trace inappropriate usage;
- Ensuring that security incidents are investigated in accordance with policy; and,
- Determining if disciplinary action, including dismissal, cancellation of contract and/or other legal remedies are warranted for personnel who have made unauthorized or inappropriate use of information system resources.

Prior to implementing information system monitoring processes Information Owners and Information Custodians must ensure:

- Monitoring activities will be compliant with legal, policy and contractual requirements and obligations;
- Personnel are informed that specific activities may be monitored; and,
- Access to data gathered through monitoring processes is restricted on a ‘need to know’ and ‘least privilege’ basis to the fewest possible number of users.

Compliance with security policies and standards

Technical compliance checking

Information Custodians must regularly test information system technical control compliance by using automated tools to:

- Conduct penetration testing;
- Determine if information system patches have been applied;

- Confirm that system technical controls have been implemented and are functioning as designed.

[header = pagebreak]

Glossary

This section provides brief descriptions of the various items and terms used to describe risk, security, networking and technology issues.

Control

A safeguard, response or countermeasure to manage (i.e. mitigate or reduce) risk, including policies, guidelines, standards, practices or organizational structures.

ISO/IEC

The International Organization for Standardization/International Electro-technical Commission.

ISO/IEC 27002

Part of the ISO 27000 series on information security. Prepared by the Joint Technical Committee ISO/IEC Information Technology Subcommittee. The current version of the standard was published June 15, 2005 and replaced the previous version ISO 17799:2000.

ISMS

Information Security Management System. The over-arching policy framework and administrative program for guiding IT security within an organization.

Risk

The combination of the probability of a threat materializing (i.e. event) and its consequence or impact. Risk management reflects coordinated activities to direct and control risk, and typically includes risk assessment, risk treatment or mitigation, risk acceptance, and risk communication.

Risk Assessment

The systematic and methodical consideration of: 1) the harm likely to result from a range of business process failures; and 2) the realistic likelihood of such failures occurring.

The risk assessment and risk management process includes estimating the magnitude of risks, comparing risk estimates against risk criteria (i.e. risk evaluation), and determining the appropriate controls for reducing risk to an acceptable level.

Threat

A potential cause of an unwanted incident, which may result in harm (i.e. impact) to a system or organization.

Vulnerability

A weakness of an asset or group of assets that can be exploited by one or more threats.

Appendix I: Version, Change and Approval History

Draft approved by ITSD, Oct 22/2014

Source URL (modified on 2016-01-25 10:09): https://policies.royalroads.ca/policies/it-services-information-security-policy

Links
[1] http://computerservices.royalroads.ca/knowledge-base-section/security
[2] http://www.royalroads.ca/about/privacy-policy
[3] http://www.cio.gov.bc.ca/cio/priv_leg/manual/index.page