Policy

Title	**Information Technology System Security**		
Classification	Administrative	**Oversight Responsibility**	Office of the Vice-President, Finance and Operations
Category	Information Management and Technology	**Responsible Office**	IT Services
Approval	Executive	**Effective Date**	2024-May-30
		Document No.	1098

This policy is applied in a manner consistent with applicable statutory and legal obligations, including university collective agreements and terms of employment.

The most up-to-date versions of the University's policies are posted on the policy and procedure website. If you have printed this policy, please check the website to ensure you have the current version.

The first appearance of terms in **Bold** in this document (except titles) are defined terms – refer to the Definitions section.

1.0 POLICY STATEMENT

The development and implementation of robust organisational, people, physical, and technological controls to safeguard Royal Roads University's (University) information technology (IT) system is of paramount importance to ensure the confidentiality and integrity of personal and business **information** and **data** in the care or control of the University.

2.0 SCOPE AND COMPLIANCE

This policy provides the direction and support for IT system security controls in accordance with government and industry legislation, regulations, and standards, and the University's information and information technology policies and extends to **members of the University Community**.

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment, contract, or other relationship with the University. Allegations of a breach and any disciplinary action are managed according to the University's established policies and procedures, applicable laws, legislation, collective agreement, or contract.

This policy and related policies, standards, and procedures (see Related Documents) form the foundation for the University's information, data, and IT security in support of the Governance policy, *Information and Data Management and Security,* and applicable statutory and regulatory obligations.

3.0 POLICY TERMS

3.1 **Asset Management**

The University maintains and monitors a valid, current inventory of known IT assets that connect to the network physically, virtually, remotely, and/or within the cloud environment in order to protect the IT system and its resources and to support the identification and remediation of unauthorized or unmanaged assets. The inventory is reviewed bi-annually.

3.2 **IT System Access**

a. The University utilizes a role-based access model to grant **users** access to the IT systems, resources, and **devices.** This model enables users to access information, data, software,

hardware, and systems only as required for their role at the University, and only at the level required to perform their role.

b. Only devices owned and managed by the University, and which conform to IT standards, are permitted to connect to the secured network. In rare and extenuating circumstances, personally owned devices may be granted permission to connect to the network in accordance with established processes. Non-conforming devices may be subject to removal by IT Services.

3.3 **External Suppliers**

IT Services is responsible for ensuring the appropriate security of external IT system suppliers and cloud services on behalf of the University. Agreements are required to set out security controls, service definitions and delivery levels to ensure maximum security for the University's IT systems, information, and data. Any electronic messaging services and information transfers between the University and external parties are protected in accordance with level of sensitivity and in compliance with applicable legislation and regulatory requirements. IT Services responsibility does not absolve external suppliers of their responsibility and accountability.

3.4 **Network Security**

Network **security** technical controls and processes are required to protect and maintain the integrity of the network infrastructure, information, data, and the overall IT system. This includes, but is not limited to:

- encryption;
- multi-factor authentication;
- credentials (e.g., passphrase, PINs);
- configuration;
- segregation of services and information systems (e.g., firewalls);
- system logs;
- backup and recovery processes developed, maintained, and reviewed regularly; and
- controls to protect log files/systems from unauthorized access, modification, and/or disposal.

3.5 **Software and Hardware**

a. Only software and hardware authorized by IT Services are permitted to operate on the University's IT system. IT Services is permitted to remove from use any unauthorized software and hardware, or to grant an exception as long as such exception is for the purposes of the University's business. Any exception is documented and reviewed on a regular basis.

b. An inventory of software and hardware installed on the IT system and throughout the life cycle is maintained, reviewed at least bi-annually, and updated as necessary.

3.6 **IT Incident Response and Adverse Event Management**

IT incident response and adverse event management plans must be in place and are required to:

- monitor, assess, track, and act on vulnerabilities;
- conduct periodic audits of the IT system;
- ensure business continuity and recovery;
- advise the Executive and the Board of Governors of adverse events and response;
- be communicated throughout the University;
- comply with applicable legislation, regulations, and University policies, standards, and procedures; and
- be reviewed, at least annually, and updated as necessary.

3.7 **IT Security Program**

The University is required to establish, maintain, and communicate an effective IT security program that promotes awareness of IT security measures through education, training, and processes.

4.0 AUTHORITIES, ROLES AND RESPONSIBILITIES

4.1 **Vice President, Finance and Operations (VPFO)**

The VPFO:

a. ensures relevant policies, standards, procedures and other documents are in place to protect IT system security;
b. receives and responds to reports regarding the current and future state of IT system security; and
c. informs Executive of any significant issue or matter that affects, or may affect, IT system security.

4.2 **Chief Information Officer (CIO)**

The CIO:

a. oversees the management and security of University IT systems to protect the integrity, confidentiality and reliable availability of all information and data that utilize IT resources, programs, and assets used for academic and administrative purposes;
b. reports to the Vice President, Finance and Operations regarding issues and trends related to IT security systems that have or may enhance or compromise the University's information and/or data; and
c. ensures appropriate practices are in place in compliance with mandated and standardized IT security directions and guidance.

4.3 **Supervisors**

Supervisors provide training and information to their staff to support compliance with the IT system security requirements.

4.4 **Users**

Users are responsible for adhering to the information and data management and security requirements and practices that safeguard the University's IT systems and its assets and to report non-compliance as set out in applicable University policies.

5.0 DEFINITIONS

For the purposes of this policy**:**

Data means raw facts and statistics that, on their own, do not have any specific meaning, but may be collected and organized to provide information that has a logical meaning.

Devices means University-issued end-user equipment such as laptops, smartphones, tablets, desktops, and workstations, and network equipment including servers, and non-computing devices programmed for applications and can transmit data over the internet or other networks, in virtual, remote, cloud-based, and/or physical environments.

Information means:

a. **Business information** – information, including confidential information, that is generated or collected for the operations of the University including, but not limited to: financial information, human resource information, technical plans, forecasts, reports, legal opinions, and budgets;

b. **Personal information** - information, including an identifying number or symbol assigned to an individual, collected and/or recorded in any format about an identifiable individual, other than contact information (e.g., name, title, business phone/email), that is within the control or custody of the University, and includes all information that the University collects and uses about identifiable members of its employees, students, and other individuals

Members of the University Community means members of the Board of Governors, employees, students, contractors, volunteers, guests, visitors and others who access and/or participate in University academic, administrative, and research activities and operations undertaken on behalf of the University on or off-campus.

Security means guarding the safety of information and data against misuse, theft, inadvertent release, or other threats and protecting confidentiality and privacy while maintaining the integrity of that information and data.

Users means members of the University community who access and/or use the University's IT resources and/or systems.

6.0 INTERPRETATION

Questions of interpretation or application of this policy or its procedures will be referred to the Vice-President, Finance and Operations for resolution.

7.0 RELATED DOCUMENTS

Royal Roads University Documents and Information

- Appendix A – Information and Data Management Security Document Suite
- IT Resources' Access and Acceptable Use (policy #1063)
- Information and Data Management and Security (policy #1097)
- Network Access (standard #1098-S))
- Privacy and Protection of Personal Information (policy #1090)
- Records Management (policy #1029)

Legislation and Other Information

- Canada's Anti-Spam Legislation (CASL), SC2010, c.23
- Center for Internet Security Controls (2023), v.8
- *Freedom of Information and Protection of Privacy Act*, RSBC 1966, c. 165 and applicable Regulations
- ISO 27001:2022 – Security Control Framework and Annex A

Review, Revision and Approval History

Date	Activity
2024-May-30	Approved by Executive; first implementation and effective date
2024-May-30	Next Review (one year post-implementation)

APPENDIX A

Information and Data Management and Security

Document Suite – Stage One

The following diagram sets out the first stage for the information and data management and security document suite (policies, standards, guidelines) for Royal Roads University. Additional documents will be added, and this diagram updated, as required. The document suite for the first stage:

- reflects the Center for Internet Security (CIS) controls (2023) and the ISO27001 (2022) Standard recommended controls for information and data management and security which "preserves confidentiality, integrity, and availability of information" and data;
- depicts major documents across the University's divisions to strengthen the bond between academic and administrative responsibilities; and
- is modeled based on the BC Government, and various universities and external organizations' approach to information and data management and security.