Royal Roads UNIVERSITY

Standard

Title	**NETWORK ACCESS**		
Parent Policy	Information Technology System Security (#1098)	**Responsible Office**	IT Services
Classification	Administrative	**Effective Date**	2024-Jul-31
Category	Information Management & Technology	**Document No.**	1098-S
Approval	Vice-President, Finance and Operations		

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

The most up-to-date versions of the University's standards are posted on the policy and procedure website. If you have printed this standard, 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 PURPOSE

This standard sets out essential requirements for access to Royal Roads University's ("University") network infrastructure to provide protection and security of the IT assets, data and information in the control and/or custody of the University.

2.0 SCOPE AND COMPLIANCE

2.1 This standard extends to **members of the University community**. Non-compliance with this standard may result in disciplinary action, up to and including termination of employment, contract, or other relationship with the University. Allegation 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.

2.2 This standard and related policies, standards, and procedures form the foundation for the University's information and data security in support of the governance policy, *Information and Data Management and Security*, and applicable statutory and regulatory obligations.

3.0 STANDARDS

3.1 **Network Access**

a. IT Services establishes a network access control process to create, manage, review, revise, and revoke access credentials and privileges for **users**, administrators, and service accounts.

b. Access within the University's internal network requires unique, named network accounts and use of a secured, appropriate **passphrase.** IT Services documents ownership of each account and maintains an inventory of such accounts. Anonymous accounts are not permitted.

3.2 **Devices**

The following identifies requirements for devices that connect to the University's internal network:

a. Only **devices** owned and authorized by IT Services are permitted to connect to the University's secured internal network, including the secured wireless network. Unauthorized devices are subject to removal by IT Services.

b. In rare and extenuating circumstances, personally owned devices may connect to the internal network upon authorization as set out in Appendix A.

c. Any modification or change to a device requires prior approval by IT Services. Requests are submitted through the IT Services' Help Desk.

d. IT Services' is permitted to access any device connected to the internal network and such access must comply with the University's established processes.

3.3 **Internal Networks**

a. Prior approval by IT Services is required for a secure connection (e.g. virtual private network) to another private network while using the University's internal network and the operation of any server or service designed to serve files or content with external hosts.

b. Remote connections are facilitated through the University's remote desktop (terminal) server. Direct connections are only permitted for purposes approved by IT Services.

c. Only authorized devices configured to use standardized authentication and strong encryption protocols established by IT Services are permitted to connect to the internal network using wireless technology.

3.4 **Guest Networks**

Guest networks are provided for the convenience of users and guests of the University. These networks are not permitted to operate any server or service designed to access files or content with an external host or to use a connection-sharing technique to create a connection between the internal network and the guest network.

3.5 **Specialty Networks**

a. Industrial Control Systems

Industrial control systems that require a network connection to an external device for purposes of monitoring and maintenance are required to use the University's virtual private network or remote desktop protocol technologies and must utilize a secure multi-factor authentication mechanism.

b. Payment Card Industry (PCI)
Devices that are part of the e-commerce environment and subject to PCI data security standards must be isolated on a separate network segment and may communicate with the internal network over specified network ports solely for purposes of processing e-commerce transactions. No other devices are permitted to connect to this network segment.

4.0 ROLES AND RESPONSIBILITIES

4.1 **Associate Vice President, IT Services (AVP IT Services)**
The AVP IT Services oversees the management of the University's information and IT systems and implements policies, standards, procedures, and other relevant documents to support their integrity and security.

4.2 **IT Services**
Under direction of the AVP, IT Services, the IT Services staff undertakes compliance verification with applicable policy, standard, and/or procedure requirements using recognized industry security practices.

4.3 **Users**
Users are responsible for doing their part to safeguard the University's assets, exercising good judgment when accessing the network and email, and to use these resources for the purposes for which they are intended.

5.0 DEFINITIONS

For the purposes of this standard:

Devices means an IT resource that connects or can connect to the University's wired, wireless, and/or cellular internal and external networks, which includes, but is not limited to desktop computers, laptops, tables, smartphones, cell phones, network jacks, cables, hubs, switches, routers, wireless access points (e.g. wi-fi "hot spots").

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.

Passphrase means a sequence of words relevant to the user and which consists of a minimum of four (4) words, 15 characters in length, and uses a combination of upper and lower case letters, numbers, and symbols.

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

6.0 INTERPRETATION

Refer questions of interpretation or application of this standard to the Responsible Office for resolution.

7.0 RELATED DOCUMENTS

Royal Roads University Documents and Information

- Appendix A – Network Access Authorization Requirements for Personally-owned Devices
- Information and Data Management and Security (policy #1097)
- Information Technology System Security (policy #1098)
- IT Resource Access and Acceptable Use (policy #1063)
- 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	Action
2024-Jul-31	Approved by VP, Finance and Operations; first implementation and effective date
2025-Jul-31	Next Review (one-year post-implementation)

APPENDIX A

NETWORK ACCESS AUTHORIZATION REQUIREMENTS FOR PERSONALLY OWNED DEVICES

1. A user may request authorization to connect their personally owned device to the University's network when:
    a. there is a business need to use their device as part of their role with the University;
    b. the device is configured with software vital to the user's role and the University does not provide such software; and
    c. the device is not provided by the University.
2. A user is required to agree to the following conditions:
    a. IT Services confirms the device meets IT standards prior to connection to the network and undertakes any necessary configuration, which may include encryption;
    b. device use complies with applicable University policies, procedures, and standards;
    c. not to store personally identifiable information on the device unless it has been configured with encrypted drive storage;
    d. files on the device may be considered university information and, if so, must be returned to the University prior to removing the device from use at the University;
    e. to undertake required maintenance and that such maintenance complies with University standards; and
    f. acknowledge that IT Services assumes no liability for the device.
3. The request for authorization must be supported, in writing, by the user's direct supervisor/manager and the unit Director and submitted to IT Services for approval by the CIO (or designate). Approval is required prior to use.