Royal Roads University Policy

Policy Number:
AD8-8
First implemented:
November 21, 2018
Approved By:
RRU Executive
Office of Oversight:
IT Services

policy_statement.jpg

Royal Roads University is committed to the principle of academic freedom. This policy should be interpreted in a manner consistent with that principle and in a manner consistent with applicable statutory and legal obligations, including collective agreements and terms of employment.

The RRU Policy pages are the official source of current, approved policies and procedures. When printed, this document is only current on the date printed. After this date, before relying on the contents of the printed copy, visit the RRU Policy Page for the current document. Questions? Feedback? Contact Don Devenney at 250.391.2600 ext. 4975.

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

OBJECTIVES

- To ensure that the network infrastructure within Royal Roads University (RRU) is protected while remaining accessible to authorised **users** in the delivery of effective and efficient services.
- To set out the minimum requirements for email use within the RRU network.
- To meet statutory and regulatory obligations to protect information in the care and custody of RRU.

POLICY

RRU adopts, implements, and monitors physical, administrative, and technical controls and provides direction regarding appropriate access to and use of its network and email systems to support the integrity and security of **University information** and **IT systems**.

This policy supports the Acceptable Use and Security of University Information and Information Technology (IT) Systems policy and is intended to be read in conjunction with that policy.

COMPLIANCE

Compliance with this policy is required by all RRU employees, faculty members, volunteers, students, and other individuals acting on behalf of RRU (including contracted service providers, as appropriate) who connect or attempts to connect to a RRU network resource. Any exception to this policy requires approval by the IT Governance Committee prior to implementation and is effective only as of the date of approval.

Non-compliance with this policy may result in disciplinary action, including restriction or withdrawal of network access to **University information** and **IT systems**, and/or termination of employment, contract, and/or appointment.

PROVISIONS

1. General Requirements

1.1 Devices

a) Only **devices** owned and managed by RRU and that conform to applicable policies and standards are permitted to connect to RRU's **internal network**. Privately-owned **devices**, including hubs, switches, routers, wireless access points (e.g. wi-fi "hot spots"), represent a significant security risk to RRU's **IT systems**, therefore, may not connect to an **internal network**. Exceptions to this provision for personally-owned **devices** may be granted by the IT Governance Council in specific circumstances and are set out in Appendix "A".

b) Any modification or change to a device requires prior authorisation through IT Services' help desk.

c) Non-conforming **devices** deployed or used are subject to removal by IT Services.

1.2 Network Access

a) Access to **devices** within RRU's **internal network** requires unique, named network accounts. Ownership of each account is documented by IT Services and each account is required to make use of a secured, appropriate passphrase. Anonymous access to the **internal network** is not permitted.

b) Network configurations (e.g., IP addresses computer system names, network protocols) are established by IT Services and any modification is carried out only by IT Services or an authorised **service provider**.

c) IT Services may conduct network security scans with authorisation on a case-by-case basis. The downloading, installing, or running security programs or utilities designed to scan for security

vulnerabilities or exploit resources is permitted to be carried out only by IT Services or an authorised **service provider**.

d) Physical access to network devices is to remain unencumbered at all times.

1.3 Email

a) Email use is intended for RRU business purposes and is guided by RRU policies, applicable legislation, laws, and accepted business practices adopted within RRU.

b) An RRU **commercial electronic message** sent to an external recipient is required to comply with Canada's Anti-Spam Legislation (CASL). Sending and/or forwarding non-RRU **commercial electronic messages** or chain emails are not permitted.

2. Internal Networks

2.1 Connections

A secure connection, such as Virtual Private Network (VPN), to another private network while connected to RRU's **internal network** as well as the operation of any server or service designed to serve files or content with external hosts requires approval by IT Services before use commences.

2.2 Remote Connections

Staff and Faculty who wish to connect to resources on our Internal network such as corporate applications or file shares may do so using RRU's Remote Desktop (Terminal) Server.

Direct connections between the internal network and an Internet connected system represent a significant security risk for RRU, and therefore are only permitted for the purposes of IT Services' troubleshooting or network maintenance.

2.3 Wireless

Only RRU **devices** configured to use standardized authentication and strong encryption protocols as established by IT Services are permitted to connect to the internal network using wireless technology. Personal devices are not permitted to connect to the **internal network** via wireless technology.

3. Guest Networks

Guest networks are provided for **users** and guests of RRU and are subject to the provisions of this policy and the Acceptable Use policy (see Reference section), specifically:

a) use of **devices** or connection sharing techniques in an attempt to create a connection between

the **internal network** and a **guest network** compromises the networks' security and stability, therefore, is not permitted; and

b) **users** of guest networks may not operate any server or service designed to serve files or content with an external host.

4. Specialty Networks – Industrial Control Systems/Payment Card Industry – Data Security Standards (PCI-DSS)

4.1 Industrial Control Systems

Industrial control systems that require a network connection to an external **device** for the purposes of monitoring and maintenance are isolated on a secure network segment. Connectivity to RRU's **internal network**, is through a secure gateway that provides the minimum connectivity required to carry out the functions. External connections to an industrial control system is achieved using Virtual Private Network (VPN) or Remote Desktop Protocol (RDP) technologies and is required to utilize a secure multi-factor authentication mechanism.

4.2 PCI

Devices that are part of the e-commerce environment and subject to PCI standards are isolated on a separate network segment and, subject to the requirements of the PCI data security standards (PCI-DSS), may communicate with **IT systems** on the **internal network** over specific network ports for the purpose of processing e-commerce transactions. **Devices** that are not part of the e-commerce environment may not connect to this specialised network segment.

5. Email

5.1 Privacy and Security

a) RRU encourages the use of email and respects **user** privacy and, does not routinely inspect, monitor, or disclose emails without the **user**'s consent. Exceptions include:

i. automated screening for malicious email and of email that contains confidential financial data;

ii. when required by and consistent with applicable legislation or law;

iii. when a user is unavailable for a significant period of time or is unwilling to provide consent and who is believed to be in possession of information required for RRU to meet its obligations;

iv. when there is reasonable evidence that a violation of legislation, law, applicable RRU policy may have or has occurred and such violation may result in harm to an individual, significant property loss, or liability to RRU; and

v. in an urgent or emergent matter whereby failure to act may compromise the safety, security and integrity of RRU or members of the RRU community.

b) Requests to inspect, monitor, or disclose email set out in s.5.1 are required to be submitted in writing (including email) and require the following approval:

1. vice-president responsible for the **user** faculty member, employee, or contracted service provider who is subject of the request and does not hold a subordinate position to the vice-president; or
2. president for a **user** at the director level and higher or for requests initiated by a vice-president when the subject of the request holds a subordinate position to that vice-president; or
3. the Board of Governors for the president.

c) Mobile **devices** used to access RRU email accounts are required to have appropriate security controls in place. Emails or other sensitive documents stored on a mobile device require encryption and must be secured by a passcode or similar security measure.

5.2 Email Retention

Emails that constitute a business record that requires preservation of the information are retained in accordance with RRU's Records Retention Schedule. **Transitory** emails are not retained and **users** are expected to remove them from the system as soon as practical.

5.3 External Email Systems

Robust controls and safeguards are required to guide **users** regarding external email systems in order to minimize impact to the safety and security of RRU's information and its systems. This includes:

a) To meet regulatory recommendations, the automatic forwarding of RRU email to a third-party email system is not permitted, unless the **user** is a faculty member or an associate faculty member who also carries out duties for another Canadian public body provided that the:

i. email account is a public sector account within Canada;

ii. email system is secure in accordance with RRU standards;

iii. **user** returns any RRU business record to RRU; and

iv. any email forward does not contain confidential information pertaining to RRU.

b) Use of and/or linking to external email systems to conduct RRU business is not permitted.

c) Users are required to contact IT Services prior to engaging an external email marketing service to ensure the proposed service meets Canada's Anti-Spam Legislation and RRU network and email security standards

6. Roles and Responsibilities

6.1 Chief Information Officer (CIO)

The CIO oversees the management of **University information and IT systems** and issues policies, procedures, and other relevant documents to support their integrity and security.

6.2 IT Services

In addition to the specific responsibilities set out in this policy, under the direction of the CIO, IT Services undertakes verification of compliance with this policy utilizing standardized industry security practices which include, but are not limited to, periodic audits (internal and external) and business reporting (formal and informal).

6.3 Supervisors

Supervisors establish and maintain University information and IT systems within their area of responsibility

6.4 Users

Users are expected to aid in safeguarding RRU's resources, exercise careful judgment when accessing the network and email, and to use these resources for the purposes for which they are intended, and to seek direction from their supervisor for issues related to this policy.

DEFINITIONS - For the purposes of this policy:

Commercial electronic message means an electronically-sent message that encourages participation in a commercial activity, including but not limited to offering, advertising, or promoting a product service, or person.

Device means an IT resource that connects or can connect to RRU's external and internal networks, by either wired, wireless, or cellular methods, which includes, but is not limited to, desktop computers, laptops, tablets, smartphones, cell phones, network jacks, cables, and other components.

IT systems means services, devices, and facilities owned, leased, or provided by RRU and that are used to store, processes, or transmit electronic information, which includes, but not limited to:

- computers and computer facilities
- computing hardware and equipment
- mobile computing devices such as laptop computers, smartphones, tablet computers

- electronic storage media such as CDs, USB memory sticks, portable hard drives
- communication gateways and networks
- email systems
- telephone and other voice systems
- software

Internal network means a collection of devices, connected to one another within RRU to form the internal resources and services (e.g. printing, home directory, shared department directories, internal mail, and administrative systems).

Transitory means a record, in any medium, of which the content is required for a limited time period and has no value or usefulness beyond an immediate or minor transaction, is not essential to RRU business, is not required for financial, legal, audit, or statutory purposes, and is in accordance with the Records Retention Schedule.

Service provider means an individual or organisation retained under contract with RRU to perform a service.

University information means recorded information, regardless of format, relating to RRU business that is received, created, deposited, or held by an individual or organisation reporting to or accountable to RRU.

User means faculty members, employees, contracted service providers, students, volunteers, and other individuals who have access to and use RRU's electronic information and IT systems.

REFERENCES

- **Appendix "A"** – Network Access Exceptions for Personally-Owned Devices
- RRU Policies:
  - Acceptable Use and Security of University Information and IT Systems
  - Credit Card Number Handling [1]
- RRU Records Retention Schedule
- Payment Card Industry – Data Security Standards
- Freedom of Information and Protection of Privacy Act, RSBC 1996
- Canada's Anti-Spam Legislation

Links
[1] http://policies.royalroads.ca/policies/credit-card-number-handling-procedures-policy