INFORMATION SECURITY

THOMPSON RIVERS UNIVERSITY
805 TRU Way
Kamloops, BC V2C 0C8
tru.ca

POLICY NUMBER	**BRD 16-1**
APPROVAL DATE	**September 25, 2026**
AUTHORITY	**Board of Governors**
CATEGORY	**Board**
PRIMARY CONTACT	**Associate Vice-President, Digital Strategies and Chief Information Officer**
ADMINISTRATIVE CONTACT	**Director, Information Security**

POLICY

This policy is intended for the general support of and to provide a foundation for the security of the University's information assets and is applicable to all members of the University community.

Information and the associated processes, systems and networks are valuable assets, and the management of personal data has important implications for individuals. The University is committed to the security of information, both within the University and in communications with third parties.

For the purposes of this Policy, "information security" means the preservation of:

a) **Confidentiality** – i.e. protecting information from unauthorized access and disclosure;

b) **Integrity** – i.e. safeguarding the accuracy and completeness of information and processing methods; and

c) **Availability** – i.e. ensuring that information and associated services are available to authorized users when required.

For the purposes of this policy "information" includes information that is printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on visual media, or spoken in conversation. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and/or contractual obligations.

REGULATIONS

1. COMPLIANCE WITH LAW

The University collects, holds and processes information about employees, students, and other data subjects for academic, administrative and commercial purposes. When handling
such information, the University, and those to whom this Policy applies, must comply with the *Freedom of Information and Protection of Privacy Act,* RSBC 1996, c 165 ("FIPPA").

2. RESPONSIBILITIES

2.1. Information security is the responsibility of all members of the University community. Every person handling University related information or using University information systems is required to observe this Policy and these Regulations.

2.2. The University's Chief Information Officer, after consulting with the University's Information Security Committee, may establish specific procedures to ensure information security about University related information. These procedures may include a matrix that defines who is responsible for the security of certain types of information and the measures required to protect that information.

2.3. All members of the University community must report immediately to the Chief Information Officer any observed or suspected security incidents where a breach of this policy has occurred.

3. SECURITY CONTROLS

The University will maintain detection and prevention controls to protect against malicious software and unauthorized access to networks and systems. All users of University computers, including laptops, and all users of computers on which University related information is kept shall comply with procedures established by the Chief Information Officer to ensure that up to date security controls are maintained on those computers. Security controls include, but are not limited to:

3.1. Continuous updates to policies, Incident Response Plan, Disaster Response Plan, Business Continuity Plan, and Risk Register.
3.2. Unified Identity Management
3.3. Multi-factor Authentication (MFA) and Single Sign On (SSO)
3.4. Managed Detection & Response (MDR)
3.5. Antivirus
3.6. Vulnerability Scanning
3.7. Penetration Testing
3.8. Phishing Awareness Training & Simulations

4. POLICY REVIEW

The University's Information Security Committee will review and make any recommendations for updating this policy on a semi-annual basis, or in response to change in regulatory compliance requirements.