THOMPSON RIVERS UNIVERSITY

INFORMATION SECURITY

POLICY NUMBER	BRD 16-1
APPROVAL DATE	MARCH 27, 2009
LAST AMENDMENT	FIRST VERSION
REVIEW DATE	MARCH 27, 2014
AUTHORITY	BOARD OF GOVERNORS
PRIMARY CONTACT	ASSOCIATE VICE-PRESIDENT, IT SERVICES AND CHIEF INFORMATION OFFICER

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 unauthorised 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 authorised 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

I. COMPLIANCE WITH LAW

The University 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 BC Freedom of Information and Protection of Privacy Act (FOIPOP) [RSBC 1996]. Responsibilities under the FOIPOP Act are set out in the University's Information Disclosure Policy -- ADM 2-1, Head (of) Freedom of Information and Protection of Privacy Policy -- ADM 2-0, and the Confidentiality of Student Information Policy -- ADM 2-2.

II. RESPONSIBILITIES

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. The University's Chief Information Officer, after consulting with the University's Information Security Committee may establish specific procedures to ensure information security with regard to 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.

3. **Security Controls** – The University will maintain detection and prevention controls to protect against malicious software and unauthorised 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 in order to ensure that up to date security controls, are maintained on those computers.

4. 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.

III. POLICY REVIEW

The University's Information Security Committee will review and make any recommendations for update of this policy to the President's Council on an annual basis or in response to change in regulatory compliance requirements.