IT END USER COMMUNICATIONS AND ENCRYPTION POLICY

PURPOSE

The IT End User Communications and Encryption Policy is designed to protect Brock University's sensitive data by ensuring that, when sensitive data is electronically transferred to another person or location, or electronically stored, this is done using appropriate encryption methods which prevent unauthorized interception.

SCOPE

This Policy applies to all employees, students, consultants, vendors or any third party who have access to University resources or transmit University data either within or outside the University network. This group will be referred to as users for the balance of this document.

This Policy also applies to employees responsible for the administration of systems or information involved in providing secure communications. This group will be referred to as system administrators for the balance of this document.

If any provision of this Policy is found to be inconsistent with the provisions of a collective agreement, the collective agreement will prevail, unless the Policy provision is required by law, in which case the Policy provision will prevail.

POLICY STATEMENT

The IT End User Communications Standards must be adhered to at all times by users as defined in the Scope above.

- Whenever sensitive data is being electronically transmitted, regardless of method (e.g., email, FTP, etc.), it must be done using appropriate encryption.
- Social media systems must never be used to transmit or post sensitive data without prior data owner consent.

- Data owners are responsible for understanding the confidentiality requirements of the information within their systems, and whether encryption is required.
- Data owners are responsible for engaging with ITS to ensure that the proper encryption is being employed for any sensitive data under their responsibility.
- Data owners must never allow credit card data to be stored in any application or system.

The IT Data Encryption Standards must be adhered to at all times by system administrators as defined in the Scope above. System administrators of sensitive data are responsible for:

- The proper, secure implementation and maintenance of encryption methods.
- The secure storage of encryption keys and passwords used when encrypting sensitive data.
- Ensuring that encryption protocols deemed by NIST (http://www.nist.gov) to be insecure or compromised are not deployed.

DEFINITIONS

Data owner: The person who can authorize or deny access to certain data, and is responsible for its integrity.

Social media system: Any system or application whose purpose is the public sharing of data or messages such as, but not limited to Yammer, Facebook, Twitter, Snapchat, YouTube, etc.

Sensitive data: Data which is deemed sensitive by the Data Owner, including personal information (as defined in the University's Access to Information and Protection of Privacy Policy), or other sensitive information such as credit card data.

System administrator: Is a person who is responsible for the upkeep, configuration, and reliable operation of computer systems; especially multi-user computers, such as servers.

User: An employee, student, consultant, vendor or any third party who has access to University resources or transmit University data either within or outside the University network.

COMPLIANCE AND REPORTING

Information Technology Services ("ITS") enforces this Policy and the related Standards at all times. Anyone who has reason to suspect a deliberate and / or significant violation of this Policy is encouraged to promptly report it to the ITS Help Desk in line with the Safe Disclosure Policy. Policy violations that come to the attention of the ITS Help Desk will be referred to the Director, Infrastructure.

Policy violations will be assessed, and action taken to remediate the violation, subject to any relevant collective agreements and/ or other contractual conditions.

Where Policy violations are considered severe and / or cannot be easily remediated, the incident will be referred to the Associate Vice-President, ITS for further action, subject to any relevant collective agreements and/ or other contractual conditions. Periodically, the AVP, ITS will provide to SAC a summary of all policy violations.

Policy owner:	Associate Vice-President, Information Technology Services
Authorized by:	Current version: Executive Team Prior versions: Board of Trustees, Capital Infrastructure Committee
Accepted by:	Senior Administrative Council
Effective date:	December 2021
Next review:	December 2022
Revision history:	2020 2019 2017
Related documents:	IT Encryption Standards IT End User Communications Standards Safe Disclosure Policy