Brock University

IT INCIDENT RESPONSE POLICY

PURPOSE

The purpose of the Information Technology (“IT”) Incident Response Policy is to limit the potential impact of IT incidents affecting enterprise level IT services.

Note that an IT incident and an IT security incident are treated differently as outlined in the associated Standards.

SCOPE

This Policy applies to all users of Brock University’s IT systems, including employees (i.e., faculty and staff), students, contractors, consultants and visitors (e.g., visiting scholars, guests, other third parties, etc.) with respect to all actual or suspected IT incidents.

In the event that any provision of this Policy is found to be inconsistent with the provisions of a collective agreement, the collective agreement will prevail.

POLICY STATEMENT

The security of the Brock University technology environment is critical to maintaining the confidentiality, integrity and availability of the University’s technology and data.

This Policy and the related Standards outline the process for identifying, containing and remediating an IT incident.

Reporting an IT incident: All IT incidents must be reported to the IT Help Desk immediately upon detection.

Responding to an IT incident: All IT incidents must be assessed by the top-ranking IT employee responding to the incident in terms of the number of users affected and the urgency of the response required.

If the incident is assessed to be an information security incident, the Information Technology Security Incident Response

Standards must be followed. All other IT incidents must follow the IT Incident Response Standards.

Documentation: An IT Incident Report must be completed and reviewed for accuracy by the incident response team and the owner of the service(s) / system(s) affected.

DEFINITIONS

IT Incident – An unplanned interruption to an IT service or reduction in the quality of an IT service.

IT Security Incident – Any event that negatively impacts or represents a serious threat to Brock University's assets such that there is a negative impact on their confidentiality, integrity or availability, or Brock assets are used to negatively impact external third parties, or negatively impact the University's reputation, or negatively impact Brock or its users financially.

CSIRT (Computer Security Incident Response Team) - The team responsible for responding to IT security incidents. The CSIRT will act under the direction of the CSIRT Manager and will be dynamically composed of personnel who are best positioned to provide an effective response in the context of the specific incident.

COMPLIANCE AND REPORTING

This Policy is under the jurisdiction of the Associate Vice-President, Information Technology Services (AVP, ITS). Each authorized user of the University's IT systems is required to comply with this Policy and related documents.

Exceptions to this Policy must be documented and authorized by the Vice-President, Administration, and presented to ITS.

Incidents determined to be in non-compliance with this Policy will be assessed for severity and will carry a possible range of sanctions. Policy violations will be assessed and action taken to remediate the violation, including consequences where appropriate, subject to collective agreements and / or other contractual conditions.

Where Policy violations are considered severe and / or cannot be easily remediated, the incident will be escalated to the AVP, ITS for further action.

Periodically, the AVP, ITS will provide to SAC a summary of known policy violations.

Policy owner:	Associate Vice-President, Information Technology Services
Authorized by:	Board of Trustees, Capital Infrastructure Committee
Accepted by:	Senior Administrative Council
Effective date:	December 2021
Next review:	December 2022
Revision history:	2017 2016
Related documents:	IT Security Incident Response Standards IT Incident Response Standards Privacy Breach Notification Procedure