IT SECURITY INCIDENT RESPONSE STANDARDS

PURPOSE

A standard includes specific low level mandatory controls that help enforce and support a policy. The purpose of this document is to support and outline in detail the requirements of the IT Incident Response Policy.

Security incidents are unique and require different handling than IT incidents. This IT Security Incident Response Standard is documented to address these differences and provide a timely and coordinated response to security incidents that could adversely impact Brock University.

The IT Security Incident Response Standards define the role, membership and responsibilities of the Computer Security Incident Response Team (CSIRT) as well as describe the 5 critical stages of IT security incident response.

Security Incident Classification Matrix

All IT security incidents are considered high priority and are defined below in the IT Security Incident Classification Matrix:

IT Security Incident Classification Matrix	
Category	**Description**
Data Breach	A security incident in which sensitive data is copied, transmitted, viewed, stolen or used by an unauthorized individual or entity.
Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
Email	Spoofed email, phishing, SPAM and other email security-related events.
Investigation	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.
Malicious Code/ Malware	Successful installation of malicious software (e.g., virus, worm, Trojan horse or other code-based malicious entity) that infects an operating system or application. This does not apply to malicious code that has been successfully quarantined by antivirus (AV) software.

IT Security Incident Classification Matrix	
Category	**Description**
Policy Violation	A violation of any published ITS policy that has a direct or indirect impact to the functionality of networks, systems or applications or is in direct contravention of any policy published by Brock University.
Unauthorized Access	Logical or physical access to a Brock University network, system application or data gained without permission by an individual.

Computer Security Incident Response Team (CSIRT)

What is CSIRT?

CSIRT is the group that develops, tests and implements responses to information security incidents. The CSIRT acts under the direction of the CSIRT Manager and is dynamically composed of personnel who are best positioned to provide an effective response in the context of the specific incident.

Reporting an IT Security Incident

All IT security incidents must be reported to the CSIRT Manager immediately upon detection.

Responding to an IT Security Incident

All IT security incidents must be assessed by the CSIRT Manager or their designate. They must assign duties to CSIRT members to identify, contain, notify and remediate the event.

Roles and Responsibilities

CSIRT Manager

In the event of a security incident, the AVP, ITS assumes the role of the CSIRT Manager unless unavailable, in which case, the Director, Client Services assumes the role.

The CSIRT Manager is responsible for the implementation of these Standards immediately upon notification or discovery of an IT security incident, and will form and manage the CSIRT to match the incident.

Responsibilities:

- Responsible for overall CSIRT response and contributes as part of the CSIRT
- Validates CSIRT involvement and ensures this process is followed
- Communicates regularly with the University's Senior Administrators as required
- May initiate contact with the University's Insurance Co-ordinator if required. A determination will be made with the insurer whether to involve an external forensics expert
- Coordinates CSIRT activities through meetings, conference calls and regular communication through Blackberry Messenger group "BBM ITS"
- Monitors CSIRT resources and engages additional resources as required
- Approves improvements to the Information Security Incident Response Process.

CSIRT members

The CSIRT may comprise of individuals from different disciplines internal and external to the University to address issues that may arise during or from a security incident.

Responsibilities:

- Resolve assigned security incidents in a coordinated response
- Engage with team members and members of other teams in a timely manner
- Escalate to vendors as required
- Work with vendors to troubleshoot as required and provide any required information (e.g., logs, etc.)
- Provide regular updates to CSIRT Manager
- Engage external entities as necessary (e.g., law enforcement, forensic support, regulatory agencies).

Members of the CSIRT include the AVP, ITS, the IT Security Specialist, Brock University legal counsel, University Communications staff, Risk Management and various IT staff with the necessary technical skills and escalated privileges to effectively respond to the security incident.

Subject Matter Expert(s)

Subject matter expert(s) ("SME") may be contacted to assist in determining the severity and resolution of the security incident. The SME must continue working on the security incident until it is resolved and / or they are relieved of their duties.

A list of SMEs is maintained in the SharePoint ITS Team site.

Reporting Source	Responsibility: • Report any suspected security incident as defined by the IT Security Incident Classification Matrix to the ITS Help Desk.

Process

All information security incidents must progress through the phases below:

1. Preparation

This phase deals with the preparation needed to properly handle incidents by the CSIRT. It is intended to foresee all the tools, policies, access and pre-established relationships that need to be in place for an efficient and swift incident response process.

2. Detection & Analysis

This stage is the primary stage where the CSIRT team receives notification of a security incident as described in the IT Security Incident Classification Matrix from:

End User	Report any suspected security incident as defined by the IT Security Incident Classification Matrix to the ITS Help Desk.
ITS Help Desk and Client Services	Responsibilities: • Assess the situation for impact and priority • Determine if the incident is an IT security incident by referring to the IT Security Incident Classification matrix above o If the incident falls into one of the security categories above, create an incident ticket and assign to CSIRT Manager

3. Containment

The primary purpose of this stage is to limit and prevent any further damage. There are several steps to this phase; each is necessary in order to completely mitigate the incident and prevent the destruction of any evidence that may be needed later.

Incident involving Personal Information

The University's Privacy Breach Notification Procedure must be enacted in the event of a security incident involving Personal Information, as defined by the University's Access to Information and Protection of Privacy Policy.

Short term containment

The focus of this step is to limit the damage as soon as possible.

Short-term containment range from isolating a network segment of infected workstations to taking down a compromised production server and having all traffic routed to a failover server. Short-term containment is not intended to be a long term solution to the problem.

System backup

A backup of all affected systems is necessary after short term containment is complete and before any additional steps are taken to remedy the security incident in order to preserve the state of the system(s).

The backup will capture the affected system(s) as they were during the incident, thereby preserving evidence in the event that the incident resulted from a criminal act or for observing how the system(s) were compromised during the lessons learned phase.

Long-term containment

This is the point at which the affected systems can be temporarily fixed in order to allow continued use in production, if necessary, while rebuilding clean systems.

The primary focus is on removing accounts and/or backdoors left by attackers on affected systems, installing security patches on both affected and neighbouring systems and doing other work to limit further damage while allowing normal University operations to continue.

Notification

The CSIRT Manager or designate must notify owners of the information systems either affected or suspected of being affected by an IT security incident. The CSIRT Manager must keep the owners

of the affected systems apprised of the progress of the incident response.

Collection of incident data

All data collected during the incident response must be kept secure and confidential at all times. Only staff involved with the incident response will have access to the collected data.

4. Eradication and Recovery

Controls implementation

The CSIRT Manager will coordinate the deployment of controls or countermeasures to ensure that the security incident does not reoccur once the service is back in production. Examples of controls include but are not limited to:

- Modifying firewall rules or device configurations;
- Applying security patches or recommending such actions where appropriate;
- Updating virus signatures;
- Rebuilding systems from known clean images.

Re-activation

If evidence of a breach cannot be established through investigation, or if the incident has been resolved, then the CSIRT Manager will authorize the reactivation of any disabled services where applicable.

5. Post incident

Subsequent disciplinary or legal action

Any subsequent disciplinary or legal action will be at the discretion of the Vice-President, Administration and / or the senior administrators with advice from the University's Legal Counsel.

Incident involving a staff member

If the security incident involves a staff member, the incident must be reported by the CSIRT Manager to the staff member's supervisor for follow-up action.

Incident involving a student

If the security incident involves a student, the incident must be referred by the CSIRT Manager to the Vice-Provost, Enrolment Management and International for follow-up action.

Incident involving

If the security incident involves parties external to the University and these parties can be identified during the course of the investigation

non-Brock community member

by the CSIRT, the incident must be referred by the CSIRT Manager to the University's legal counsel for follow-up action.

Lessons learned

The **CSIRT lessons learned meeting** should be held as soon as possible, and ideally within two weeks of the incident.

The lessons learned meeting should include, but not be limited to the following:

- When was the problem first detected and by whom;
- The scope of the incident;
- How the incident was contained and eradicated;
- Worked performed during recovery;
- Areas where the CSIRT team was effective;
- Areas that need improvement.

The meeting should also include time for suggestions and discussion between CSIRT members on how to improve the overall process. This phase is extremely beneficial, as it allows members to share ideas and information, and improve team effectiveness in future incidents.

Documentation / Reporting and Communication

Documentation

An IT Incident Report must be completed for all security incidents. The report should answer the following: Who, What, Where, Why, and How questions that may come up during the lessons learned meeting.

The overall goal is to learn from the incident to improve the team's performance and serve as reference materials in the event of a similar incident.

Documentation may also be used as training material for new team members, or as a benchmark for future incidents.
All documentation, including the IT Incident Report, must be filed in Footprints.

Reporting

A Privacy Breach Report must be provided to the Coordinator, Freedom of Information And Privacy by the AVP, ITS for any security incident involving Personal Information as defined by the University's Access to Information and Protection of Privacy Policy.

Communication: external agencies	Only the University's legal counsel or the Coordinator, Freedom Of Information And Privacy is authorized to liaise directly with external agencies regarding security incidents. This includes requests from law enforcement agencies, government departments or private corporations.
Communication: media	Only the Marketing and Communications Department is authorized to respond to questions from media representatives regarding the security incident.