STANDARD	**SECURITY INCIDENT RESPONSE**
Owner: **BTS**	Approved Date: **November 13, 2024**

SUMMARY

The purpose of this standard is to support the secure use of NorQuest computer equipment. These rules are in place to protect both the employee and NorQuest. Inappropriate use of computer equipment exposes NorQuest to risks including virus attacks, compromise of network systems and services, availability of services and bandwidth in the pursuit of the organizational goals and legal issues. This standard enforces the principle of defense in depth and monitoring the effectiveness of security controls, while ensuring compliance with organizational, legal and regulatory requirements.

Business Technology Services (BTS) has the responsibility to ensure appropriate practices are adopted to conform to this standard and the Digital Security Policy that it supports.

APPROVAL

Approved by:	David Melanson	**Position:**	Director, BTS
Signature:	David Melanson	**Date:**	**October 30, 2024**
Approved by:	Jill Matthew	**Position:**	VP, Administration & CFO
Signature:	Jill	**Date:**	**November 13, 2024**

SCOPE

All digital systems utilized for the purpose of carrying out the mission of NorQuest College.

AUTHORITY

This standard has been created under the authority of Corporate Services & Finance and BTS which maintains the right to ensure that this standard is adhered to.

LINK ACCESSIBILITY

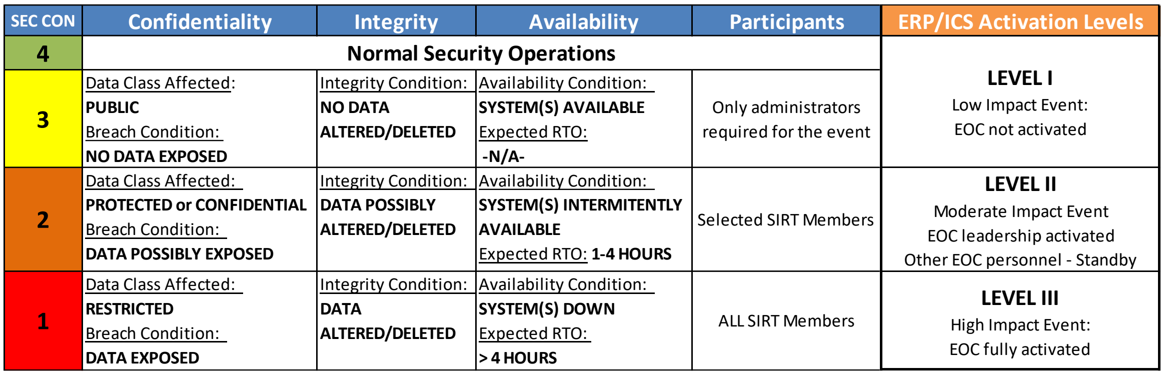
Note: Some of the links included in this document are intended for internal use only. Please be aware that access to these links may be restricted to authorized personnel.

EXCEPTIONS

A request for exception to this standard must be submitted for approval to the Director of BTS by following the process as described in the Digital Security Exception Request Procedure. Granted exceptions will be for up to a one year term and will be reviewed annually at which time the exception may be revoked, revalidated or extended for another one year term. Exceptions will be maintained by BTS.

STANDARD

1. **Mission:** The mission of the Security Incident Response Team (SIRT) is to contribute to the continual improvement of the security of NorQuest's information infrastructure and to detect, analyze, contain, eradicate and recover from security incidents affecting the constituency.
2. **Constituency:** The constituency of the NorQuest SIRT is defined as "NorQuest", the domain "norquest.ca" and any associated domains.
3. **Purpose:** The purpose of the SIRT during a security event is to:
    a. **Analyze –** Understand the nature of the event
    b. **Contain –** Suppress the incident from growing larger and causing further/greater harm to the environment
    c. **Eradicate** – Remove or permanently disable and render harmless the causes of the event
    d. **Recover** – Bring systems and or data back to as close as possible to pre-event operation
4. **Authority:** The SIRT Lead has the authority, in consultation with the SIRT, to take any and all action required in the detection, analysis, containment, eradication and recovery of NorQuest Digital Systems during a declared Security Incident.
5. **Declaration of a Security Incident:** The SIRT Lead declares a security incident and the corresponding closure of a security incident.
6. **Security Incident Prioritization:** The declaration of a Security Incident will be accompanied by a Security Condition (SEC CON) level determined using the following table for determination:

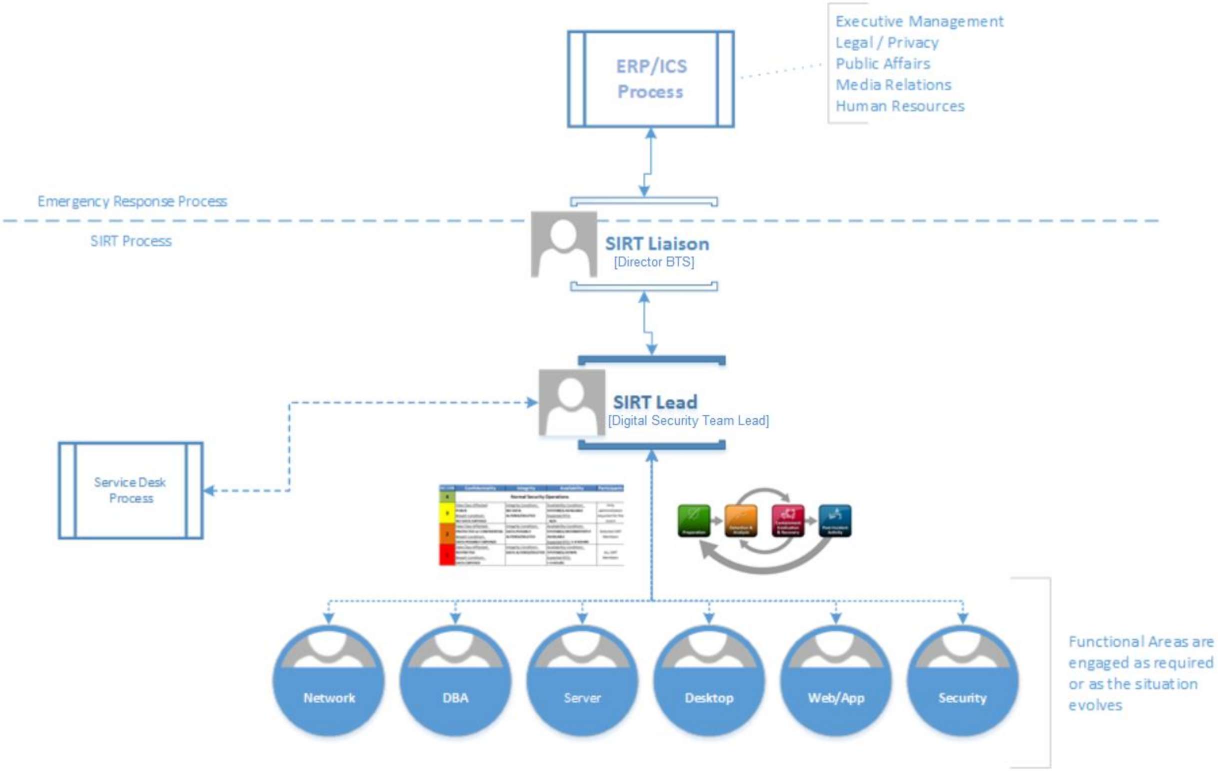


SEC CON	Confidentiality	Integrity	Availability	Participants	ERP/ICS Activation Levels
4	**Normal Security Operations**				**LEVEL I** Low Impact Event: EOC not activated
3	Data Class Affected: **PUBLIC** Breach Condition: **NO DATA EXPOSED**	Integrity Condition: **NO DATA ALTERED/DELETED**	Availability Condition: **SYSTEM(S) AVAILABLE** Expected RTO: **-N/A-**	Only administrators required for the event	
2	Data Class Affected: **PROTECTED or CONFIDENTIAL** Breach Condition: **DATA POSSIBLY EXPOSED**	Integrity Condition: **DATA POSSIBLY ALTERED/DELETED**	Availability Condition: **SYSTEM(S) INTERMITENTLY AVAILABLE** Expected RTO: **1-4 HOURS**	Selected SIRT Members	**LEVEL II** Moderate Impact Event EOC leadership activated Other EOC personnel - Standby
1	Data Class Affected: **RESTRICTED** Breach Condition: **DATA EXPOSED**	Integrity Condition: **DATA ALTERED/DELETED**	Availability Condition: **SYSTEM(S) DOWN** Expected RTO: **> 4 HOURS**	ALL SIRT Members	**LEVEL III** High Impact Event: EOC fully activated

7. **SIRT Membership:** The SIRT shall include representation from the following groups/ functional areas:
    a. Network
    b. Database Admin
    c. Server Admin
    d. Desktop
    e. Web Admin
    f. Application Admin
    g. Security
    h. Service Desk
8. **SIRT Leadership:** The SIRT shall be led by the Digital Security Team Lead and the Digital Security Team Lead shall liaise with the Director of BTS as required to interface with the college ERP process (as required).

9. **ERP/ICS:** The SIRT will have access to the following corporate functions through the Emergency Response Plan / Incident Command System, if access is invoked due to the SECCON level declared.

    a. Executive Management
    b. Legal / Privacy
    c. Public Affairs
    d. Media Relations
    e. Human Resources



10. **Reporting:** Upon closing of a Security Incident, a report shall be created that includes at minimum:

    a. A summary of the Security Incident
    b. Actions taken to identify, contain and eradicate the incident
    c. A summary of recovery efforts
    d. Any lessons learned and remediation items to be undertaken

11. **Communications**

    a. Internal Communications – shall be handled through the Service Desk to the appropriate internal audience.
    b. External Communications – (if required) shall be handled through the ERP/ICS Structure.

PLAYBOOKS

NorQuest College utilizes playbooks with detailed steps for containing security incidents. Access our incident containment playbooks here for more information on the strategies in place.

CONTACTS

For urgent incident response or assistance, please search for the positions below on the NorQuest Organizational Chart to identify the person's name, then search for their contact information on Connect.

- Digital Security Team Lead
- Director, BTS (Business Technology Services)
- Manager, Emergency and Business Services

DEFINITIONS

1. **Connect** – NorQuest's internal platform that centralizes internal documents and the NorQuest Organizational Chart.
2. **Emergency Operations Center (EOC)** – This is the construct setup to allow for a central location for the orchestration of a declared emergency.
3. **Emergency Response Plan / Incident Command System (ERP/ICS) –** Is a term used in the NorQuest Emergency Response Plan and denotes the Emergency Response Plan itself (which can be found on Connect); Incident Command System is the structure in place to allow for communications when there is an emergency declared.
4. **Recovery Time Objective (RTO)** – is the targeted duration of time within which a business process must be restored after a disaster (or disruption like a Security Incident) in order to avoid unacceptable consequences.
5. **Security Incident –** As per the National Institute of Standards and Technology (NIST), a security incident is a cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.

REVISION AND REVIEW HISTORY

This Standard is to be reviewed annually, with the allowance for ad hoc changes as required.

Date	Version	Evaluation	Author	Summary
Mar 21, 2017	0.1	Review	Curtis L. Blais	Initial Draft
Mar 29, 2017	0.2	Review	Curtis L. Blais	Separated Web & Application Admins as Members of SIRT
Aug 14, 2017	0.3	Review	Curtis L. Blais	Adjusted scope text
Feb 12, 2018	0.4	Review	Curtis L. Blais	Adjusted for review by BTS
May 2, 2018	1.0	Revision	Curtis L. Blais	Finalize
Nov 2, 2021	1.1	Review	Curtis L. Blais	Updated the Dept/Div. To match current organization.
Feb 22, 2022	1.2	Revision	Peter Rajic	Updated "Incident Communication Structure" to "Incident Command System"
Aug 15, 2023	1.3	Revision	Dorian Maldonado	Updated "Security Incident" definition. Updated SIRT Liaison to "Director BTS". Updated CISO to Digital Security Team Lead.
Oct 25, 2024	1.4	Revision	Daniel Q. del Lama	Updated Data Classification to Public. Added Link Accessibility, Playbooks and Contacts section.
Oct 30, 2024	1.5	Revision	Dave Melanson	Corrected minor grammatical errors.
Nov 13, 2024	2.0	Revision	Dave Melanson	Approved Version