BANFF
CENTRE
FOR ARTS AND
CREATIVITY

Banff Centre Policy
Banff Centre Procedure
Additional Information

Category	Information Technologies and Services
Type	**Procedure**
Title	**Information Security - Incident Response Plan**
Approval Authority	VP, Administration and Chief Financial Officer
Implementation Authority	Chief Information Officer
Related Policy	Information Security Policy
Related Procedure(s)	Information Security - Storage and Distribution
Related Additional Information	N/A
Original Approval Date	July 18, 2017
Original Effective Date	July 18, 2017
Most Recent Revision Date	March 1, 2019
Next Review Date	March 1, 2021

PURPOSE

Centralized notification and control of **Information Security Incident** investigations is necessary to ensure that immediate attention and appropriate resources are applied to control, eliminate and determine the root cause of events that could potentially disrupt the operation of **Banff Centre** or compromise **Banff Centre Information**.

The goal of this Procedure is to:

- Identify accountability for responding to Information Security Incidents,
- Ensure appropriate escalation,
- Ensure effective administrative response to Information Security Incidents,
- Streamline the response process, and
- Secure and protect Banff Centre Information in order to minimize the organizational impact of Information Security Incidents.

SCOPE

This plan applies to Information Security Incidents that affect **Banff Centre Community**'s information technology facilities, infrastructure or data assets, including but not limited to servers, workstations, firewalls, routers, switches, and externally hosted systems and infrastructure.

PROCEDURE

1. **Reporting an Information Security Incident**
    a. All suspected Information Security Incidents must be reported immediately to **Banff Centre ITS.** From 8:30pm to 4:30pm call the ITS Help Desk at 403-762-6268. Outside of these hours call ext. 6673 (MORE) from an internal phone or 403-762-6673 from an

external phone. The message will give you instruction to press 0. Your call is then routed either to a third party technician or to one of our IT/S on-call staff. Internal ext. 4357 (HELP) can be used as well. Where the Information Security Incident involves physical security issues in addition to Banff Centre Information security issues, the incident must be reported to Banff Centre's Campus Security via 403-762-6438 who will in turn alert the ITS Help Desk or on-call staff outside of business hours.

b. Information Security Incident types include but are not limited to:
   i. Malicious code attacks - attacks by programs such as viruses, Trojan horses, worms, rootkits, and scripts to gain privileges, capture passwords, and/or modify audit logs to hide unauthorized activity;
   ii. Unauthorized access - includes unauthorized users logging into a legitimate account, unauthorized access to files and directories, unauthorized operation of "sniffer" devices or rogue wireless access points;
   iii. Disruption of services - includes erasing of programs or data, ransomware, email spamming, denial of service attacks or altering system functionality;
   iv. Misuse - involves the utilization of computer resources other than for official purposes;
   v. Espionage - stealing information to subvert the interests of Banff Centre or a related entity;
   vi. Hoaxes - for example, an email warning of a nonexistent virus;
   vii. Unusual events – includes erratic and persistent unusual system behavior on desktops, servers or the Banff Centre network; inexplicable lock out of user accounts; or the existence of a strange process running and accumulating significant CPU time.

2. Managing the Information Security Incident

a. All incidents

i. Chief Information Officer (or designate) will assign a **CSIRT Coordinator**.

ii. CSIRT Coordinator and Chief Information Officer (in consultation with the VP, Administration and Chief Financial and/or **FOIP** Coordinator (or designates) as appropriate) will identify the incident severity with regard to the scope and type of problem, and classify the incident as minor, medium or severe based on the perceived risk to Banff Centre resources:

   1. Minor - incidents for which there are routine solutions where sensitive information has not been exposed or accessed by unauthorized parties. The consequences of this incident would either
      a. threaten the efficiency or effectiveness of some institution services, but would be dealt with internally by management. Monetary, privacy, health, safety & well-being or public confidence loss would be of low consequence.

Or

b. be dealt with by routine institution operations. Monetary, privacy, health, safety & well-being or public confidence loss would be of negligible consequence.;

2. Medium - The consequences of this incident **<u>would not</u>** threaten the delivery of services, but **<u>could</u>** mean the business operations and administration of Banff Centre services would be subject to significant review or changed ways of operating involving the **<u>Senior Leadership Team</u>**. Monetary, privacy, health, safety & well-being or public confidence loss would have medium consequences to Banff Centre.; or
3. Severe - incidents that involve significant personal data leakage or compromised Banff Centre Information, or that impact a significant number of users, all of which have significant consequences. The consequences of this incident **<u>would</u>** threaten the delivery of key services and **<u>would</u>** mean the business operations and administration of Banff Centre would be subject to significant review or changed ways of operating involving the **<u>Senior Leadership Team</u>** **<u>and/or Board intervention</u>**. Monetary, privacy, health, safety & well-being or public confidence loss would have very high consequences for Banff Centre.

iii. CSIRT Coordinator will help support the **CSIRT** members by administering the following:

1. Creating an incident file;
2. In consultation with other CSIRT members, ensuring appropriate organizations external to Banff Centre are notified in accordance with legislation or otherwise (including relevant police agencies and the Office of the Information and Privacy Commissioner of Alberta where necessary under Alberta's *Freedom of Information and Protection of Privacy Act* (**FOIP**);
3. Taking corrective action in accordance with best practices for securing and preserving electronic evidence;
4. Together with the Chief Information Officer, reporting, as needed, to the appropriate Banff Centre department for further action or discipline (in consultation with Human Resources); and
5. Closing the incident file.

b. **Minor incidents**

i. Chief Information Officer (or designate) will identify the members for the CSIRT and supervise the CSIRT Coordinator in administering the response to the Information Security Incident.

c. **Medium and severe incidents**
    i. The Chief Information Officer will:
        1. Brief the VP, Administration and Chief Financial Officer.
    ii. Chief Information Officer, VP, Administration and Chief Financial Officer in consultation with the FOIP Coordinator (or designates) will:
        1. Form a CSIRT to include the relevant owner(s) of the data or issue; and
        2. Identify the other members for the CSIRT drawn from the following individuals (or their designates) as deemed necessary for addressing the incident in question:
            a. CSIRT Coordinator;
            b. Chief Information Officer;
            c. VP, Administration and Chief Financial Officer;
            d. Legal counsel;
            e. Insurance company;
            f. Breach consultant;
            g. FOIP Coordinator;
            h. Vice President, Human Resources;
            i. Director, Program Administration, Office of the Registrar;
            j. Manager, Security;
            k. Vice President, Marketing and Communications; and/or
            l. Others as determined necessary by the Chief Information Officer and the VP, Administration and Chief Financial Officer.
        3. Determine if there has been loss of, unauthorized access to or unauthorized disclosure of personal information. In the event personal information has been compromised, Banff Centre shall comply with any additional reporting obligations required by legislation, including reporting to the Office of the Information and Privacy Commissioner of Alberta where necessary under FOIP.
    iii. CSIRT Coordinator will, under the supervision of the Chief Information Officer:
        1. Administer the response to the incident (except for those tasks specifically administered by the Chief Information Officer and/or VP, Administration and Chief Financial Officer as noted below for severe incidents);
        2. Provide regular briefings to the CSIRT by email at least once a day and more often at the outset - even if there has been "no change"; and
        3. Write a closing incident report that is shared with the CSIRT.
    iv. On a quarterly basis, the Chief Information Officer shall prepare a report summarizing the following activities:
        1. an update on information security measures; and
        2. details of any medium and severe Information Security Incidents.

    The Chief Information Officer shall present this report to the VP, Administration and Chief Financial Officer for reporting to the **Senior Leadership Team** and as a standing item for quarterly reporting to the Board of Governors of Banff Centre or the Audit and Finance Committee (as appropriate).

d. Medium Incidents
    i. The VP, Administration and Chief Financial Officer will:

1. Within 24 hours of receiving the briefing referred to in section 2(c)(i)(1) above, will notify the Assistant Deputy Minister.
2. Share the preliminary Cyber Security Incident Reporting Form with the Assistant Deputy Minister.

e. **Severe incidents**

i. The Chief Information Officer will:

1. Brief any other relevant members of the Senior Leadership Team;
2. Receive regular reports on risks from the CSIRT and communicate them to the VP, Administration and Chief Financial Officer, FOIP Coordinator and any other relevant members of the Senior Leadership Team;
3. Ensure risk is managed in consultation with the VP, Administration and Chief Financial Officer and any other relevant members of the Senior Leadership Team;
4. Activate Banff Centre's Disaster Response Plan (DRP) if the situation requires, based on the impact on persons, property and the environment; and
5. Provide the closing incident report to the VP, Administration and Chief Financial Officer, and any other relevant members of the Senior Leadership Team that assisted in the management of the incident.

ii. The VP, Administration and Chief Financial Officer will:

1. Upon receiving the briefing referred to in section 2(e)(i)(1) above, immediately notify the President and CEO and the Chair of Banff Centre's Board of Governors; and
2. Present a summary of the closing incident report to the President and CEO and the Chair of Banff Centre's Board of Governors.

iii. The President and CEO will:

1. Within 24 hours of receiving the briefing referred to in section 2(e)(ii)(1) above, will notify the Deputy Minister.
2. Share the preliminary Cyber Security Incident Reporting Form with the Deputy Minister.

3. **Closing the Information Security Incident**

a. A closing incident report shall be prepared by the CSIRT Coordinator for medium and severe incidents.

b. The closing incident report shall be stored on SharePoint in a secure area after approval from the VP, Administration and Chief Financial Officer.

c. The closing incident report shall include:

i. Chronology of the incident and actions taken;

ii. Scope of risk Banff Centre faced during the incident (e.g., number of records and degree of exposure);

iii. Description of action taken to mitigate and resolve the issue;

iv. Communications that were provided;

v. Brief explanation of basis for key decisions;

vi. Evaluation of whether response plan was followed; and

vii. Identification of internal improvements to infrastructure, systems and the incident response plan, along with any other actions that are recommended.

d. For medium and severe incidents share the finalized Cyber Security Incident Reporting Form with the Ministry.

4. Managing rogue access points

A centrally monitored system shall be used to continually detect unauthorized/rogue wireless devices within the Banff Centre network. If a rogue access point is detected within 50 meters of a **Cardholder Data Environment**, an alert shall be generated and Banff Centre ITS shall automatically be contacted to investigate and, if appropriate, remove the wireless device.

DEFINITIONS

Any definitions listed in the following table apply to this document only with no implied or intended institution-wide use.

Defined Term	Definition
Approval Authority	The individual or entity with the authority to approve this Procedure.
Banff Centre	Banff Centre for Arts and Creativity.
Banff Centre Community	Persons associated with Banff Centre including: • members of Banff Centre’s Board of Governors; • members of the Board of Directors of The Banff Centre Foundation; • members of the Senior Leadership Team ; • staff, including sessional workers; • volunteers; • artists, including practicums; • others performing activities or providing goods or services at or under the auspices of Banff Centre, including consultants, guests, vendors and contractors.
Banff Centre Information	Information, regardless of its source, that is stored or shared on any medium in the custody or under the control of Banff Centre, including copyrighted material in the custody or control of Banff Centre Community members, such as works of art or computer software.
Banff Centre ITS	Banff Centre’s Information Technologies and Services department.

Cardholder Data Environment	The computer environment wherein credit cardholder data is transferred, processed, or stored, and any networks or devices directly connected to that environment.
CSIRT	Computer security incident response team
CSIRT Coordinator	The CSIRT Coordinator is a member of the Information Technologies and Services team assigned this role by the Chief Information Officer and is charged with administering an Information Security Incident.
Cyber Security Incident Reporting Form	The Post-Secondary Institution Cyber Security Incident Reporting Form is used to notify the appropriate stakeholders at Advanced Education of a significant incident within their institution. A copy of the form is located in SharePoint with the Information Security Policy and Procedures.
FOIP	Alberta's *Freedom of Information and Protection of Privacy Act*
FOIP Coordinator	The person assigned this role who is responsible for managing Banff Centre's access and privacy responsibilities.
Implementation Authority	The individual or position with responsibility for implementing this Procedure.
Information Security Incident	An incident where there is suspicion that: • confidentiality, integrity or accessibility of Banff Centre Information has been compromised; • computer systems or infrastructure has been attacked; and/or • vulnerability in technology or systems Banff Centre is using to house Banff Centre Information has been made public.
Ministry	The Ministry of Advanced Education is responsible for public post-secondary institutions in Alberta.
Senior Leadership Team	Includes President and CEO, and Vice Presidents of Banff Centre.

RELATED DOCUMENTS

- **Relevant legislation**
  - Alberta's *Freedom of Information and Protection of Privacy Act (FOIP)*

    - *Personal Information Protection and Electronic Documents Act (PIPEDA)* - applicable to The Banff Centre Foundation only
    - Alberta's *Personal Information Protection Act (PIPA)* – applicable to The Banff Centre Foundation only
    -
- **Relevant Banff Centre policies and procedures**
    - *Policy – Information Security Policy*
    - *Procedure – Information Security - Storage and Distribution*
    - *Banff Centre's Disaster Response Plan*

MODIFICATION HISTORY

Original Approval Date:	July 18. 2017
Effective Date:	July 18. 2017
Subsequent Revision Dates:	March 1, 2019

CONTACT

For enquiries relating to this Procedure, please contact the Chief Information Officer:

- Email: cio@banffcentre.ca
- Phone: Ext. 6543