Banff Centre Policy
Banff Centre Procedure
Additional Information

Category	Information Technologies and Services
Type	**Policy**
Title	**Information Security Policy**
Approval Authority	Board of Governors of Banff Centre
Implementation Authority	Chief Information Officer
Related Policy	N/A
Related Procedure(s)	• Information Security - Storage and Distribution • Information Security - Incident Response Plan • Information Security – Technology and Travel
Related Additional Information	N/A
Original Approval Date	May 26, 2017
Original Effective Date	June 18, 2017
Most Recent Revision Date	March 1, 2019
Next Review Date	March 1, 2021

PURPOSE

Banff Centre is committed to creating a secure yet open information and communication environment in which **Banff Centre** can teach, learn, conduct research, perform administrative functions and carry out other business related purposes. Banff Centre has business, ethical, and legal responsibilities to protect all forms of records and information in its custody and/or control.

This Policy establishes general guidelines and responsibilities to protect **Banff Centre Information**, regardless of its source, from accidental or unauthorized access, use, modification or disclosure whilst supporting the open, information-sharing needs of Banff Centre.

This Policy determines four levels of security classification that Banff Centre shall utilize to establish effective information security classification procedures as further detailed in *Procedure – Information Security - Storage and Distribution.*

SCOPE

Compliance with this Banff Centre Policy extends to all members of **Banff Centre Community** and to any other parties granted access to information, systems or facilities where Banff Centre Information is handled or stored.

Following the Effective Date, Banff Centre shall have a 24 month transition period during which time it shall update its practices and procedures so as to be fully compliant with this Policy and related Procedures by the end of the transition period.

POLICY STATEMENT

1. GENERAL

Banff Centre shall put in place such reasonable security measures as are necessary to achieve Banff Centre's commitment to the protection of privacy and compliance with Alberta's *Freedom of*

Information and Protection of Privacy Act (**FOIP**) and other relevant legislation.

2. BEST PRACTICES

The Chief Information Officer shall establish and continuously evaluate and improve Banff Centre Information security procedures, standards, and guidelines to meet or exceed established enterprise security best practices around information and data and to comply with pertinent legislation and regulations. The Chief Information Officer shall also carry out an annual review of effectiveness and make recommendations for improvement.

3. INFORMATION PROTECTION

- **a.** Each member of Banff Centre Community who enters into a formal relationship with Banff Centre must take reasonable steps to protect the confidentiality, integrity, and availability of all Banff Centre Information in their custody or under their control. Further, each member must take reasonable steps to safeguard this information against accidental or unauthorized access, use, modification or disclosure. Reasonable steps include ensuring that appropriate protective measures are in place and are carried out regarding the storage, processing, transmission, sharing, use, disclosure, and disposal of personal or other sensitive information or records.
- **b.** The Chief Information Officer will ensure regular threat and risk assessments are completed to determine potential threats to the security of Banff Centre Information, and to assess the level of risk associated with the identified threats. These assessments would include whether and how personal or sensitive information could be lost, changed, accessed, used, disclosed or be subject to improper disposal.
- **c.** The Chief Information Officer will also ensure that the safeguards outlined in the *Procedure – Information Security - Storage and Distribution* or other related procedures are applied to Banff Centre Information at the security classification level deemed necessary by the threat and risk analysis.
- **d.** The Chief Information Officer, with support from Human Resources, is responsible for ensuring that adequate information and/or training regarding this Policy and its associated Procedures is provided to all members of Banff Centre Community handling Banff Centre Information.

4. BANFF CENTRE INFORMATION – SECURITY CLASSIFICATION

- **a.** Banff Centre Information on any medium shall be assigned to one of the security classification categories noted in the table below; being public, internal, confidential, highly confidential, restricted or prohibited information.
- **b.** The *Procedure – Information Security - Storage and Distribution* shall set out the process by which any Banff Centre Information is assigned to an appropriate security classification category.
- **c.** The *Procedure – Information Security - Storage and Distribution* shall also provide direction on the storage requirements and distribution methods within and outside of Banff Centre, according to the security classification category of the relevant information.

Security Classification Categories

	Prohibited	Restricted	Highly Confidential
Definition	Information that is deemed by industry regulations, legislation or other mechanism to be prohibited.	Information that requires **specific** protection measures defined by industry regulations and standards.	Information that is so sensitive or critical that it is entitled to extraordinary protections.
Legal Requirement	Such information may not be stored or distributed by Banff Centre in any form.	Restrictions on information storage and specific protection requirements are dictated by industry regulations and standards.	Protection of information where it is required by law or regulation, or as determined by contractual obligation.
Reputational Risk	Critical loss of trust/credibility. Significant media attention.	Critical loss of trust/credibility. Significant media attention.	Critical loss of trust/credibility. Significant media attention.
Operational Risk	Risk will render the business unit unable to achieve its overall objectives or mandate.	Risk will render the business unit unable to achieve its overall objectives or mandate.	Risk will render the business unit unable to achieve its overall objectives or mandate.
Financial Risk	Major revenue loss or impact on business unit budget, including funding, fines or damage awards.	Major revenue loss or impact on business unit budget, including funding, fines or damage awards.	Major revenue loss or impact on business unit budget, including funding, fines or damage awards.
Disclosure Risk	Highly-adverse negative impact on Banff Centre, individuals or affiliates.	Highly-adverse negative impact on Banff Centre, individuals or affiliates.	Highly-adverse negative impact on Banff Centre, individuals or affiliates, including identity theft.
Examples	• Any illegal or offensive content	• Credit card information storage and distribution must follow Payment Card Industry Data Security Standard (PCI DSS)	• Legal suits and/or information that is subject to any type of legal privilege, including solicitor-client privilege • Any information protected by provincial or federal regulations, or information protected by confidentiality agreements • Closed or in-camera Board of

			Governors documents • Appeals and grievances • Criminal records checks • Health, disability or counselling information • Harassment and discrimination reports • Authentication credentials

Security Classification Categories (continued)

	Confidential	Internal	Public
Definition	Information that is considered to be highly sensitive business or **Personal Information**, or a critical system. It is intended for a very specific use and may not be disclosed except to those who have explicit authorization to review such information, even within a workgroup or department.	Information that is intended for use within Banff Centre or within a specific workgroup, department or group of individuals with a legitimate need-to-know. Internal Information is not approved for general circulation outside the workgroup or department.	Information that is public knowledge or information that has been approved for distribution to the public by the information owner or through some other valid authority such as legislation or policy.
Legal Requirement	Banff Centre has a statutory and/or contractual, legal obligation to protect the information.	Banff Centre has a contractual obligation to protect the information.	Information may be mandated by legislation (e.g., FOIP) to be public information.
Reputational Risk	Significant loss of trust/credibility. Guaranteed to generate media attention and increased scrutiny.	Potential for lost trust/credibility. May generate some media attention and result in increased scrutiny.	Some reputational risk, but can't be avoided.
Operational Risk	Significant impact on business unit's ability to achieve its objectives.	Moderately impacts business unit's ability to achieve its objectives.	Little or no impact on the business unit's ability to achieve its objectives
Financial Risk	Significant revenue loss or impact on business unit budget, including funding, fines or damage awards.	Minor negative financial impact for the business unit.	Impact is within normal operating budget margin fluctuations.
Disclosure Risk	Highly-adverse negative impact on Banff Centre, individuals or affiliates, including identity theft.	Possible adverse impact on Banff Centre, individuals or affiliates.	Disclosure of public information requires no further authorization and may be freely disseminated without potential harm to Banff Centre or its affiliates

Examples	• Third party business information or trade secrets, including commercial, financial, scientific, technical, or labour relations information, supplied explicitly or implicitly in confidence and where the disclosure would be expected to significantly harm the third party • Personal Information • All information in Personal Information Banks as listed under Banff Centre in the Alberta Directory (195) or any subsequent version of the directory • Information whose disclosure would be harmful to individual or public safety • Information whose disclosure would reveal information supplied, explicitly or implicitly, in confidence • Information whose disclosure would reveal Banff Centre confidences • Information whose disclosure would reveal advice from officials (which could include program or outcomes evaluations) • Information whose disclosures would be harmful to the economic and other interests of Banff Centre • Student data, **Banff Centre Community** information,	• Building and infrastructure plans • Banff Centre developed source code • Internal electronic mail (email) provided no Personal Information is shared • Budget information • Select department procedures • Student grades (including test scores, assignments, and class grades) provided no Personal Information is shared	• Banff Centre's public websites • Policies • Publications • Annual reports • Advertising and media releases • Product and service information • Employee directory listings • Academic calendar • Published research presentations or papers • Job postings • Training manuals • Name of degree, diploma and certificate recipients • Campus maps

	donor/alumni information and business/vendor data including: ○ Social Insurance Number ○ Personnel files ○ Personal financial information ○ Home/Personal address, phone number, cell number, email address ○ Information protected by non-disclosure agreements		

5. INFORMATION SECURITY INCIDENT

Where there is an active concern of an **Information Security Incident**, specific notification must be provided to the Chief Information Officer, VP, Administration and Chief Financial Officer and the FOIP Coordinator, and an Information Security Incident report must be completed immediately as described in the *Procedure - Information Security - Incident Response Plan*. As outlined and defined in the Procedure, all severe Information Security Incidents shall be reported immediately to the President and CEO and the Chair of Banff Centre's Board of Governors. Banff Centre shall also 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. Such measures do not constitute evidence that any individual has intentionally or accidentally lost or allowed inappropriate access to information but provide basis for an investigation to ensure information has been appropriately protected as well as inform actions to recover lost or inappropriately accessed information.

6. MANAGEMENT REPORTING

- **a.** On a quarterly basis, the Chief Information Officer shall prepare a report summarizing the following activities:
  - **i.** an update on information security measures; and
  - **ii.** details of any medium and severe Information Security Incidents as defined in the *Procedure - Information Security - Incident Response Plan*.
- **b.** The Chief Information Officer shall present this report to the VP, Administration and Chief Financial Officer for reporting to the **Senior Leadership Team** and the Board of Governors of Banff Centre through the Audit and Finance Committee (as appropriate).

7. NON-COMPLIANCE

a. When more time is needed to adopt a certain requirement of the Policy, or when it is not practical or feasible to follow the direction of the Policy, an exemption may be granted. The exemption must be approved by the VP, Administration and Chief Financial Officer, and the President and CEO. A remediation plan (as appropriate) with timeline for compliance would be included with the exemption request.

- **b.** Suspected or actual violations of this Policy may result in the VP, Administration and Chief Financial Officer and/or Chief Information Officer (as appropriate) in consultation with Human Resources, recommending or implementing corrective action, suspending, disabling, terminating, or removing access to some or all Banff Centre Information, or taking such other action (disciplinary or otherwise) up to and including termination of employment or other relationship with Banff Centre. Disciplinary action will be taken in accordance with the provisions of any applicable collective agreement or any other applicable policy or law, including Banff Centre's *Policy - Code of Ethics*.

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 Policy.
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 (paper or electronic) 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.
FOIP	Alberta's *Freedom of Information and Protection of Privacy Act*
Implementation Authority	The individual or position with responsibility for implementing this Policy.
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.
Senior Leadership Team	The President and CEO, together with the Vice Presidents of Banff Centre.
Personal Information	Recorded information about an identifiable individual, as defined in section 1(n) of FOIP.

RELEVANT 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 (in limited circumstances)

- Alberta's *Personal Information Protection Act (PIPA)* – applicable to The Banff Centre Foundation only

- **Relevant standards**
  - ISO - International Organization for Standardization
    - ISO 27002 – Information Security
  - ITIL v3 - Information Technology Infrastructure Library
    - 4.6.4.3 – Service Design: The Information Security Management System
    - 4.5 - Access Management
  - CSEC - Communications Security Establishment Canada
    - ITSG-06 – Clearing and Declassifying Electronic Data Storage Devices
  - COBIT - Control Objectives for Information and Related Technologies
    - AI3.3 - Infrastructure Maintenance
    - DS5.7 - Protection of Security Technology
    - DS11.1 - Business Requirements for Data Management
    - DS11.4 - Disposal
    - DS12.2 - Physical Security Measures
    - DS13.1 – Operations Procedures and Instructions
  - PCI Security Standards Council - Data Security Standard
    - Protect Cardholder Data
    - Implement Strong Access Control Measures
- **Relevant Banff Centre policies and procedures**
  - *Policy – Code of Ethics*
  - *Procedure – Information Security - Storage and Distribution*
  - *Procedure – Information Security - Incident Response Plan*

MODIFICATION HISTORY

- Original Approval Date: May 26, 2017
- Effective Date: June 18, 2017
- Subsequent Revision Date: May 25, 2018
- Subsequent Revision Date: March 1, 2019

CONTACT

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

- Email: cio@banffcentre.ca

Phone: Ext. 6543