

Security Policy



| | | | | |
|---|-------------------------------------|-------------------------------------|------------------------------------|-----------------|
| Section Douglas Family Art Centre | Date April 28, 2026 | By-Law Number 48-2026 | Page 1 | Of 11 |
| Subsection Security | Repeals By-Law Number N/A | | Policy Number DFAC-01-05 | |

1.0 Purpose

This Policy establishes governance, minimum controls, and operating procedures used to prevent, deter, detect, respond to, and recover from security incidents that may affect people, collections, facilities, or information at the Douglas Family Art Centre (DFAC”).

2.0 Definitions

Building Automated System (BAS) - a centralized, networked system of hardware and software that automatically monitors and controls a facility's mechanical systems. It integrates HVAC, security, and fire safety to maintain environmental conditions, reduce energy consumption, and lower operational costs.

Collection: All accessioned artworks, loans (incoming and outgoing), and items under DFAC custody.

Crime Prevention Through Environmental Design (“CPTED”): design strategies applied to reduce opportunities for crime through sight lines, lighting, and territorial cues.

Dissociation: The loss of artworks, artwork information, or the ability to reliably connect objects with their records.

Incident: Any event or near miss that threatens the safety, security, or integrity of people, collections, facilities, or information (e.g., theft attempt, vandalism, door-prop alarm, environmental alarm, data breach).

Security Policy

| | | |
|---|-------------------------|------------------------|
| Policy Number DFAC-01-05 | Page 2 | Of 11 |
|---|-------------------------|------------------------|

3.0 Scope

- 3.1 This Policy applies to the Douglas Family Art Centre (including the Annex), all staff, volunteers, contractors, and visitors, and to all collections whether on display, in storage, in work areas, or in transit. This document is to be read in concert with the DFAC Emergency & Disaster Plan. (Appendix A)
- 3.2 Security is coordinated with life safety, fire protection, environmental management, workplace health and safety, cyber security, and emergency preparedness. This is managed as a single integrated protection program.

4.0 Objectives

These are the objectives of this policy:

- A. A safe and secure environment for staff, visitors, and collections is maintained.
- B. Security incidents are detected, reported, and resolved promptly.
- C. A culture of security awareness and accountability is embedded in daily operations.
- D. Security is integrated with life-safety, emergency preparedness, occupational health and safety, and inspection/testing/maintenance (ITM).

5.0 PART I – Governance and Responsibilities

- 5.1 The Director serves as DFAC's Security Authority and is accountable for institutional security oversight and compliance. The Director integrates this Policy with the DFAC Emergency & Disaster Plan and ensures compliance with City of Kenora policies and procedures. This document has been written to avoid any conflict with City of Kenora policies.
- 5.2 Reports summarizing incidents, drills, training, tests, and improvements, will be included in the monthly Directors Report delivered at the Muse Board meeting. Interim briefings may be requested following major incidents.
- 5.3 Collections-security procedures for exhibition, storage, handling, loans, and transit are implemented by the Curator and other authorized staff members.
- 5.4 DFAC staff, volunteers, and Board Member are expected to report security concerns, risks, incidents (including near-misses) to the Director promptly.

Security Policy

| | | |
|---|-------------------------|------------------------|
| Policy Number DFAC-01-05 | Page 3 | Of 11 |
|---|-------------------------|------------------------|

5.5 DFAC staff will work with City Facilities / City IT, and contractors, to ensure the integrity and maintenance of security systems (CCTV, intrusion alarms, access control, BAS), including vendor oversight and records of inspection, testing, and maintenance.

5.6 Reports summarizing incidents, drills, training, tests, and improvements, will be included in the monthly Directors Report delivered at the Muse Board meeting. Interim briefings may be requested following major incidents.

6.0 Part II - Training and Compliance

6.1 Monthly health and safety meetings are to be attended by all staff. Meetings will include training that covers site risks, recent incidents, prevention of slips, trips, and falls, and emergency procedures.

6.2 Annual evacuation procedure drills are conducted in spring.

6.3 Training on this policy will be provided on an ongoing basis to ensure compliance.

7.0 Inspection, Testing & Maintenance (ITM)

A documented ITM program is followed:

- A. Monthly alarm signal tests and extinguisher checks are completed.
- B. Monthly sensor walk-tests are completed.
- C. Monthly panic-alarm tests are completed.
- D. Annual certifications for intrusion, fire, and CCTV systems are completed by certified contractors.
- E. Routine vendor inspection, testing, and maintenance for sprinklers, alarms, HVAC or BAS, and emergency lighting are completed.

8.0 Emergency Preparedness

8.1 A DFAC Emergency and Disaster Plan will be maintained and updated on an annual basis in January.

8.2 Staff will be trained in basic first aid and emergency response procedures outlined in the DFAC Emergency And Disaster Plan.

Security Policy

| | | |
|---|-------------------------|------------------------|
| Policy Number DFAC-01-05 | Page 4 | Of 11 |
|---|-------------------------|------------------------|

- 8.3 Physical copies of the DFAC Emergency And Disaster Plan will be kept on site in the disaster bin. Copies will also be kept off site in two locations. One copy will be kept at the City of Kenora Facilities Office, and one in a secure place at the Lake of the Woods Museum. Digital copies will also be available from any internet connected computer terminal.
- 8.4 DFAC maintains business continuity measures to support recovery and continuation of operations following a major security/emergency incident. That plan is contained in the DFAC Emergency and Disaster Plan.

10.0 Part III – Security Risk Assessment

- 10.1 Security risk assessment documents are designed to evaluate the likelihood and risk to the DFAC, and will be prepared, and included, as part of the DFAC Emergency and Disaster Plan. Security risk assessments include plausible risks to the staff, collection, facilities, or information technology of the DFAC.
- 10.2 Security risk assessments will be reviewed and updated as necessary each January during the annual renewal of the DFAC Emergency & Disaster Plan. They can also be updated or renewed before or after any major change such as construction or a high-value exhibition. The assessment covers threats, vulnerabilities, and consequences by section of the building and by priority objects.
- 10.3 Protection levels for the perimeter, public spaces, galleries, vault, and special exhibitions are established from this assessment. They also inform staffing, procedures, and technology such as secure hanging hardware or adding attendants/docents in the gallery spaces.
- 10.4 Common foreseeable security risks could include:
- A. Opportunistic theft;
 - B. Forced entry;
 - C. Vandalism;
 - D. Unauthorized photography;
 - E. Data leak; and
 - F. Insider misuse.

11.0 Part IV – Incident Management & Reporting

Immediate Actions

- 11.1 During any incident, staff safety is prioritized. When it is safe to do so the following actions are taken:
- A. Emergency services are to be called or the panic alarm is activated.
 - B. The Director or delegate is alerted;
 - C. Evidence such as CCTV exports, photographs, and witness names are preserved without compromising safety; and
 - D. A personal report of the incident is made by all involved staff as soon as possible after the event.

Reporting & Review

- 11.2 All incidents and near-misses are documented using the standard Kenora Incident Report form, and shared with city management and the City of Kenora Joint Health and Safety Committee.
- 11.3 Response and recovery are coordinated by the Director in conjunction with City Facilities/City IT, and with law enforcement if required.
- 11.4 After an incident, a post-incident review is completed by the Director. Corrective actions are assigned and are tracked to completion by the Director.
- 11.5 After any incident, staff will be offered appropriate supports.

12.0 Part V - Protecting People

Public & Personnel Safety

- 12.1 DFAC prioritizes safety of visitors, staff, volunteers, and contractors. Controls include:
- A. single entrance under constant supervision;
 - B. panic button alarms at front desk and in admin space;
 - C. CCTV coverage;
 - D. monthly health and safety inspections;
 - E. Annual City of Kenora health and safety training;
 - F. training in use of panic button and de-escalation techniques;

Security Policy

| | | |
|---|-------------------------|------------------------|
| Policy Number DFAC-01-05 | Page 6 | Of 11 |
|---|-------------------------|------------------------|

- G. training in emergency procedures and protocols;
- H. training in evacuation procedures; and
- I. first aid training.

- 12.2 Police record checks including, vulnerable sector check, are required for staff/program volunteers.
- 12.3 The DFAC staff will follow City of Kenora health and safety policies, including monthly health & safety inspections, emergency preparedness, material handling, and personal protective equipment (PPE) use.
- 12.4 DFAC will maintain a respectful and safe workplace, following both *City of Kenora Policies HR 1-4 Workplace Harassment Policy* and *HR 2-26 Community Conduct Policy*, as well as all relevant provincial legislation.
- 12.5 Any threats or incidents of violence will be addressed promptly and reported. If at any time a staff member feels threatened they should press the "panic button" or call 911.
- 12.6 In the event of a theft or public disturbance, staff will prioritize personal safety.
- 12.7 Any incident should be reported to the Director. Staff will be asked to provide a written record of their experience to include with the incident report.

13.0 Part VI - Protecting Collections & Physical Assets

Loss Prevention

- 13.1 The DFAC's collection and physical (IE its materials and equipment) will be safeguarded to prevent loss or dissociation. Procedures and preventative measures will be used to limit access and movement of such assets. Loss prevention measures apply to both external and internal risks. To achieve this, the DFAC will:
 - A. Maintain a catalogue of all fine art items in the collection as outlined in *DFAC-01-02 Collections Management Policy*;
 - B. Label all equipment (vacuums, blowers, tools etc);
 - C. Ensure that the movement or loaning of non-collection assets are tracked in the loan log book;

Security Policy

| | | |
|---|-------------------------|------------------------|
| Policy Number DFAC-01-05 | Page 7 | Of 11 |
|---|-------------------------|------------------------|

- D. Document the entry and removal of collection, and other assets, to/from building;
- E. Document the internal and external movements of all cultural property;
- F. Carry out collection inventory verifications after large exhibitions, and investigate if an artwork does not appear to be in its designated spot in the vault; and
- G. Perform inventory verifications as part of risk-based reviews.

13.2 In the event of theft, staff will immediately notify the Director, and notify the police. If there is a crime scene, it will be sealed off from the public until police arrive. While the police are working, the Director will follow up with Insurers (if necessary), the Muse Board, and the City Administration.

14.0 Contractors

Contractors must sign in/out and may be escorted in non-public areas. If staff deem necessary, contractor toolboxes and bags may be inspected before entry and exit when work occurs in or near collections areas.

15.0 Gallery & Exhibition Security

- 15.1 Food and drink in galleries are prohibited unless an exception is authorized by the Curator.
- 15.2 Backpacks or large bags/purses are prohibited in the galleries. Guests are encouraged to use the cloak room for coats.
- 15.3 Photography for personal use is permitted in the galleries. Professional photography equipment, or photography for commercial use, is generally not permitted in the galleries. Exceptions can be authorized by the Curator, on a case by case basis, for special events (weddings, political ceremonies, etc).
- 15.4 Any contractor or City staff members working in the galleries must meet with the Curator to be trained on how to move safely in sensitive spaces.
- 15.5 Some exhibitions may require gallery attendants (paid or volunteer) to monitor visitor behaviour, enforce bag policy, and report anomalies. Prior to any work, gallery attendants will be trained in DFAC emergency procedures. Gallery attendants are not permitted to physically intervene in incidents. They should report concerns to DFAC staff immediately.

16.0 Physical Safeguards in Galleries

Examples of physical safeguards used in the galleries include, but are not limited to:

- A. Security screws;
- B. Concealed hanging locks;
- C. Brackets, and/or display cases with tamper-resistant hardware;
- D. Stanchions; or
- E. Added gallery attendants as risk warrants.

17.0 Loans & Transit

Loan Conditions

17.1 Security and environmental requirements of lenders or borrowers are to be confirmed before any shipment.

17.2 Artwork condition reports will be completed by the Curator on arrival and on departure.

18.0 Packing Artwork

Loading of artwork is supervised by staff and under CCTV in the shipping and receiving area. Access to shipping and receiving area is restricted to staff.

19.0 Transport

19.1 The Curator will decide what mode of transportation is appropriate for loaned items. Transport methods are matched to object vulnerability, lender requirements, and risk assessment. Some options for shipping include:

- A. Fine Art Shipper;
- B. Personal Delivery by Curator or designate;
- C. Private courier;
- D. Canada Post (or other postal service); and
- E. Freight shipping company.

19.2 Applicable federal requirements for controlled cultural property are followed. This includes export permits under the Cultural Property Export Control List and CBSA procedures. For foreign loans in Ontario, protection under the *Foreign Cultural Objects Immunity from Seizure Act* may be sought.

Security Policy

| | | |
|---|-------------------------|------------------------|
| Policy Number DFAC-01-05 | Page 9 | Of 11 |
|---|-------------------------|------------------------|

20.0 Part VII - Protecting Facilities

- 20.1 Only the main entrance and balcony are kept unlocked during public hours.
- 20.2 The vault is kept locked at all times. Only authorized staff may enter. All visitors to the vault are to be escorted. Photography and workroom activities in the vault are prohibited.
- 20.3 CPTED measures for lighting, sight lines, and signs are applied outdoors. The perimeter is reviewed periodically with the City of Kenora s Neighbourhood Empowerment Team (NET) to reduce after-hours risks and nuisance activity around the exterior of the building.

21.0 Electronic Security Systems

Intrusion Detection, Access Control & CCTV

- 21.1 All exterior doors are equipped with contact sensors. Volumetric motion detectors are armed when the building is unoccupied. A contracted alarm call centre monitors the building at all times. Police are dispatched on alarms and the Director is notified to meet police. Motion detector walk-tests are performed as part of the monthly health and safety inspection. Annual certifications are completed by certified contractors.

22.0 Key & Fob Management

- 22.1 Access is controlled by electronic fobs that are issued to staff. Programmed schedules define auto-lock/unlock, with the default being locked. Electronic fobs issuance, access zones control, and returns are logged and maintained by City of Kenora IT staff.
- 22.2 A key fob register with holder, areas, issue/return dates, and authorization is maintained by City of Kenora IT staff.
- 22.3 Key fobs are deactivated when lost, or with a role change/termination. Staff will contact the Director and report the loss as soon as the loss is realized. The Director will follow up with IT.
- 22.4 DFAC spare keys are to be kept in a separate, locked key cabinet with controlled access for staff.

Security Policy

| | | |
|---|--------------------------|------------------------|
| Policy Number DFAC-01-05 | Page 10 | Of 11 |
|---|--------------------------|------------------------|

23.0 Closed-Circuit Television (CCTV)

- 23.1 Continuous recording via CCTV is maintained at entrances, galleries, circulation areas, stairs, administrative areas, and exterior approaches.
- 23.2 The DFAC will abide by *City of Kenora Policy AF-1-3 - Video Surveillance Policy*. In addition:
- A. The array of security cameras in the DFAC will be maintained by a third party security contracting company;
 - B. Signs are installed to notify the public of video surveillance activity;
 - C. Staff will monitor visitor behaviour in real time during open hours;
 - D. Footage is retained for a period of at least 30 days and not more than 90 days;
 - E. Staff will cooperate with law enforcement when asked for security camera footage of building and grounds;
 - F. CCTV cameras are not to be used as a primary tool for staff/personnel surveillance; and
 - G. Under no circumstances is CCTV footage to be made public.

24.0 Fire Protection

The DFAC will maintain the following fire protection measures:

- A. wet-pipe sprinklers;
- B. fire alarm pulls;
- C. zoned water shut-offs;
- D. annual maintenance and inspection by qualified contractors;
- E. Monthly extinguisher checks as part of the monthly health and safety inspection;
- F. staff trained on basic fire response, evacuation; and
- G. sprinkler isolation.

25.0 Part VIII - Protecting Information

Security Records & Privacy

- 25.1 Security records that include incidents, access logs, inspection or testing or maintenance reports, and CCTV exports are treated as confidential. CCTV is operated under the *City of Kenora Policy AF-1-3 - Video Surveillance* and the *Municipal Freedom of Information and Protection of Privacy Act*.
- 25.2 Staff passwords and access controls are to be used to protect personal work stations, network access, and any digital records.

Security Policy

| | | |
|---|--------------------------|------------------------|
| Policy Number DFAC-01-05 | Page 11 | Of 11 |
|---|--------------------------|------------------------|

- 25.3 Paper copies of staff passwords are kept in a secure location on site.
- 25.4 Where recommended by City IT, staff will use two-factor authentication.
- 25.5 Weekly backups are to be maintained and stored via a cloud based solution off site.
- 25.6 Staff will abide by City of Kenora *HR- 2-06 Technology Usage Policy*, and work with City of Kenora IT staff and contractors to prevent phishing attempts, malware, and other IT related issues, including annual training.
- 25.7 In collaboration with City IT, security and BAS networks are segmented. Strong authentication including multi-factor authentication for remote access is enforced. Vendor credentials are controlled and logs are available for review.

26.0 Part IX - Renewal

This Policy is reviewed by staff annually in January and after any significant incident, in parallel with the Emergency & Disaster Plan s annual refresh cycle. Updates are to be submitted to the Muse Board for approval and communicated to all personnel.

This policy will be reviewed by the Muse Board at least every three years.