Essential Cybersecurity for Arts Organizations
2026 Guidelines

Essential Cybersecurity for Arts Organizations is a collaboration between the Rozsa Foundation, Calgary Arts Development, Calgary Foundation, and Technology Helps.

Contents

ABOUT THE PROGRAM

Arts organizations across Canada are increasingly reliant on digital tools, including online ticketing, donor databases, collaboration platforms, and other systems essential to daily operations. However, this digital shift also exposes them to growing cybersecurity risks.

Recent incidents affecting arts organizations and non-profits nationwide have highlighted vulnerabilities related to phishing, data theft, and other cyberattacks. These events underscore the urgent need for proactive cybersecurity measures, but many arts organizations are facing ongoing resource constraints that make it difficult to invest in system assessments and protective technologies.

To help address these challenges, the Rozsa Foundation, Calgary Arts Development, and Calgary Foundation have partnered with Technology Helps, a Calgary-based non-profit to offer access to EverSecure, a cybersecurity program designed specifically for nonprofits, to up to 25 arts organizations in Southern Alberta.

EverSecure is both technical and strategic, combining everything from antivirus software and firewalls to incident response plans, controls, training and policies. It integrates deeply with existing business tools, IT, HR, legal operations, and organizational culture to create and foster a secure

environment. This integrated model helps reduce the risk of business interruption, data compromise, and financial loss.

Arts organizations in Treaty 7 ready to enhance their cybersecurity are encouraged to apply and take the next step toward digital resilience.

WHAT RECIPIENTS WILL RECEIVE

There is no direct financial contribution made to arts organizations through this program. Instead, recipient organizations will be enrolled in Technology Helps' EverSecure cybersecurity program at no charge for a period of one year. This access would typically cost upwards of $5,000.

EverSecure encompasses the following:

1. Full Cybersecurity Assessment
Technology Helps will conduct a thorough evaluation of each recipient organization's digital environment, including email systems, ticketing platforms, CRM tools, financial systems, and third-party services. The assessment will:

- Identify vulnerabilities and configuration gaps
- Map critical assets and third-party dependencies
- Provide a prioritized, actionable remediation plan tailored to each organization's size, mission, and capacity

This assessment is essential, as third-party tools are increasingly leveraged by attackers to launch phishing campaigns and compromise sensitive data.

2. One Year Enrollment in EverSecure
Following the assessment, organizations will receive 12 months of full EverSecure service, including:

- **Protective security technologies:** Deployment of secure email filtering, multifactor authentication, endpoint protection, identity safeguards, and validated backups.
- **Continuous monitoring and expert response:** Realtime, 24/7 threat detection, alerting, and professional triage to reduce the time between detection and resolution, minimizing downtime and reputational impact.
- **Human-centred defence:** Ongoing staff training on digital hygiene, password security, MFA, safe file handling, and incident reporting, supported by routine phishing simulations to reinforce learning and strengthen awareness.

There is no requirement to continue with the EverSecure program beyond the one-year period of support. Implemented protections and safeguards will remain in place and policies will remain available, leaving a legacy of strengthened diligence towards cybersecurity. Ongoing training and monitoring beyond the first year will require the organization to contract Technology Helps separately.

PROGRAM BENEFITS

Participating organizations will gain:

- **Operational resilience**, ensuring ticketing and program delivery continue uninterrupted.
- **Protection of patron trust and donor confidence** through secure handling of personal information.
- **Cost avoidance and reputational protection** via fewer disruptions and faster incident response.
- **Improved cybersecurity maturity**, giving boards and leaders confidence in their digital infrastructure.

Strengthening digital defenses helps arts organizations safeguard their essential role in the community, keeping theatres, galleries, and cultural spaces running smoothly and securely. Selected organizations will participate in regular progress reviews with Technology Helps to ensure adoption of controls, staff engagement in training, and measurable improvements in cyber resilience.

The Rozsa Foundation, Calgary Arts Development, and Calgary Foundation are committed to strengthening Southern Alberta's arts sector in the digital age. By providing access to EverSecure, we aim to raise cybersecurity standards across the region and empower arts organizations to pursue their missions with confidence.

2026 DEADLINES

There is no specific deadline for the Essential Cybersecurity for Arts Organizations program. Applications will be accepted and assessed throughout 2026 until the program is full.

We encourage you to submit your application as soon as you are able.

Decisions are typically made within 3-weeks of when you apply.

WHO CAN APPLY?

This program is open to arts organizations committed to improving their cybersecurity practices.

Your organization may be eligible to apply if you meet all the following criteria:
- Your organization is a **registered Canadian charity** with a valid CRA charitable business number (9 digits, 2 letters, 4 digits) OR **registered not-for profit** organization, and
- Your organization is **arts-focused and presents arts-based work for a public audience**, and
- Your organization is **operating in the Treaty 7 region of Southern Alberta**, encompassing Calgary and the surrounding area, as well as Banff, Canmore, Drumheller, Medicine Hat, Lethbridge, Red Deer, and others, and
- Your organization has an **annual operating budget of at least $250,000**, and
- Your organization has a **minimum of two professional staff (full or part-time)**, and
- You **commit to designating a staff member as Project Lead** to liaise with Technology Helps, and

- You will **commit 10–15 hours of the Project Lead's time** for meetings, information gathering, and implementation tasks, and
- You **commit to ensuring that all staff, and other organizational members with access to digital systems, complete quarterly cybersecurity training** (approximately one hour per quarter).

Applicants will be evaluated based on:
- Demonstrated need and readiness to implement recommended security measures, and
- Capacity and commitment to collaborate with Technology Helps and ensure the implementation of security measures and completion of staff training.

Not sure about your eligibility? Contact Simon Mallett at simon@rozsafoundation.com.

HOW TO APPLY

Please read through these program guidelines to get an initial understanding of the program and what is required of your organization if approved. Complete your application via our online application form here: https://rozsafoundation.formstack.com/forms/cybersecurity_application

Application Templates

If you would like to prepare your application offline, please download the application template available on the program webpage (https://www.rozsafoundation.com/cybersecurity).

You are welcome to complete your application writing in this template and then copy/paste your answers into the online form. All applications must be made via the online form, unless an alternate application process was determined in collaboration with the Rozsa Foundation.

NOTIFICATION OF RESULTS

After submitting your application or making a presentation your application will be reviewed by representatives of the collaborating organizations. We will reach out to you if the committee has additional questions, or if they require additional information or clarification to make a decision.

All applicants, regardless of funding outcome, will be notified about the committee's funding decision by email.

We aim to send notification of results within three weeks of the application deadline.

CONTACT US

If you are curious about your organization eligibility for this program, or if you have questions about the application, submission process or expectations of participation if approved, please contact the Rozsa Foundation's Executive Director, Simon Mallett at simon@rozsafoundation.com.

APPLICATION CHECKLIST

Organization Name
Organization Mailing Address
Organization Phone Number
Organization Website (if applicable)
Organization Mandate or Statement of Purpose
Organizational Structure: Registered Charity or Registered Non-Profit

Charitable Registration Number (for Registered Charities only)
Non-Profit Registration Number (for Registered Non-Profits only)

Artistic Discipline: *requested for internal statistical reporting*.
Annual operating budget: *annual operating budget of at least $250,000 to be eligible*
Number of Full Time and Part Time Staff
Year Organization was founded

Primary Applicant Contact Information: *main contact for managing this application*.
Board Chair Contact Information

Current State and Vulnerabilities: Tell us about the technology systems you are currently using at your organization, including any digital protections your organization has in place. Where do you see vulnerabilities in your current systems and processes?

Total Number EverSecure Participants: Approximately, what is the total number of staff members and others (contractors, board members, etc) in your organization who have access to digital systems (email access, file sharing, accounting systems, etc) who will be required to participate in EverSecure?

Project Lead Contact Information
Note: Organizations must commit to designating a staff member as Project Lead to liaise with Technology Helps. We estimate this commitment to be 10–15 hours of the Project Lead's time for meetings, information gathering, and implementation of tasks.

If approved, we commit to providing the necessary Project Lead staff time to work with TechHelps to complete the implementation of EverSecure at our organization. YES or NO

If approved, we will commit the time necessary for ongoing staff training and to ensure it is completed by all staff, and others who have access to our digital systems (contractors, board members, etc). *Approximately 1 hour per person per quarter*. YES or NO

If approved, we commit to implementing the recommendations received through EverSecure wherever possible/feasible. YES or NO

Additional Comments (optional): Please share anything else you think we should know.

Most Recent Financial Statements: Please upload a PDF copy of your organization's most recent audited financial statements to the online form. Files must be 2MB or smaller. PDF files only.