Alberta Security Infrastructure Program (ASIP)

Program Guidelines

Alberta

Contents

1. PROGRAM PURPOSE AND OBJECTIVES 1

2. PROGRAM OVERVIEW 1

3. DEFINITIONS OF HATE CRIME AND INCIDENTS 2

4. DEFINITION OF SECURITY RISK ASSESSMENT 2

5. SECURITY RISK MANAGEMENT PLAN 2

6. ELIGIBILITY CRITERIA 2

7. PROGRAM ELIGIBILITY TIMEFRAME 4

8. FUNDING CATEGOIRES (A, B1, B2 AND C) 4

9. CONFLICT OF INTEREST 8

10. FINANCIAL REPORTING REQUIREMENTS 9

11. APPLICATION PROCEDURES 10

12. FUNDING CONDITIONS 10

13. AUDIT 11

14. NOTIFICATION 11

15. *PROTECTION OF PRIVACY ACT (POPA) & ACCESS TO INFORMATION ACT (AITA)* 11

16. OFFICE CONTACT INFORMATION 11

17. FREQUENTLY ASKED QUESTIONS 12

APPENDIX A: SECURITY RISK ASSESSMENT 13

APPENDIX B: SECURITY RISK MANAGEMENT PLAN 14

APPENDIX C: PUBLICLY FUNDED INSTITUTION 15

ALBERTA SECURITY INFRASTRUCTURE PROGRAM

1. PROGRAM PURPOSE AND OBJECTIVES

The Alberta Security Infrastructure Program (ASIP) grant provides funding for security assessments, security infrastructure upgrades, training and immediate security response to not-for-profits serving identifiable groups at risk of hate or bias-motivated crimes or incidents.

2. PROGRAM OVERVIEW

2.1 The ASIP has two funding streams: **Cost Recovery Stream** and **Regular Grant Stream.**

2.2 ASIP Cost Recovery Grant Program

ASIP COST RECOVERY GRANT				
Category:	**A**	**B1**	**B2**	**C**
Overview:	Professional Security Risk Assessment	Implementing Security Risk Assessment	Education and Training	Immediate Security Response
Funding limit	$10,000 maximum	$25,000 maximum	$10,000 maximum	$10,000 maximum (per application)
Reimbursement timeframe	Cost must have been incurred after June 1, 2021.			
Grant agreement	Embedded in application			
Required documentation	• Copy of Security Risk Assessment • Receipts/paid invoices	• Copy of Security Risk Assessment • Receipts/paid invoices related to security equipment and infrastructure	• Receipts/paid invoices related to training	• Police report; or police file number; or letter of support from police member • Receipt/invoices

2.3 ASIP Regular Grant Stream Program

ASIP REGULAR GRANT STREAM PROGRAM			
Category:	**A**	**B1**	**B2**
Overview:	Professional Security Risk Assessment	Implementing Security Risk Assessment	Education and Training
Funding limit	$10,000 maximum	$25,000 maximum	$10,000 maximum
Project completion	12 months		
Grant agreement	Embedded in application		
Required documentation	• Quote(s)	• Copy of Security Risk Assessment • Minimum two (2) quotes for security equipment and infrastructure	• Quote(s) related to training
Final reporting	• Final report • Copies of receipts/invoices • Actual expense spreadsheet		

3. DEFINITIONS OF HATE CRIME AND INCIDENTS

3.1 Hate Crime and Hate Incidents

For the purpose of the ASIP grant, the following guiding definitions of hate crimes and hate incidents will be considered:

Hatred	A sentiment of intense animosity or hostility that, if exercised against members of an identifiable group, implies that those individuals are to be despised, scorned, denied respect and made subject to ill-treatment on the basis of group affiliation.
Bias	An inclination of temperament or outlook, especially a personal and sometimes unreasoned judgment.
Prejudice	An antipathy (or enmity) based upon a faulty and inflexible generalization. It may be felt or expressed. It may be directed toward a group as a whole or toward an individual because they are a member of that group.
Hate/bias motivated crime	An criminal offence committed against a person or property that is perceived to be motivated and/or is motivated in whole or in part by the suspect's hate, bias or prejudice based on the victim's real or perceived ancestry, race, national or ethnic origin, language, colour, religion/creed, sex, age, mental or physical disability, gender identity, sexual orientation or any other similar factor.
Hate/bias motivated incident	An incident involving behaviours that are perceived to be motivated and/or are motivated by hate, bias or prejudice against a victim's real or perceived ancestry, race, national or ethnic origin, language, colour, religion/creed, sex, age, mental or physical disability, gender identity or sexual orientation and are not criminal acts.

4. DEFINITION OF SECURITY RISK ASSESSMENT

A security risk assessment is the activity of assessing and reporting security risks for physical infrastructure to help make well-informed, risk-based decisions. A security risk assessment also recommends remedies for identified security issues.

See **Appendix A** for more details.

5. SECURITY RISK MANAGEMENT PLAN

Security planning considers how security risk management practices are designed, implemented, monitored, reviewed and continually improved.

See **Appendix B** for more details.

6. ELIGIBILITY CRITERIA

6.1 Eligible applicants

To be eligible for grant funding, organizations must:

- Be physically located in Alberta;
- Be a registered non-profit or charitable organization in good standing with the Government of Alberta; and
- Serve one or more members of an identifiable group at risk of hate or bias-motivated activity because of their real or perceived:
    - ancestry,

- sex,
- race,
- nationality,
- ethnicity,
- language,
- colour,
- religion/creed,
- age,
- mental disability,
- physical disability,
- gender identity,
- sexual orientation, or
- other similar factors.

Examples of potential eligible organizations include:

- Places of worship such as a temple, mosque, synagogue, Gurdwara or church, where a group of people can gather to perform acts of religious praise, meditation, honour or devotion;
- Independent educational institutions accredited by the Alberta Ministry of Education, including primary and secondary schools serving diverse student bodies;
- Community centers, such as a community drop-in center or Indigenous Friendship Centre, where members of any identifiable group gather for social or cultural activities;
- Cemeteries or burial facilities with a primary focus on members of an identifiable group;
- Shelters serving individuals of an identifiable group;
- Ceremonial facilities or monuments used by individuals of an identifiable group; and/or
- Store front organizations serving identifiable groups.

6.2 Ineligible applicants

- private residential dwellings
- daycares
- for-profit organizations
- municipalities
- police services
- crown corporations
- public agencies, boards and commissions, including their operations
- publicly funded institutions
- individuals
- property still under construction/development

6.3 ASIP funding received in 2021 or 2022

ASIP funding received in 2021 or 2022 will be counted against ASIP's current funding maximums based on what the 2021 or 2022 funding was used for (e.g., $10,000 received in 2021 for the installation of cameras will be counted against what is currently Category B1 funding).

7. PROGRAM ELIGIBILITY TIMEFRAME

7.1 Organizations can apply to one or both funding streams available.

7.2 Application eligibility timeframe

	Cost Recovery Grant Stream	Regular Grant Stream
Eligible timeframe	June 1, 2021 onward	N/A

7.3 The ASIP program will remain open dependent on availability of funds. Notice of program closure will be posted on the Alberta government ASIP website at https://www.alberta.ca/alberta-security-infrastructure-program- grant.aspx.

NOTE: Due to a predetermined program budget, not all requests that meet the established criteria will be approved and/or guaranteed for funding or reimbursement.

8. FUNDING CATEGORIES (A, B1, B2 AND C)

8.1 Applicants may apply for funding under one or more of funding categories.

8.2 If applying to more than one funding category, the application will be assessed based on the criteria of each category. Therefore, funding may be approved wholly, in part, or not at all.

8.3 Please review the conditions of funding and eligible expenses carefully for each funding category as they vary between categories.

8.4 Category A: Security Risk Assessment

8.4.1 Funding or cost reimbursement for a completed Professional Security Risk Assessment (example: Crime Prevention Through Environmental Design (CPTED))

8.4.2 Funding maximum: up to $10,000 per organization

8.4.3 Security Risk Assessments that qualify for reimbursement include:

- Security Risk Assessments conducted by a qualified service provider in accordance with the SAFE Design Standard.
- CPTED assessments conducted by an accredited service provider in accordance with ISO 22341 guidelines.
- Security Risk Assessments conducted by a qualified service provider in accordance with ISO 31000 Risk Management Guidelines.

8.4.4 For this program, a qualified service provider is defined as a registered corporate entity providing security services under direct supervision of an individual holding verifiable credentials as a security professional. Acceptable professional credentials include:

- Current ASIS International designation as a Certified Protection Professional (CPP).
- Current ASIS International designation as a Physical Security Professional (PSP).
- Current National Institute of Crime Prevention's Crime Prevention Through Environmental Design Professional Designation (CPD).
- Current International Crime Prevention Through Environmental Design Association designation as an International CPTED Certification Program (ICCP) Certified CPTED Practitioner (ICCP-Practitioner).

- Current International CPTED;
- association as an ICCP Certified CPTED Professional (ICCP-Professional); and
- recognition as a subject matter expert in security risk assessment competencies based on demonstrated education, training and/or experience, including:
    - a minimum of five (5) years experience as a sworn police officer in combination with training certificate(s) in conduct of security risk assessments;
    - a graduate level degree (master's degree or PhD) in security and risk management in combination with a minimum of five (5) years experience in conducting security risk assessments; or
    - qualification, from a court of law, as an expert on matters relating to crime prevention and crime reduction.

8.4.5 Conditions of funding:

- The Security Risk Assessment must be for physical facilities belonging to or primarily used by the applicant organization.
- The Security Risk Assessment must be conducted by an accredited/certified service provider.
- Other security assessments must meet the described minimum standards above.
- Infrastructure being assessed must be located in Alberta.
- There must not be any real or perceived conflict of interest regarding the individual or company providing the security assessment (refer to Section 9).
- A copy of the quotes or receipt/paid invoice for the Security Risk Assessment, as well as a copy of the assessment (if applicable) must be provided.

NOTE: The request total must be equal to, or less than, the value of the receipts provided. If the request cannot be validated, the grant application will be declined.

NOTE: The Alberta Security Infrastructure Program (ASIP) funds professional security risk assessments for physical infrastructure only. Cyber security risk assessments are not eligible for funding. Cyber security awareness training may be supported under Category B2: Education and Training, up to $10,000 per organization.

To access additional resources related to cyber security awareness, including baseline cyber security controls and free eLearning resources for small and medium organizations, please visit the Canadian Centre for Cyber Security: https://www.cyber.gc.ca/en/small-medium-businesses

8.4.6 General resources for identifying qualified service providers:

- Edmonton Police Service CPTED information
- Calgary Police Service CPTED information
- Alberta Provincial Rural Crime Watch Association CPTED information
- Canadian Security Association (CANASA)
- ASIS Calgary / Southern Alberta Chapter 162
- ASIS Chapter 156 Edmonton/Northern Alberta

8.5 Category B1: Implementation of Security Risk Assessment Plan

8.5.1 Cost reimbursement or advance funding request to implement mitigation/countermeasures identified through the Professional Security Risk Assessment (example: CPTED)

8.5.2 Funding maximum: up to $25,000 per organization

8.5.3 Security planning, infrastructure and equipment purchases ($25,000 max. per organization)

Eligible mitigation measures and/or countermeasures include:

- Contract expenses relating to the implementation of Security Risk Assessment recommendations, such as:
    - the development of a facility security risk management plan; or
    - the development of facility security policies and procedures.
- Security equipment and security related infrastructure and changes articulated within the facility security risk management plan:
    - purchase, installation and/or upgrade of security equipment (examples: cameras, gate, etc.)

8.5.4 Conditions of funding:

- A security risk assessment must be conducted and dated prior to the purchase/installation of equipment.
- A copy of the security risk assessment must be submitted with the application.
- Rationale and security objectives for all equipment must be identified within a security risk management plan.
- There must not be any real or perceived conflict of interest regarding the individual or company providing the security risk assessment (refer to section 9).
- Quotes or receipts/invoices for equipment and installation must be dated at the same time or after the security risk assessment.
- Consent from the facility/site owner must be obtained if the applicant does not own the facility/site.

NOTE: the request total must be equal to, or less than, the value of the receipts/paid invoices provided. If the request cannot be validated the grant application will be declined.

8.6 Category B2: Education and Training

8.6.1 Education and training expenses relating to security risk management and community resilience for the purpose of preventing or responding to hate or bias motivated crime or incidents:

- Tuition expenses relating to skills development for current organization staff or regular volunteers members, such as:
    - Alberta basic security guard training course;
    - first aid training courses;
    - mental health awareness and de-escalation courses;
    - conflict avoidance and violence prevention courses; and
    - Incident Command System (ICS) courses.
- Cyber security awareness training, such as:
    - passwords and login safety;
    - safe browsing habits;
    - protecting devices;
    - data protection;
    - how to report security concerns/incidents;
    - phishing scams;
    - safe social media practices;
    - public Wi-Fi risks; and

    - cyber-bullying/online harassment awareness.
- Tuition, venue and/or contract expenses relating to education initiatives for community members, such as:
    - upstander training; legal awareness (a.k.a. know your rights training);
    - hate crime awareness seminars/information workshops;
    - victim services seminars/information workshops; and
    - newcomer/refugee integration workshops.
- Expenses relating to translation and production of security-related awareness and education materials for community members.

8.6.2 Conditions of funding:

- Rationale and objectives for all training must be identified.
- There must not be any real or perceived conflict of interest regarding the individual or company providing the security assessment (refer to section 9).
- Two quotes or receipts/paid invoices.

NOTE: The request total must be equal to, or less than, the value of the receipts/paid invoices provided. If the request cannot be validated the grant application will be declined.

8.7 Category C: Immediate Security Response

8.7.1 Cost reimbursement for immediate short-term security response needs related to a high-risk (potentially violent) hate or bias motivated incident that was reported to police, or perceived threat thereof.

8.7.2 Funding maximum: up to $10,000 per application.

8.7.3 Eligible expenses include:

- security personnel for 30 days or less;
- immediate repairs (directly related to an incident) to the facility to prevent access or to address a concern that could cause further trauma (examples: lock replacement, door repair, etc.); and
- graffiti removal.

8.7.4 Conditions of funding:

- A police report OR police file number OR letter(s) of support from a police service member.
- Proof of payment (receipts/paid invoices) for equipment, repairs, services, etc., must be provided at the time of application.
- Expenses that have already been covered by insurance are not eligible for reimbursement.
- There must not be any real or perceived conflict of interest regarding the individual or company providing the security assessment (refer to section 9).

NOTE: The request total must be equal to, or less than, the value of the receipts provided. If the request cannot be validated the grant application will be declined.

8.8 Ineligible expenses (all categories: A, B and C)

8.8.1 Ineligible expenses include, but are not limited to the following:

- cyber security assessments;
- cyber security implementation beyond awareness training;
- costs incurred prior to the eligibility timeframe (prior to June 1, 2021);

- capital costs that include land or vehicle purchases and the construction of buildings;
- salaries/wages for applicant organization staff;
- permanent or long-term (over 30 days) security staff (security guards, etc.);
- legal costs;
- insurance costs (premiums, deductibles, etc.);
- unrelated debt repayment;
- ongoing subscription or service fees (example: monthly alarm service/monitoring fees);
- time and labour provided towards preparation of funding applications;
- financing charges and interest payments on loans;
- costs covered under an insurance policy;
- costs for electrical upgrades or general facility upgrades;
- security service worker licencing fees;
- internet service fees;
- security professional certification program fees (i.e., CPP, PCI, PSP, APP, CPD, ICCP-Practitioner, ICCP-Professional); and
- post-secondary education tuition for diploma, certification or academic degree programs.

NOTE: this grant program will not provide reimbursement in cases where expenses have been paid for by another entity other than the organization making the application

9. CONFLICT OF INTEREST

9.1 In addition to complying with the ASIP guidelines and the terms in the grant application, an individual affiliated with an ASIP grant application or recipient(s) should not place themselves in an apparent or actual conflict of interest related to the grant funds.

9.2 A conflict of interest arises when a conflict between an individual's personal interests (what they could gain financially or otherwise) and their duty to apply for or administer the grant funds in an accountable and transparent manner are in question.

9.3 A conflict of interest may be actual or perceived. Actual conflict exists where an individual's personal interests could improperly influence the recipient's duty to utilize the grant funds in a responsible and accountable manner. For example, an individual employed by the recipient wants to use the grant funds to rent space from a private company owned by the individual. An actual conflict of interest exists because the individual personally benefits from this decision.

9.4 Perceived conflict of interest exists when there is the appearance that an individual has a private interest that could improperly influence the individual's duty to act in the best interests of the grant recipient.

9.5 Whether a conflict of interest is categorized as actual or perceived, the individuals affiliated with the grant recipient should avoid placing themselves in a situation where their personal interest could interfere with their duty to be transparent and accountable with the use of the grant funds. For example, the individual should ensure that their family members or the businesses they have an interest in have no involvement with the project and in no way personally benefit from the Government of Alberta funding that was provided.

9.6 As soon as reasonably possible after becoming aware of a personal interest that causes or is likely to cause a conflict of interest in relation to a grant application, the grant applicant or recipient must give notice of the conflict to the Ministry of Alberta Public Safety and Emergency Services' Community Initiatives Support staff by contacting them via asip@gov.ab.ca. After giving notice of a conflict, the grant applicant may not

commence nor continue until instructed to do so by the Community Initiatives Support staff and may not be allowed to proceed.

9.7 There must not be any real or perceived conflict of interest regarding the individual or company who has conducted or provided a security risk assessment for the applicant organization.

10. FINANCIAL REPORTING REQUIREMENTS

10.1 ASIP Cost Recovery Stream

10.1.1 In order to be considered for reimbursement under any of the funding categories, you must provide proof of payment for goods and/or services at the time of application.

10.1.2 Proof of payment (receipts/paid invoices): Itemized receipts and/or invoices related to the funding request must be submitted with the grant application.

10.1.3 An Itemized Expenses/Budget Template must be submitted with the grant application.

10.1.4 All expenses that are included in the funding request for reimbursement should be listed individually with the associated dollar value.

10.1.5 The total amount indicated in the Itemized Expenses/Budget Template should match the funding request.

10.1.6 The funding request and Itemized Expenses/Budget Template can be used to validate receipts/invoices submitted with the grant application.

10.1.7 The **Itemized Expenses/Budget Template** will be included as Appendix A of the grant agreement.

10.2 ASIP Regular Grant Stream

10.2.1 In order to be considered for funding under any of the funding categories, you must provide valid quotes that are valid at the time of submission.

10.2.2 An Itemized Expenses/Budget Template must be submitted with the grant application.

10.2.3 All requested expenses should be listed individually with the associated dollar value.

10.2.4 The total amount indicated in the Itemized Expenses/Budget Template should match the funding request.

10.2.5 Grant recipients must complete their financial accounting for the project using the **Itemized Expenses/Budget Template** and include receipts/invoices that support the expenditures.

10.2.6 The final reporting must be properly completed and signed by an authorized representative having legal and/or financial signing authority for the organization. The final report must include all supporting documentation (i.e. receipts/invoices).

10.2.7 Expenses not able to be validated by proper documentation will be considered ineligible and funds must be returned.

10.2.8 Any recipient that does not comply with the reporting requirements may be ineligible to receive additional funding from other Alberta Public Safety and Emergency Services grant programs until acceptable reporting is provided.

IMPORTANT NOTE: The requested amount in each category, and the total request, should be equal to or less than the cost to the organization as indicated by the documentation. If the request total is not equal to, or less than, the value of the receipts or quote provided, the grant application will be declined.

11. APPLICATION PROCEDURES

11.1 Each funding category has specific criteria including documents that must be submitted at the time of application, for example, itemized receipts or Security Risk Assessment, etc.

11.2 Applicants should ensure they are applying to the funding category or categories that best suit their need. Applicants are encouraged to contact the Community Initiatives Supports (CIS) program office for assistance with completing the application.

11.3 In order to process applications, the information requested from applicants needs to be fully completed and all questions on the forms must be answered. Applications that are incomplete and/or are submitted without the required documentation will not be considered.

11.4 Check boxes are included on the application to ensure the application is complete and all supporting documentation and mandatory attachments are included. Applicants should be sure to submit all required and supporting documents when applying.

11.5 Organizations can submit their application package by email: asip@gov.ab.ca.

12. FUNDING CONDITIONS

Applicants that are successful in receiving grant funding must be aware of and observe the following funding conditions:

12.1 After the review, approval and payment of a grant relative to an application to the ASIP Cost Recovery Grant and/or the ASIP Regular Grant, the applicant is bound by the terms and conditions of the grant agreement that forms part of the Cost Recovery Grant and/or the ASIP Regular Grant application.

12.2 Grant funds must be spent according to approved eligible costs as outlined in the ASIP Guidelines and determined by Alberta Public Safety and Emergency Services/CIS staff.

12.3 Grant funding not used or accounted for in accordance with the approved eligible costs shall be repayable by the grant recipient to the Government of Alberta. CIS staff should be contacted for instructions.

12.4 If the expenses approved in the original application change or the applicant wishes to change the scope of the project, a written request must be made to CIS staff requesting approval. Expenses must fall within the mandate and intention of the ASIP grant program.

12.5 Financial reporting must be completed and submitted to ASIP CIS staff within the following timeframes:

- ASIP Cost Recovery Grant: at the time of application.

- ASIP Regular Grant: within 30 days of term end date.

NOTE: The ASIP Regular Grant Stream term ends 12 months following payment.

13. AUDIT

13.1 Your organization may be randomly selected for audit related to your application. By participating in the ASIP program, you are agreeing to provide the requested material, such as receipts, documents, etc. in order to allow for a fair adjudication of your grant application in accordance with the Conditional Grant Agreement embedded in section 1 of the grant application.

14. NOTIFICATION

14.1 Applicants will receive written notification/email of the decision regarding their application.

14.2 All decisions on grant applications are final, and no appeals will be considered.

15. *PROTECTION OF PRIVACY ACT (POPA) & ACCESS TO INFORMATION ACT (AITA)*

15.1 The personal information that is provided on the grant application form will be used for the purpose of administering ASIP and advising the applicant of grant program updates and relevant ministry initiatives. This collection is authorized by section 4(c) of the *POPA* and is protected by the privacy provisions of *POPA*.

15.2 The *Access to Information Act* (*ATIA)* applies to any information that is provided to Alberta Justice/Public Safety and Emergency Services. This information may be disclosed in response to an access request under the *ATIA*, subject to any applicable exceptions to disclosure under the *ATIA*.

15.3 Please note, once an application has been approved and funding issued to an organization, the community/city, grant recipient, project, amount funded and fiscal year become a matter of public record.

15.4 Occasionally, Alberta Public Safety and Emergency Services may contact applicant organizations to provide information about ministry initiatives or announcements related to the following topics:

- grant program changes, funding announcements and opportunities to provide input/opinion on programs; and
- awareness of Ministry resources or events available to organizations.

15.5 Only authorized contact representatives noted in the grant application may request specific information about grant applicants from the CIS office.

15.6 For questions about the collection and use of this information, please contact the CIS staff at asip@gov.ab.ca.

16. OFFICE CONTACT INFORMATION

Email: asip@gov.ab.ca

Main line: 780-415-1819

Toll-free: 780-310-0000 (780-415-1819)

Website: https://www.alberta.ca/alberta-security-infrastructure-program-grant.aspx

17. FREQUENTLY ASKED QUESTIONS

Question	Answer
Can my organization apply to both the ASIP Cost Recovery Program and the ASIP Regular Grant Program at the same time?	Yes, if you meet the requirements outlined in the ASIP Program Guidelines, you can apply to both programs at the same time.
We would like to apply for both the Cost Recovery Grant and the Regular Grant. Do I need to fill out both applications?	Yes. When applying for both grants, you must complete both a Cost Recovery Grant application and a Regular Grant application.
My organization paid for a security risk assessment on their own and now we are ready to implement the recommendations. Which grant should we apply for?	If you have not previously received grant funding for the security risk assessment, you may apply for reimbursement under the ASIP Cost Recovery Grant. To apply for funding to implement the security measures (i.e. purchase/install equipment), you may apply under the ASIP Regular Grant.
Our quote is six months old. Do I need to get a new one?	Quotes are only valid for the period of time indicated on the quote (example: 90 days). If your quote is invalid at the time of application, please get a new quote as part of your submission. Invalid or stale dated quotes may impact the outcome of your application.
We received an ASIP Regular Grant. Can we purchase different equipment than what was included in our application?	Expenses must fall within the mandate and intention of the ASIP grant program. If the expenses approved in the original application change or the applicant wishes to change the scope of the project, a written request must be made to CIS staff requesting approval.
Does the Alberta Security Infrastructure Program fund cyber security risk assessments?	No, the program only funds professional security risk assessments for physical infrastructure. Cyber security risk assessments are not eligible for funding. However, funding may be available for cyber security awareness training under Category B2: Education and Training, up to $10,000 per organization. Small and medium businesses can access free cyber awareness resources through the Canadian Centre for Cyber Security: https://www.cyber.gc.ca/en/small-medium-businesses
Do I have to return unspent funds?	Yes, grant funding not used or accounted for in accordance with the approved eligible costs must be repayable by the grant recipient to the Government of Alberta.
I applied to the former ASIP grant program and was not approved/ partially approved. Can I apply again?	Yes. Organizations are encouraged to make contact with ASIP in advance of resubmitting to discuss reasons for the initial denial.

Should I print and sign my application or budget page?	Please fill out the attestation statement at the end of the documents electronically; a hand-written signature is not necessary.
How should I submit my receipts/quotes, or other supporting documents?	If possible, attach electronic files/scan and email all supporting documents to asip@gov.ab.ca
I've received advice from a third party about my eligibility for an ASIP grant, but I'm not sure if my application meets the program's eligibility criteria. What should I do?	If you are unsure about eligibility or have questions about the program, please contact ASIP staff directly at asip@gov.ab.ca

APPENDIX A: SECURITY RISK ASSESSMENT

The first step in the process of managing security risks is to identify and analyze the threats and vulnerabilities facing a facility by conducting a Security Risk Assessment (SRA). An SRA is a tool to assist organizations in making decisions on the need for countermeasures to address threats and vulnerabilities.

A Security Risk Assessment is a systematic process that evaluates the likelihood that a threat against a facility–such as a hate/bias motivated crime or incident–will be successful and considers the potential severity of consequences to the facility, its occupants, the organizations operations and the surrounding community. The objective of conducting a SRA is to identify security hazards, threats and vulnerabilities facing a facility, and to evaluate the countermeasures to provide for the protection of the facility, its occupants and the organization's operations. Security risks can be assessed and strategies can be formed to reduce vulnerabilities as required.

A basic premise is that not all security risks can be completely prevented. The security objectives generally employ four basic strategies to help minimize the risk:

1. Deter
2. Detect
3. Delay
4. Respond

Appropriate strategies for managing security can vary widely depending on the individual circumstances of a facility, including the type of facility, its usage(s), its occupants and the threats facing the facility. Risk assessments can be either qualitative or semi-quantitative depending on the level of risk, the amount of data available to the assessor and the methodology used.

There are numerous security risk assessment techniques and methods available to organizations, including:

- CPTED - Crime Prevention through Environmental Design,
- SAFE Design Standard ®,
- ASIS International General Security Risk Assessment,
- Security Vulnerability Assessment,
- RCMP Harmonized Threat Risk Assessment,
- THIRA - Threat and Hazard Identification and Risk Assessment, or
- US Homeland Security Risk Management Doctrine.

All share common risk assessment principles. The SRA method and depth of analysis should be chosen relative to the nature of the facility. Differences in geographic location, type of operations and occupants all play a role in determining the scope of SRA and the approach taken.

Regardless of the method used, all security risk assessment techniques should include the following activities:

Identify elements at risk	Understand the organization and identify the people, assets (i.e., property) and operations at potential risk.
Identify threat sources	Security threats are deliberate actions intended to cause harm to people and/or damage to the facility. A threat (inclusive of, but not limited to, those relating to hate/bias motivated crime and incidents) is characterized as the combination of both intent and capability of a threat actor or threat source to realize a threat or attack against an asset. General threat categories may include crimes against people, crimes against property, and quality of life/harmful societal behaviours impacting facility operations.
Identify vulnerabilities	A vulnerability is any susceptibility, flaw or condition that can be exploited for the successful realization of a potential threat against the facility and its users. Vulnerability conditions can be classified into two types: physical and procedural. A physical vulnerability condition is an actual physical deficiency, flaw or absence of physical measures designed to deter, detect, delay and/or respond to a security breach. A procedural vulnerability condition relates to the existence, implementation and oversight of policies and procedures, which are designed to deter, detect, delay, respond or recover against a security breach.
Assess the likelihood of an incident	The combination of threat and vulnerability relates to the likelihood (i.e., probability and frequency) of a threat being realized through exploitation of a vulnerability. Probability may be based upon considerations of such issues as prior incidents, trends, warnings or threats, and such events occurring at the facility. Frequency of events relates to the regularity of event.
Identify the consequences of an incident	Determine the impact of a threat being realized. The physical, psychological, financial and related costs associated with the probable incident.
Prioritize security risks	Security risk is the combination of likelihood and consequence, generally articulated as credible scenarios of threats applied against the elements at risk (i.e., people, property, services). A risk severity rating is evaluated for each scenario to support considerations of mitigation actions required.
Identify potential mitigation measures/countermeasures	Identify options available to prevent or mitigate risk scenarios through physical, procedural, logical or related security processes. Study the feasibility of implementation of options, and the practicality of implementing the options without substantially interfering with the facility's operation.
Determine residual risk acceptability	Perform a cost/benefit analysis – a systematic attempt to measure or analyze the value of all the benefits that accrue from particular mitigation options.

APPENDIX B: SECURITY RISK MANAGEMENT PLAN

Organizations should develop a security plan that sets out how they will manage their identified security risks and how security aligns with their priorities and objectives. The plan should describe how policies, procedures and controls (i.e., security equipment) are to be implemented to minimize or eliminate identified security risks identified by the security risk assessment process. Where feasible, the plan should include scalable control measures to respond to increases or decreases in risk when a threat to the entity changes.

Education and training can be an important aspect of a successful security management plan. This may include training for management and security personnel to better monitor, respond, evaluate and report security incidents. It may also include education and training for facility occupants and users to build understanding and resilience against identified security risks.

Security risk management is a cycle, not a linear path. Given continual evolution of the threat environment and inherent uncertainties, a security risk management plan should be a living document.

APPENDIX C: PUBLICLY FUNDED INSTITUTION

To support organizations interested in applying for ASIP to determine if they are considered a publicly funded institution (otherwise known as a quasi-autonomous non-government organization or QUANGO), please follow the below decision tree:

Test: Is this organization considered a publicly funded institution in Alberta?

Use the following **checklist** to assess:

1. Funding source
    - Does the organization receive **core operational funding** from a municipal, provincial or federal government body?
        - **Yes** → Likely considered a publicly funded institution.
        - **No** → Proceed to next question.

2. Governance
    - Is the organization governed by a **board or council with members appointed by a municipal, provincial or federal government?**
        - **Yes** → Likely considered a publicly funded institution
        - **No** → Proceed to next question.

3. **Inclusion in government lists**
    - Is the organization listed as a:
        - **Public post-secondary institution** (e.g., U of A, SAIT)?
        - **Health authority** (e.g., Alberta Health Services)?
        - **School board or division**?
        - **Crown corporation**?
        - **Agency, board, or commission** (ABC)?
        - **Yes** to any → Publicly funded.
        - **No** → Likely not a publicly funded institution.