Annex N

Scheduled Outreach Service
Security Assessment Requirements
Manager's Tool Guide

It is important that employees and managers are familiar with the Treasury Board Secretariat mandate and the Department's obligation to fulfill its expectations under the Government of Canada in serving the public at Scheduled Outreach locations.

The objective of the Treasury Board Secretariat's Policy on Government Security is to support the national interest and the Government of Canada's business objectives by safeguarding employees and assets and assuring the continued delivery of services.

The policy statement under TBS states that:

- Employees under threat of violence must be safeguarded according to baseline security requirements and continuous security risk management.
- Assets must be safeguarded according to baseline security requirements and continuous security risk management.
- Continued delivery of services must be assured through baseline security requirements, including business continuity planning, and continuous security risk management.

Accountability

Deputy Heads are accountable for safeguarding employees and assets under their area of responsibility and for implementing this policy.

Roles and Responsibilities

- ➢ Departments are responsible under the Canada Labour Code, Part II, and under Treasury Board policy for the health and safety of employees at work. This responsibility extends to situations where employees are under threat of violence because of their duties or because of situations to which they are exposed.
- ➢ Managers are responsible for making employees aware of their security responsibilities and requirements while working in, or travelling to and from, Scheduled Outreach locations. All Scheduled Outreach activities are subject to departmental policies, standards and guidelines.
- ➢ Employees are responsible for the protection of sensitive information and valuable assets under their control in the conduct of providing Scheduled Outreach services. This includes the use of equipment to perform the duties of a Scheduled Outreach service provider.

Due to geographical locations and cost associated with conducting threat and risk assessments it may not be deemed feasible for the TRA to be conducted by the Regional Security Office. The manager, in consultation with the Regional Security Officer, must conduct an assessment to specify the security measures to be employed at the Scheduled Outreach location.

To this extent, a Security Assessment Requirement Checklist has been developed and included in this document to assist managers when conducting a threat and risk assessment at Scheduled Outreach sites. The following list of sections within the Checklist will provide managers with a better understanding of what criteria is involved when conducting the assessment and completing the Checklist.

Section A – Personnel Security (PERSEC) Screening

- ➢ All new and existing staff considered for Scheduled Outreach service delivery functions must have a valid security screening (reliability status) with a valid credit check prior to taking on this responsibility. Specifically, each staff member must have an approved credit check if the “position, role and responsibilities include the handling, collection, disbursement and electronic manipulation of negotiable assets on behalf of the Government of Canada”.

(Note: This involves the completion of the Personnel Security Consent and Authorization (PSCA) form, TBS330-23, providing employee consent to conduct the checks and forwarding the form to the Regional Security Office for processing)

- ➢ A list of proposed staff that will fill the positions must be forwarded to the Regional Security Office in order to ensure that all new and proposed staff meets PERSEC requirements prior to training.

Section B – Training and Awareness

<u>Scheduled Outreach Tool Kit</u>

Ensure that employees are provided sufficient training and have obtained a working knowledge of operational use of all electronic equipment (if required, i.e. panic button, secure briefcase, alarms, etc.) used for their personal safety and the security of departmental assets assigned to them.

Take steps to ensure that all safety and security requirements in the *Directive on Scheduled Outreach Service* are being met:

- ➢ Provide a cellular or satellite telephone to all Scheduled Outreach employees required to travel to Scheduled Outreach sites.
- ➢ Routine testing of all equipment to ensure and maintain in good working order.
- ➢ If an automobile is being used, briefcases, containers or valuable equipment (e.g. laptop computers) must be placed in the locked trunk or, where this is not possible, out of sight while ensuring the automobile is locked. Vehicles with a trunk release in the glove

compartment and “hatchback” type offer little security and should not be used for short or long term storage of asset.

- If public transportation is used, sensitive information and valuable assets must be stored in briefcases or containers and kept in the passenger area and under visual control at all times. Sensitive documents must not be exposed at any given time.

When there is a requirement to travel (e.g. by train or plane) with documents too bulky to be carried in locked briefcases, documents must be sent in a secure approved container which is checked in before departure. Check with your Regional Security Office for guidance.

<u>1) Personal Safety</u> – Provide safety training and awareness to all Scheduled Outreach service providers required to travel to and from work at alternate delivery sites. This will include, but is not limited to, the following considerations:

- Drive Safe program
- Emergency procedures and continuity planning
- Dealing with distressed/aggressive client behaviours

<u>2) Security of Information and Valuable Assets</u>

Training and awareness must be provided to employees on the required safeguards identified in security related policies, procedures and guidelines for the protection of sensitive information and valuable assets. This will include, but is not limited to:

- Levels of information handled by the department.
- Guidelines on the handling, collection, marking, transmitting, transporting, storage, etc.
- Reference to *Access to Information Act and Privacy Act* (ATIP) legislative tool behind the security requirements (Information Classification Guide – ref. guide).
- Security of information/assets while in transit. (Ref. Telework Policy).
- Telework Security Briefing form.
- Loan of Departmental Equipment and Return of Departmental Equipment forms.

Section C – Employee Safety and Emergency Response

The Director or delegate is required to develop, test and maintain emergency plans for their offices to protect employees and clients, and safeguard sensitive information and assets during emergencies. Security contingency plans are to include such emergencies as: fire; natural disasters; bomb threats; unauthorized occupations; break and enters; and other unforeseen incidents.

The Manager will need to ensure that the following requirements are included in the overall assessment. The examples provided are not exhaustive but will provide the manager with guidance when considering these types of service offerings at alternate sites.

(Examples: valid driver’s license / insurance - vehicle walk-around inspection - emergency tool kit (flares, flashlight, batteries, matches, candles, booster cables, chocolate, water, wool blanket, cones, etc.) - inclement weather conditions (required equipment e.g. snow tires, shovel) -

roadside assistance - service centers - emergency contact numbers (local police, ambulance, fire, CAA, host site, etc) - road maps - alternate route changes - potential emergencies while in transit – guidelines)

Note: An additional emergency contact list must be carried on the person at all times in the event that other predetermined ones are not easily accessible.

Section D – Physical Security

Physical security applies to structures, buildings and the space within them. The main objective of physical security measures is to provide sufficient protection for employees and premises, and prevent compromise of classified and/or protected information and material assets.

Components in the Checklist consist of exterior lighting, parking lots, emergency exits and secure storage.

- Sensitive information and/or negotiable assets stored overnight must be secured in an approved safe or container. Combinations must be changed regularly and be known only by those requiring access to the assets.
- While in transit, a secure approved briefcase must be used for sensitive information and valuable assets (Contact the RSO for guidance/advice)
- At the site, the briefcase can be used as a storage container, equipped with an approved locking cable affixed to a stationary piece of furniture while on site.
- Name tags, photo ID cards must be worn at all times while on site.
- Keys to secure cabinets, privacy cabinets must be protected accordingly and only provided to those on a need to know/have basis.

Section E – Secure Zones / Access Controls

The department is required to establish progressively restrictive zones in order to control access to classified and protected information.

Defining zones to protect staff, sensitive information and assets is an integral part of security design. The effective use of zoning depends on the implementation of appropriate security procedures in accordance with a TRA.

The assessment includes a description of the site and identification of other alternate partners/community service providers present and outline common shared areas such as washrooms, cafeteria, kitchen etc, and the location of the employee workstation.

Section F – Workstation Design

The location and details surrounding the employee workstation is intrinsic to the overall assessment. It must include an overall review of the set up and any risks associated with its location and design. It is important that the workstation provides easy egress from the area in the event of an emergency resulting from a threatening situation (e.g. fire, threat to personal safety and security). Other factors involved would centre on any additional security measures proposed for implementation into the overall design (e.g. panic alarm systems, closed circuit video equipment (CCVE), etc.).

Section G – Incident Reporting

The Regional Security Office must be notified immediately in the event of security incidents involving employees, clients and sensitive departmental information and assets by way of electronic mail (e-mail), facsimile (fax), or other authorized means (e.g. telephone). The completion of the Security Incident Report (ADM3061B) must be provided to the manager as soon as possible.

Additional Information

- To maintain the required security, managers must ensure that Scheduled Outreach arrangements comply with the following conditions:

    - Functions requiring the removal/transportation/temporary storage of files containing personal client information or other sensitive material must have appropriate mechanisms in place (secure briefcase/container) to ensure a level of security equivalent to that on-site;
    - Functions requiring ongoing electronic access to departmental databases and systems containing personal or other sensitive information must have a secure gateway and encryption devices in place, or use of dedicated lines. The respective Local Area Network Administrator should be contacted to authorize and establish this access;
    - All government information and assets used for Scheduled Outreach purposes must be immediately returned to the Department upon termination of the Scheduled Outreach arrangement;
    - The RC Director or Regional Security Officer (RSO) should be immediately notified of any security incident;
    - Staff members must at all times display their departmental identification cards while working at any Scheduled Outreach location for security and personal safety reasons.
    - When travelling to a Scheduled Outreach location on a regular basis, it is recommended that the same route be taken each and every time, and a record of the route be placed on file at the home office. Approximate departure, arrival and duration of travel times should be noted with a contingency plan in place in the event of serious deviation.
    - Staff should be apprised of the Scheduled Outreach location’s emergency evacuation plans/procedures and all relevant exits. A list of local emergency numbers should be easily accessible at all times with readily available communication devices.

Note: A Scheduled Outreach security threat and risk assessment must be completed anytime there is a change to existing operations, service offerings and/or locations, site refits and/or /redesigns.

Service
Canada

Annex N

Scheduled Outreach Security Assessment Requirements Checklist

The RC Director, or delegate, is responsible for having a site Security Assessment conducted to identify security measures required to adequately protect staff, sensitive information and valuable assets. The following table provides a checklist of security and safety factors that must be considered and corrective action taken to ensure that identified deficiencies are addressed accordingly. Consult the Regional Security Office for advice, guidance and support. A copy of the checklist must be provided to the Regional Security Office upon completion.

Date of Scheduled Outreach Security Assessment conducted: _____ / ___ / ___

Scheduled Outreach Site Identification

Complete Address, Description and Scheduled Outreach Hours of Operation

Statistics on Security Incidents

Please identify the number of incidents that were reported to management since the beginning of the current fiscal year:

	Break and Enters/Thefts
	Personal property thefts
	Vandalism/mischief
	Abusive/irate clients
	Harassment
	In-person threats
	Mail threats
	Telephone threats
	Other (specify):

Security and Safety Checklist Index

SECURITY REQUIREMENTS	N/A	YES	NO	OBSERVATIONS
A. PERSONNEL SECURITY SCREENING REQUIREMENTS				
a) Does the employee(s) hold a valid Reliability Status that includes a: - Criminal Record Name Check; and - Credit Check?				
B. TRAINING AND AWARENESS ***I. Personal Safety***				
a) Have employees undergone training and awareness on how to deal with incidents relating to personal safety and security while performing this type of service delivery in rural, remote areas?				
b) Have employee's undergone first-aid / CPR training and hold a valid certificate in the event of a situation occurring that requires self or assisted administration?				
c) Are employee's provided with training on how to conduct a vehicle inspection (e.g. lights, tires, etc.)?				
d) Are employee's provided with a list of emergency contact numbers requiring both vehicle and personal emergency services within the community and while travelling to and from the Host site?				
e) Are employee's aware of the procedures in place in the event that an incident occurs that threatens their personal safety and security?				
f) Have employee's been briefed on how and when to report an incident?				

SECURITY REQUIREMENTS	N/A	YES	NO	OBSERVATIONS
B. TRAINING AND AWARENESS ***II. Security of Information and Assets***				
a) Have employees undergone security awareness on the protection of sensitive information and valuable assets?				
b) Is the employee aware of the Telework Policy?				
c) Has the Telework Security Briefing form (ADM5019B) been reviewed and signed by both the manager and employee?				
d) Is a Security approved briefcase provided for the secure storage of sensitive information and valuable assets while in transit?				
e) Is there physical equipment provided for the secure storage of sensitive information and valuable assets while at the site?				
f) Has the Loan of Departmental Equipment form (ADM3004) been completed for the removal of valuable assets from the home sites?				
g) Are the employees provided with a quick reference document regarding the protection, collection and storage of sensitive information and valuable assets (Information Classification Guide)?				
h) Has training been provided on how to complete the revised Security Incident Report (ADM3061B) when an incident occurs that involves a compromise to a client's personal information and/or departmental sensitive information?				
i) Have employees been made aware of the delegation of authorities with regard to releasing personal client information to local law enforcement?				
j) Have employees undergone IT security awareness sessions?				
k) Have employees been made aware of IT security requirements with regard to the protection of sensitive information contained on laptops, USB sticks and/or other electronic media?				

SECURITY REQUIREMENTS	N/A	YES	NO	OBSERVATIONS
C. EMPLOYEE SAFETY AND EMERGENCY RESPONSE				
a) Has the employee been provided with a cell/satellite phone, with antenna, into which an emergency number has been programmed?				
b) Are employees familiar with the local emergency service providers within the community?				
c) Have contingency plans been developed to respond to: fire; bomb threats; public demonstrations/illegal occupations; hostile/abusive clients; physical threats; telephone threats?				
d) Are contingencies reviewed / updated accordingly every 12 months; following site locations, relocations; changes in service delivery for these sites?				
e) Are the emergency procedures known to employees and have employee's been trained in the established protocols?				
f) Are emergency evacuations or evacuation drills conducted at these sites at least once a year?				
g) Are enhanced security measures, such as alarm systems (duress/panic alarm) services, available to assist in emergency situations affecting the safety and security of staff and clients? If yes, i) are employees aware of the procedures to operate and activate these systems and ii) are systems tested on a monthly basis?				
h) Is the vehicle equipped with an emergency supply kit, including a first aid kit?				

SECURITY REQUIREMENTS	N/A	YES	NO	OBSERVATIONS
C. EMPLOYEE SAFETY AND EMERGENCY RESPONSE				
i) Are known alternate routes to and from the Host site documented in the event of the need to make other travelling arrangements?				
j) Is a road/community map provided and shows emergency service provider locations? (e.g. hospital/medical clinic, fire/police station, etc.)				
D. PHYSICAL SECURITY				
1. Security Lighting				
a) Has adequate lighting been installed to illuminate entry/egress doors, windows and other points of entry, perimeter barriers, and vulnerable areas?				
b) For safety and security requirements, do lights: i) avoid shadows, and ii) provide a safe environment for staff when working extended hours at twilight and after sunset?				
c) Is there sufficient illumination in parking lots for security of employees and clients?				
2. Emergency Exits				
a) Are emergency exit signs posted above doors leading to the exterior of the building?				
b) Are emergency doors installed to swing outward?				
c) Are emergency doors equipped with panic hardware to facilitate opening?				

SECURITY REQUIREMENTS	N/A	YES	NO	OBSERVATIONS
C. EMPLOYEE SAFETY AND EMERGENCY RESPONSE				
d) Is the operation of hardware on emergency exits inspected periodically by qualified personnel?				
D. PHYSICAL SECURITY				
e) Is there auxiliary battery back-up lighting for all emergency doors?				
3. Parking Lots				
a) Are parking spots available for the employees and situated to minimize the threat to employee's and other departmental assets, by facilitating surveillance of high-risk areas?				
b) Are parking lots adequately illuminated for employee/visitor safety/security?				
4. Security Equipment				
a) Is the Host site equipped with an RCMP approved secure container for the storage of sensitive information and valuable assets?				
b) Is a cable lock provided to be affixed to stationary furniture in the event that the briefcase must be secured by this means?				
c) Is the workstation equipped with a lock/drop-box for the daily storage of sensitive information and/or valuable assets?				
d) Is this site equipped with an RCMP approved shredder?				

SECURITY REQUIREMENTS	N/A	YES	NO	OBSERVATIONS
E. SECURE ZONES, ACCESS CONTROL				
1. Zones				
a) Is the area shared with other tenants/community partners? If yes, describe.				
b) Is there a procedure in place for sign-in/sign-out for visitors/clients?				
c) How close is the workstation to the closest exit?				
d) Will the employee be responsible for the opening and closing of the Host site?				
2. Closed Circuit Video Equipment (CCVE)				
Is there a closed-circuit video equipment (CCVE) system in use at this site?				
3. Common Service Spaces				
a) Are there common service areas for the use and convenience of the employee and general public such as: i) cafeterias, and ii) washrooms?				
F. WORKSTATION DESIGN				
a) Is the workstation in close proximity to other areas within the Host site?				
b) Is the workstation designed in a way that affords privacy and confidentiality to the client and prevents unauthorized disclosure of sensitive information/discussions?				
c) Is there a quick access list of emergency contact numbers and procedures posted in the event that the employee requires immediate assistance?				

SECURITY REQUIREMENTS	N/A	YES	NO	OBSERVATIONS
F. WORKSTATION DESIGN				
d) Is the workstation designed in a way that allows the employee to have quick egress should a possible threatening situation occur?				
e) Is the phone equipped with a dedicated line for local emergency response? (e.g. police, ambulance, fire department).				
G. INCIDENT REPORTING				
1. Threats and Abuse				
a) Is there a history of past threatening situations at this site? If yes, please describe.				
b) Are employees aware that it is a mandatory requirement to report all incidents of threatening personal situations to the manager and to complete the Security Incident Report form (ADM3061B)?				
c) Are managers aware that the ADM3061B report is to be sent immediately to Regional Security?				
d) Are procedures in place for response and/or action of such incidents?				
e) Are employees advised of counseling services available to them if required?				
f) Is there a Work Place Health and Safety Committee or Representative established at the home site to deal with threatening situations of an actual or implied threatening behaviour experienced at the Host site or while in transit?				
Additional Observations, Comments and Recommendations:				

Note: Policy and Form Reference Tools Attached (Last page)

Section 6 – Acknowledgement of Voluntary Compliance

I have read and understood the above guidelines and certify that the premises and staff at (_____*address*_ ____________) are in compliance, except for the following areas:

____
Signature of Manager/Director

____
Date

Section A – PERSONNEL SECURITY SCREENING REQUIREMENTS

Issue No.	Description	Current Condition	Work Required	Completion

Section B – TRAINING AND AWARENESS

Issue No.	Description	Current Condition	Work Required	Completion

Section C – EMPLOYEE SAFETY AND EMERGENCY RESPONSE

Issue No.	Description	Current Condition	Work Required	Completion

Section D – PHYSICAL SECURITY

Issue No.	Description	Current Condition	Work Required	Completion

Section E – SECURE ZONES / ACCESS CONTROLS

Issue No.	Description	Current Condition	Work Required	Completion

Section F – WORKSTATION DESIGN

Issue No.	Description	Current Condition	Work Required	Completion

Section G – INCIDENT REPORTING

Issue No.	Description	Current Condition	Work Required	Completion

Assessment Conducted by: ______________________________ Date: _____ / ___ / ___
Director / Delegate / Manager

Home office Address: _________________________
____
____

Phone number: ( ) xxx - xxxx

Approved by: ______________________________ Date: _____ / ___ / ___
Director's Signature

Phone number: ( ) xxx - xxxx

Reviewed by: ______________________________ Date: _____ / ___ / ___
Regional Security Officer Signature

Reference Tools

E-Forms Link

Name	Number
Loan of Departmental Equipment	ADM3004B
Return of Departmental Equipment	ADM5018B
Telework Security Briefing Form	ADM5019B
Security Incident Report	ADM3061B
Hazardous Occurrence Investigation Report	LAB1070B

http://forms-formulaires.prv/eform99/index.cfm?App=Launch&FormID=1180&GroupID=140&LANG=E

Security Policy Links

Departmental Security Policy and Procedures Manual
http://iservice.prv/eng/is/security/docs/SecurityManual.pdf

G. Telework Security
http://intracom.hq-ac.prv/sc-isb-dsi/eng/security/security_manual1.shtml#teleworkpolicy

Regional Security Officers – Contact List
http://iservice.prv/eng/is/security/contact_us/rso_contacts.shtml

Approved by: **ORIGINAL SIGNATURE ON FILE**
Marc Proulx, Director
Corporate Security

Date: 2010 / 05 / 28

Revised: 2012-05-28

Revisions Approved by: ___________________________________
Lucie Clément, Director Corporate Security
Internal Integrity and Security Directorate (IISD)

Date: ____/__/__