|  |  |
| --- | --- |
| Operating PolicyCanada and Bermuda Territory | **N:\A - Personal\Locker\Personal\Pictures\Graphics\SA\Shield & Crest\SA_GivingHopeToday_red_hor_lrg_rev_black.jpg** |
| Policy | Privacy |
| Value | Dignity | OP Number | GV 01.009 |

Table of Contents

[1. Policy 2](#_Toc117747749)

[2. Purpose 2](#_Toc117747750)

[3. Scope 2](#_Toc117747751)

[4. Definitions 2](#_Toc117747752)

[5. Roles and Responsibilities 3](#_Toc117747753)

[**5.1.** Territorial Privacy Officer 3](#_Toc117747754)

[**5.2.** MU/DHQ Privacy Officer, THQ Department Head (DH) 4](#_Toc117747755)

[**5.3.** Supervisors 4](#_Toc117747756)

[**5.4.** Mission Partners 4](#_Toc117747757)

[6. Policy Requirements 4](#_Toc117747758)

[**6.1.** Compliance with Legal Requirements 4](#_Toc117747759)

[**6.2.** Alignment with Privacy Law Principles 4](#_Toc117747760)

[6.2.1. Purpose, Consent, Limiting Collection, Uses and Disclosures 4](#_Toc117747761)

[6.2.2. Accuracy, Accountability, Openness, Limiting Retention 5](#_Toc117747762)

[6.2.3. Individual Access, Challenging Compliance 5](#_Toc117747763)

[6.2.4. Safeguards 6](#_Toc117747764)

[**6.3.** Personal Information Requests (PIRs) 6](#_Toc117747765)

[**6.4.** Privacy Complaints 6](#_Toc117747766)

[7. Policy Compliance 6](#_Toc117747767)

[8. Procedure Links 6](#_Toc117747768)

[9. Form Links 6](#_Toc117747769)

[10. Related Policy and Document Links 7](#_Toc117747770)

[11. Approval and Document Control 7](#_Toc117747771)

# Policy

This policy governs The Salvation Army's (TSA) management of personal information in the custody or control of TSA.

# Purpose

The purpose of this policy is to ensure TSA's practices meet legal obligations and standards related to privacy, and describes the responsibilities related to privacy associated with different roles within TSA.

# Scope

This policy applies to all personal information in the custody or control of TSA and applies to all TSA mission partners.

# Definitions

| Term or Acronym | Description |
| --- | --- |
| Disclosure | Disclosure means external disclosure - showing, sending, telling or giving some other organization or individual information. Disclosure can take various forms, including oral transmission of recorded information, by telephone or in person, by provision of personal information on paper, by facsimile copy or in another format and by electronic transmission through email, data transfer or the internet. |
| Extent of access | The amount and type of information to which a mission partner has access. |
| Improper disposal of PI | Disposal of PI that is not completed in accordance with TSA's policies. |
| Legal requirements  | Requirements that arise from legislation or contracts, including funding contracts, non-disclosure/confidentiality agreements and confidentiality statements.  |
| Level of access | The kind of access to information that a mission partner has (read-only or broader access, such as the right to modify, delete information, etc.) |
| Manage | To collect, access, use, copy, modify, store, convert the format of, deliver, disclose, transmit, handle, destroy, erase, dispose of. |
| Mission Partner | All officers, auxiliary-lieutenants, auxiliary-captains, envoys, cadets, employees (full-time, part-time, casual or on contract) and volunteers.  |
| Personal Health Information (PHI)  | PHI is personal health information as defined by the legislation that applies to a TSA ministry unit. PHI generally means identifying information, in oral or recorded form, about an individual, if the information relates to:1. the physical or mental health of the individual, including health history of the individual's family,
2. providing of health care to the individual, including the identification of any person providing health care to the individual,
3. a plan that sets out the home and community care services for the individual provided by a health service provider,
4. payments, coverage, or eligibility for health care for the individual,
5. the donation by the individual of any body part or bodily substance of the individual, or is derived from the testing or examination of any such body part or bodily substance,
6. the individual's health number, or
7. identification of an individual's substitute decision-maker.
 |
| Personal Information (PI)  | PI is personal information as defined by the legislation that applies to a TSA ministry unit. PI generally means any information about an identifiable individual and includes information such as a person's name, phone number or address, as well as factual and subjective information in any format (paper, electronic, audio, video, oral). It is also referred to as personally identifiable information (PII). |
| Personal Information in TSA's control | PI for which TSA is accountable, even if not in TSA's physical possession, e.g., PI in the custody of a third-party service provider under contract with TSA. |
| Personal Information in TSA's custody | PI in TSA's possession, accompanied by some right to deal with the information or some responsibility for its care and protection.  |
| Privacy Incident  | A privacy incident occurs when it is known or believed that any PI or PHI has been the subject of:1. unauthorized collection, access, use, copying, modification, disclosure or destruction/disposal,
2. loss (including improper destruction/disposal) or theft, or
3. any other misuse or breach of privacy.
 |
| Sensitive Personal Information (Bermuda only) | Sensitive PI is any PI relating to an individual's place of origin, race, colour, national or ethnic origin, sexual orientation, sexual life, physical or mental disability, religious beliefs, political opinion, biometric or genetic information, health information, financial information and any other information that may be sensitive depending on the context. |
| Supervisor | A mission partner's direct report. |
| Use | Use generally means the use of information within TSA and includes the transfer of information to a third-party service provider. |
| Use (Bermuda only) | Use, in relation to PI means carrying out any operation on PI, including collecting, obtaining, recording, holding, storing, organizing, adapting, altering, retrieving, transferring, consulting, disclosing, disseminating or otherwise making available, combining, blocking, erasing or destroying. |

# Roles and Responsibilities

## Territorial Privacy Officer

Is responsible for:

* Recommending updates to this policy and promoting compliance with it
* Assisting MUs/DHQ/THQ departments with various privacy-related issues, including investigations into privacy incidents
* Processing complaints that are not resolved at the MU/DHQ/THQ department level and addressing privacy-related matters related to closed MUs.

## MU/DHQ Privacy Officer, THQ Department Head (DH)

The corps officer or executive director of a MU is the MU's privacy officer. The divisional commander (DC) is the privacy officer of DHQ. A corps officer/executive director/DC/DH may designate a mission partner to perform this function or delegate their duties to a mission partner; such transfer of responsibility must be formally documented.

A DH or MU/DHQ privacy officer is responsible for:

* Receiving, processing and responding to inquiries about PI practices, personal information requests and privacy complaints
* Investigating departmental privacy incidents, completing and submitting an FRM Privacy Incident Report to the territorial privacy officer

In addition, a MU/DHQ privacy officer must fulfill any additional obligations that are specific to the privacy officer role in the jurisdiction or at that location

## Supervisors

Supervisors are responsible for:

* Ensuring that mission partners manage PI in accordance with privacy requirements
* Reporting privacy incidents to the privacy officer/DHs

## Mission Partners

Mission partners are responsible for:

* Managing PI in accordance with privacy requirements
* Reporting privacy incidents to their supervisor

# Policy Requirements

## Compliance with Legal Requirements

MUs/DHQs must comply with the privacy-related legislation and contracts that apply to their operations.

## Alignment with Privacy Law Principles

### Purpose, Consent, Limiting Collection, Uses and Disclosures

Any collection, use or disclosure of PI must be for a purpose that a reasonable person would consider appropriate in the circumstances

The amount and type of PI collected, used or disclosed must be limited to what is directly relevant and necessary to accomplish the purpose identified

An individual must be informed of:

* The purpose(s) for which the individual's PI is to be collected, used or disclosed;
* The types of PI that are to be collected, used or disclosed;
* The manner in which/means by which PI is to be collected, used or disclosed;
* How PI is to be used;
* The third parties or types of third parties to whom PI may be disclosed;
* The rights that the individual has regarding PI, including the right to access PI, correct PI and withdraw consent regarding further collection, use or disclosure of the individual's PI; and
* If the PI is collected in Quebec, the possibility that the information may be shared outside Quebec, if applicable.

The above information must be communicated to the individual before or at the time of collection and must be documented.

Collection, use and disclosure of PI must occur only with the consent of the individual unless the applicable legislation allows for an exception to this rule. An additional purpose/use/ disclosure of PI requires further consent from the individual.

An individual who refuses to consent to the collection, use or disclosure of PI must not be denied services, unless there are legitimate reasons for the denial of service, such as legal requirements, which must be explained to the individual.

An individual may withdraw consent to the further collection, use or disclosure of the individual's PI, subject to applicable legal or contractual restrictions and subject to reasonable notice. In such a case, the individual must be informed of the implications of withdrawal and the information provided must be documented.

### Accuracy, Accountability, Openness, Limiting Retention

PI collected, used or disclosed must be as accurate, complete and current as possible.

The title and office contact information of the person who can respond to questions about PI practices must be made available to mission partners and to members of the public.

Where third-party service providers manage PI on behalf of TSA, the PI must be protected by adequate contractual provisions.

PI must be retained only as long as necessary to fulfill the purpose for which it was collected or to comply with legal requirements. Where PI has been used to make a decision about an individual, it must be retained long enough to allow the individual to access the PI, as required by IT 04.001 Data Retention policy and disposed of as required by IT 04.002 Data Destruction policy.

### Individual Access, Challenging Compliance

Information about how to make a PI request/privacy complaint and to whom such a request/complaint should be directed (the person's job title, business contact information) must be made available to mission partners and to members of the public.

### Safeguards

PI must be managed in a secure manner. This requires PI is always protected by physical, administrative and technical safeguards that are appropriate given the sensitivity and other characteristics of the PI involved. PI must be protected from loss, including improper destruction/disposal, from theft and from unauthorized action, including unauthorized access, collection, use, disclosure, copying, modification and destruction/disposal by people from within or outside TSA.

Access to PI must be strictly limited to authorized mission partners only. Where access is required, the extent and level of access must be limited to what is necessary for the performance of the authorized mission partner's duties. Mission partners are required to sign confidentiality agreements.

## Personal Information Requests (PIRs)

A funder's process regarding the processing of PIRs must be followed. In the absence of a funder-required process, individuals may make PIRs directly to TSA for the purpose of:

* Accessing, updating or correcting their PI that is in the custody/control of TSA;
* Withdrawing consent to TSA's continued collection, use or disclosure of their PI;
* Exercising other rights, such as erasure of PI or transfer of PI, in jurisdictions where such rights exist.

When granting access to PI is not a legal requirement, TSA may limit access to PI.

## Privacy Complaints

Individuals may make a privacy complaint about the way in which their PI was managed by TSA or about how their PIRs were processed by TSA.

# Policy Compliance

Compliance with this policy is mandatory. Non-compliance may lead to disciplinary action as determined by TSA and could constitute an offence under applicable legislation. All mission partners are responsible for reporting policy violations.

# Procedure Links

[PRO - Safeguarding Personal Information](https://tsacb.sharepoint.com/%3Aw%3A/s/OPP/EcfOkdq653pCjIyZLtOi77oB2cqrvWyjGJW3QbIXw4M1JA?e=zDABTE)

# Form Links

[FRM Confidentiality Agreement for Mission Partners](https://tsacb.sharepoint.com/%3Aw%3A/s/OPP/Ea7_Xbuo2ZhHkoFPSMU6OhsBU3_6SX5a1e4k2-znhOYctA?e=Dlxl86)

[FRM Personal Information Request](https://tsacb.sharepoint.com/%3Aw%3A/s/OPP/ERDDOZs8HflBlsMRn3C7r-4BaCwDTw0tDgtxog-oVI0wOA?e=vvlo29)

[FRM Privacy Complaint](https://tsacb.sharepoint.com/%3Aw%3A/s/OPP/EVl4kWjWdEVLkzHYVJCcLxMBUnoQypSvfahUenJtsFidKg?e=80tm5H)

[FRM Privacy Incident Report](https://tsacb.sharepoint.com/%3Aw%3A/s/OPP/EV8BCEcNf81Fh1DUpGY3tuUB5kC2bdBFdNT_sV935E2kuA?e=RhdNCy)

[FRM Privacy Questionnaire for Third-Party Service Providers](https://tsacb.sharepoint.com/%3Aw%3A/s/OPP/ESlBlHq121NJs8Tu7Vh6n54BruA4lL-gC3t4Pnsn3xpnQQ?e=KSKsAP)

[FRM Sample Client Consent](https://tsacb.sharepoint.com/%3Aw%3A/s/OPP/EUuHq1ZImRFJmsiaa4tuj1cB8YmplB9eHlmUi_6C4xzoYw?e=fdQySm)

# Related Policy and Document Links

[SUP Guidelines: Applicable Privacy Legislation](https://tsacb.sharepoint.com/%3Aw%3A/s/OPP/EYPBvsvXGsVOjgF2zBeyq_wBt1tHINqrgzQLc9tfzGn6Zg?e=gNUvWQ)

[SUP Guidelines: Collection of personal data: Social Insurance, Personal Health, Driver's License and Passport Numbers](https://tsacb.sharepoint.com/%3Aw%3A/s/OPP/Ef0_TYwdEklPpY3kEyihcGUB0QaUFaL1fW39wNe1sCOFgA?e=UJ55ws)

[SUP Guidelines: Contractual Provisions](https://tsacb.sharepoint.com/%3Aw%3A/s/OPP/Edciv8zziQpCpePO8oBNZGkByAiXpC1c55Fws-q-JN87-Q?e=3u5rvE)

[SUP Guidelines: Personal Health Information Definitions](https://tsacb.sharepoint.com/%3Aw%3A/s/OPP/EZWBI6tnRQ5GoSDRRnAfvDkBD0kyH4raTCYtGw4J5D2euQ?e=dQeZKs)

[IT 02.001 Computers and Information Technology Acceptable Use](https://tsacb.sharepoint.com/%3Aw%3A/s/OPP/EST87V2cdbxClwMkhlmbfOUBvjDxczrFi2HdNGXHZ_V6nQ?e=Uol2SN)

[IT 02.002 Information Security](https://tsacb.sharepoint.com/%3Aw%3A/s/OPP/ERa4CpgTdGlLh-UN3geOg90Bros8g3ZmPi3-cg1UItpeYg?e=Y8Z1Rc)

[IT 04.001 Data Retention](https://tsacb.sharepoint.com/%3Aw%3A/s/OPP/EVMf7kE_oj9Ko0bAeGImIVEBWc-xfPGFQJKfFXpWaIVfGg?e=GIrZnW)

[IT 04.002 Data Destruction](https://tsacb.sharepoint.com/%3Aw%3A/s/OPP/EbXPWjJgJAlFrKQzU2Zl-9QB4ObJRWBOsqSlyuPK_g-LmA?e=hPDpGZ)

[IT 04.003 Data Classification](https://tsacb.sharepoint.com/%3Aw%3A/s/OPP/EYfGoLDBjxlBhdpdl2t1qdIBLJ5Ojev3_QLaizlEKmMVpQ?e=uY8ypJ)

Destruction of Devices and Media Policy (under development)

# Approval and Document Control

**Approved by:**

Territorial Management Board

Canada and Bermuda Territory

**Only the online version of this operating policy is official and current.**

| **Document Control Information** |
| --- |
| **Category** | Governance: General |
| **Committee/Board****Responsible** | Business Administration Committee |
| **Policy Sponsor** | Legal Department |
| **Approved Date** | 18 Mar 2008 | **Next Review Date** | 24 Oct 2024 |
| **Document History** |
| **Version** | **Date Revised** | **Summary of Changes** |
| V-01 | New |  |
| V-02 | 12 Nov 2020 | Format to new OPP Template |
| V-03 | 24 Oct 2022 | Full content revision to reflect changes in legislation |