1. Overview

The Public Service Client Support Program (PSCSP) provides services to citizens, organizations, and internal government departments. The program operates under a framework of legislation, policies, and internal directives that govern eligibility, privacy, service standards, and compliance requirements.

This document summarizes key rules and procedures overseen by the PSCSP, including obligations for both employees and clients.

2. Legislative and Policy Framework

2.1 Governing Legislation and Statutory Obligations

The policies and procedures outlined in this document are governed by several key pieces of legislation, ensuring compliance with public administration standards, client data protection, and accessibility mandates. Departments must strictly adhere to the provisions set forth in the following Acts:

a. Public Service Administration Act (PSAA)

The Public Service Administration Act is the foundational legislation that governs the operational authority and accountability of all government departments and agencies.

- **Defines Departmental Authority and Service Delivery:** The PSAA explicitly defines the scope of authority for departments to manage and execute public service delivery. This includes the power to establish necessary administrative structures, allocate resources efficiently, and determine appropriate methods for service provision to meet public needs.
- **Establishes Reporting and Public Accountability:** The Act places mandatory requirements on departments for transparent reporting to the relevant legislative body and to the public. This includes providing regular updates on performance metrics, financial stewardship, and adherence to service standards. This requirement is central to upholding the principle of public accountability and building citizen trust.
- **Mandates Accessible, Non-Discriminatory Service Channels:** A core tenet of the PSAA is the requirement for all departments to maintain service channels that are accessible to the broadest possible range of clients and free from any form of discrimination. This ensures equity in access to government services, necessitating ongoing review of service delivery methods to remove systemic barriers.

b. Client Information Protection Act (CIPA)

The Client Information Protection Act is the primary statute regulating how government entities handle the sensitive personal and private information of clients.

- **Regulates the Client Data Lifecycle:** CIPA provides stringent regulations governing every stage of client information management, from its initial **collection** (ensuring data minimization and relevancy) and **use** (restricting use to the stated purpose), through to its **retention** (establishing clear limits on how long data can be stored), and eventual secure **disposal** (mandating irreversible destruction when the data is no longer legally required).
- **Requires Consent for Non-Essential Data Collection:** The Act specifies that explicit, informed consent must be obtained from the client before any data collection occurs that is not strictly necessary for the statutory function or core service being provided. Departments must clearly articulate the purpose and intended use of such non-essential data.
- **Restricts Cross-Departmental Data Sharing:** A crucial protective measure of CIPA is the limitation on sharing client information across different government departments or agencies. This prohibition stands unless specific exceptions are met, as detailed under **Section 12** of the Act. These exceptions typically relate to legal requirements, matters of public safety, or clearly documented shared service agreements where the client has been informed.

c. Accessible Service Delivery Act (ASDA)

The Accessible Service Delivery Act mandates a proactive approach to ensuring that all public services are accessible to persons with disabilities, going beyond the basic requirements of the PSAA.

- **Mandates Accessible Communication Formats:** ASDA requires departments to provide all official communication materials (e.g., forms, brochures, policy documents, notices) in multiple accessible formats upon request. This includes, but is not limited to, large print, braille, audio formats, and digital formats compatible with screen readers, ensuring effective communication for all users.
- **Requires Provision of Alternative Service Channels:** To meet the diverse needs of clients with accessibility requirements, the Act mandates that departments maintain and actively offer a variety of alternative channels for interacting and receiving services. This includes dedicated support through **phone** (e.g., TTY/teletypewriter services), **web** (e.g., fully WCAG-compliant websites), and structured **in-person** assistance, ensuring no client is disadvantaged based on their accessibility needs.

---

3. Mandatory Departmental Policies3.1 Identity Verification Policy: Comprehensive Guide

The Department maintains a strict Identity Verification Policy to protect client confidentiality, prevent fraud, and ensure the accurate delivery of services. **Adherence to this policy is mandatory for all departmental employees.**

3.1.1 Mandatory Verification Scenarios

Employees **must** verify the identity of a client or their authorized representative under the following high-risk circumstances:

- **Requesting Access to Restricted Services:** Any action that grants a client access to sensitive or restricted departmental services, systems, or information (e.g., establishing online portal access, accessing confidential files, or changing security settings).
- **Modifying Personal Information:** Any request to alter a client's core personal data on file, including but not limited to, name changes, date of birth corrections, address updates (especially for benefit delivery), or changes to marital/dependency status.
- **Initiating a Benefit Application on Behalf of Another Individual:** When an employee is processing an application where the client is acting as a proxy, guardian, or representative for the primary recipient. This ensures the representative has the legal authority to act on the recipient's behalf.

3.1.2 Accepted Verification Methods (Tiered System)

Identity verification must be completed using one of the following official, non-expired methods:

1. **Primary Method: Government-Issued Photo Identification**
    - One piece of identification issued by a federal, provincial, or state authority that includes a photo and signature (e.g., passport, driver's license, government-issued photo health card).
2. **Secondary Method: Two Secondary Documents**
    - In the absence of a primary ID, two separate secondary documents must be presented. These documents must confirm both the client's name and current residential address. Acceptable examples include:
        - Utility bill (electricity, gas, water) from the last 90 days.
        - Current bank or credit card statement (digital or physical).
        - Current residential lease or property tax assessment.
        - Letter from a recognized shelter or social service agency.
3. **Digital Verification: Digital Government Identity Credential (DGIC)**
    - Verification can be completed through the departmental **Digital Government Identity Credential (DGIC)** system, provided the client has a registered and

active credential that meets Level 2 or higher assurance standards. The DGIC is the preferred method for remote or online service delivery.

3.1.3 Documentation and Audit Trail

For every verification performed, the employee must:

- Record the type of verification used (e.g., "Driver's License - Ontario," "DGIC," or "Two Secondary Docs - Hydro Bill & Bank Statement").
- Note the document's unique identifier (where applicable and permissible by privacy laws).
- Date and timestamp the verification event in the client's file.

Failure to properly document verification may result in the suspension of the transaction until proper documentation is provided.

3.1.4 Policy Exceptions (Section 3.1.5)

Identity verification is a cornerstone of service integrity, but the policy recognizes scenarios where strict adherence may impede essential service delivery. Exceptions are permissible only under the following strictly defined conditions:

- **Emergency Humanitarian Cases:** Situations where immediate assistance is required to prevent death, serious harm, or severe suffering, and the delay caused by verification would exacerbate the crisis.
- **Clients in Remote Communities with No Access to ID Documents:** Verified cases where clients reside in geographically isolated areas or have faced catastrophic loss (e.g., fire, flood) that makes acquiring standard ID documents immediately impossible.
- **Youth Clients Involved in Protective Services Programs:** Where a youth's participation in a mandated protective service program must proceed immediately, and obtaining formal ID is a process managed by the protective service agency.

Process for Approving Exceptions:

1. The initiating employee must complete the **Identity Verification Exception Form (IVEF-A).**
2. The exception request **must be approved by a Level-2 Officer** (Supervisor or Manager).
3. Upon approval, the Level-2 Officer is responsible for ensuring the exception is **logged in the Identity Verification Exception Registry** immediately. This centralized registry is subject to mandatory quarterly audit reviews by the Compliance Office.

Note: An approved exception allows service delivery to proceed but does not negate the requirement for the client to provide valid identification *at the earliest feasible opportunity* as a condition of continued service.

4. Service Delivery Guidelines4.1 Response Standards and Protocols

All departments are mandated to adhere to the following stringent timelines to ensure timely and effective service delivery. These standards are designed to manage client expectations and maintain operational efficiency.

Case Type	Mandated Response Timeline	Scope and Definition
General Inquiries	5 business days	Standard requests for information, policy clarification, status updates on routine matters, or non-critical support issues that do not immediately impact health, safety, or legal standing.
High-Priority Cases	48 hours	**Critical cases** explicitly involving immediate threats to health and safety, imminent legal deadlines, court-mandated actions, or situations requiring emergency intervention to prevent significant organizational or personal damage.
Formal Complaints	15 business days	Written submissions from clients or stakeholders expressing dissatisfaction with service, staff conduct, or policy implementation, requiring a formal investigation and documented resolution process.

4.2 Extension Criteria and Communication

Strict adherence to the timelines above is expected; however, service departments may apply for an extension under specific, unavoidable circumstances. The granting of an extension is not automatic and requires formal internal approval based on the following criteria:

1. **Exceptional Case Volume Surge:** When the incoming volume of new cases across the department exceeds a verified 20% increase over the rolling 30-day average, demonstrably straining staff capacity.
2. **Reliance on External Agencies:** Delays caused by waiting for critical information, documentation, or decisions that must be furnished by third-party external regulatory bodies, legal counsel, or other non-internal agencies. The delay must be directly attributable to the external party.
3. **Significant System Downtime:** Any unscheduled system outages of core service delivery platforms (e.g., CRM, case management system, network access) that persist for a cumulative period longer than 2 hours within a single business day, crippling the ability of staff to process and respond to cases.

Mandatory Client Communication Protocol for Timeline Extensions

When a timeline extension is necessary and approved, the responsible department **must** provide the affected client with the following essential information:

1. **Explanation for the Delay:** A clear reason (e.g., "High volume," or "Awaiting external information").
2. **Revised Timeline:** The estimated *new* date for case resolution or the initial substantive response.
3. **Point of Contact:** The name and contact information for the staff member managing the case for follow-up.

4.2 Comprehensive Communication Policy for Employees

This policy outlines the mandatory standards and prohibited actions for all employee communications, particularly those involving client and stakeholder interactions, to ensure clarity, consistency, and compliance.

Mandatory Employee Communication Standards (Employees Must):

1. **Policy Clarity and Accessibility:**
    - **Provide plain-language explanations of policies:** All communication regarding company policies, programs, and procedures must be conveyed in clear, accessible, and jargon-free language. Employees are responsible for ensuring that clients and stakeholders fully understand the information being presented, translating complex legal or technical terms into easily digestible concepts.

2. **Impartiality and Fair Assessment:**
    - **Avoid making eligibility assumptions:** Employees must maintain strict impartiality. Any communication about program eligibility or service suitability must be based *only* on a thorough review of documented facts and official policy criteria. Employees must not pre-judge, speculate, or make assumptions about a client's eligibility status or outcome before the formal assessment process is complete.
3. **Record Keeping and Accountability:**
    - **Document all client interactions in the Case Management System (CMS):** Every interaction with a client or relevant stakeholder—including phone calls, in-person meetings, emails, and any significant decision or advice provided—must be accurately and promptly recorded in the designated Case Management System (CMS). Documentation must be comprehensive, factual, time-stamped, and reflect the full context of the discussion to ensure continuity, audit compliance, and effective service tracking.

Prohibited Employee Communication Actions (Employees Must NOT):

1. **Advising Outside Scope of Practice:**
    - **Provide legal advice:** Employees are strictly prohibited from offering opinions, interpretations, or recommendations that constitute legal advice, including but not limited to, advising on legal rights, litigation strategy, or the specific application of external laws or regulations. If a legal question arises, employees must direct the client to seek independent legal counsel.
2. **Speculation and Unofficial Forecasts:**
    - **Speculate on future program changes:** Employees must not discuss, predict, or offer personal opinions regarding potential or rumored changes to company policies, services, or legislative frameworks. Communication must be limited to officially approved, current information. Any discussion of future changes must be sourced directly from and use the language approved by the Executive Office or Legal Department.
3. **Guaranteeing Outcomes:**
    - **Promise service outcomes not guaranteed by legislation:** Employees must never guarantee, imply, or promise a specific positive service result, benefit, or timeline that is not explicitly and formally guaranteed by current company policy or governing legislation. Communication should focus on process and effort, managing expectations realistically and within the defined scope of available programs and statutory limits.

5. Program Eligibility Rules for the Provincial Support for Client Security Program (PSCSP)

5.1 General Eligibility Criteria for Receiving PSCSP Support

To ensure the PSCSP resources are allocated effectively and appropriately, a client must satisfy all of the following criteria to be deemed eligible to receive support under the program. Strict adherence to these rules is mandatory for processing any application.

- **Established Residency Status:** The individual must be a bona fide resident as defined and stipulated under **Section 2 of the relevant Residency Regulation**. Proof of residency must be current and verifiable through accepted forms of documentation, such as a valid provincial ID, recent utility bills, or a lease agreement.
- **Alignment with Recognized Client Categories:** The applicant must clearly fall within one of the officially recognized client categories established for the program. These categories include, but are not limited to, **individual citizens**, certified **small businesses** operating within the jurisdiction, and registered **not-for-profit organizations** with a clear community mandate.
- **Timely Submission of Required Documentation:** The client is obligated to provide all necessary and requested supporting documentation, including verification of financial and situational need, **within thirty (30) calendar days of the formal application submission date**. Failure to meet this deadline will typically result in the application being closed and requiring a new submission.
- **Fulfillment of Financial or Situational Need:** The applicant must demonstrably meet the specific financial thresholds or situational criteria that establish the need for security support, as comprehensively defined and detailed in

Annex 4.1: Financial and Situational Criteria Matrix. This may involve income assessment, demonstration of a specific security vulnerability, or proof of a recent relevant incident.

5.2 Circumstances Leading to Program Ineligibility

The following conditions will result in an applicant being formally deemed ineligible for PSCSP support. These rules are in place to safeguard the integrity of the program and ensure compliance with provincial and federal statutes.

- **Failure to Meet Documentation Timelines:** An automatic declaration of ineligibility will occur if **required documents are not submitted within the established thirty-day timeline**. This rule is applied strictly to maintain efficient program processing.
- **Discovery of Fraudulent Information:** Any application found to contain **false, misleading, or fraudulent information** at any point during the review process or after funding is dispersed will result in immediate ineligibility, a request for the immediate return of any disbursed funds, and potential referral to the appropriate legal authorities for investigation.
- **Inability to Establish Legal Residency:** If the applicant's **residency cannot be definitively established** or verified according to the criteria outlined in Section 5.1, the application will be rejected on the grounds of ineligibility.
- **Conflict with Federal Jurisdictional Authority:** A client's request will be deemed ineligible if the nature or scope of the required support **falls under a federally regulated program or authority** that exists entirely outside the scope and mandate of the PSCSP. Staff are required to clearly identify the relevant federal program and inform the client.

5.3 Requirements for Ineligibility Notices

When a formal determination of ineligibility is made, the client must be notified promptly and in writing. The **Ineligibility Notice** must be clear, comprehensive, and include all of the following elements to ensure transparency and uphold due process:

- **Specific Rule Invoked:** The notice must clearly articulate **the exact section, subsection, and clause of the program policy or regulation that was violated or not met**, leading to the decision of ineligibility.
- **Detailed Appeal Rights:** The notice must explicitly outline the client's **rights to appeal the decision**, including the steps for initiating an appeal, the relevant deadlines, and the contact information for the appropriate review body or ombudsman.
- **Guidance on Further Actions:** The notice should provide information on **additional steps the client may take**, such as resubmitting a corrected application (if applicable), identifying alternative sources of support (e.g., federal programs), or guidance on rectifying the cause of ineligibility (e.g., submitting missing documents if the deadline has passed for the current application).

6. Privacy & Information Handling Requirements

This section establishes the mandatory protocols and standards for the collection, storage, access, and eventual disposal of all sensitive and non-sensitive information managed by employees, ensuring compliance with all relevant legislation, including the Comprehensive Information Protection Act (CIPA).

6.1 Collection Rules and Data Minimization

The principle of data minimization is central to all data collection activities:

- **Necessity and Proportionality (CIPA Section 7):** Employees are strictly required to collect *only* the minimum necessary data to achieve a specified and legitimate purpose. Any collection activity must be proportionate to the objective and directly relevant. Excess or non-essential data collection is strictly prohibited.
- **Explicit Consent for Sensitive Information:** Any data classified as sensitive (e.g., personal health information, financial data, or certain biometric identifiers) necessitates obtaining explicit, informed, and demonstrable consent from the client or data subject *prior* to collection. The scope, duration, and purpose of use must be clearly communicated during the consent process. Records of this consent must be maintained in the client file.
- **Approved Methods and Secure Channels:** All information, regardless of sensitivity, must be collected using officially approved digital forms, validated software applications, and secure, encrypted channels. Collection via unencrypted email, personal devices, or unapproved third-party tools is strictly forbidden to mitigate the risk of interception or compromise.

6.2 Storage, Access Control, and Data Integrity

The integrity and security of stored data are paramount and governed by strict protocols:

- **Mandatory Secure Document Repository (SDR) Storage:** All official records, documents, and data files must be uploaded and stored exclusively within the designated Secure Document Repository (SDR). Local or network drive storage is permissible only for temporary work-in-progress files, which must be moved to the SDR immediately upon completion. The SDR maintains continuous auditing and encryption standards.
- **Role-Based Access Control (RBAC):** Access to data within the SDR is strictly controlled via Role-Based Access Control (RBAC) matrices. Employees will only be granted access to data sets and records essential for their specific job functions. Access attempts, data retrievals, and modifications are logged automatically and monitored for anomalies.
- **Controlled Data Export Procedures:** The manual export of data from the SDR (e.g., to physical media, external drives, or unmanaged devices) requires prior management

approval. A comprehensive **justification note** must be filed with the team lead and retained for audit purposes, detailing the necessity, the data volume, the recipient, and the security measures applied to the exported data.

6.3 Breach Identification and Incident Procedures

In the event of a suspected or confirmed privacy breach (e.g., unauthorized access, loss, disclosure, or modification of data), immediate and systematic action must be taken:

1. **Immediate Notification (1-Hour Window):** The employee who first identifies or suspects a privacy breach must immediately notify the **Departmental Privacy Officer** via the designated emergency contact channel (phone or secure instant message) **within one (1) hour** of discovery. This is critical for activating the response chain.
2. **Detailed Incident Documentation:** All known details concerning the breach—including the time of discovery, the type of data compromised, the number of records affected, and the suspected vector of attack—must be meticulously documented in the official Incident Log. This log is the foundation for forensic analysis and mandatory reporting.
3. **Cessation of Data Processing:** All employees and systems related to the compromised data set must immediately cease all processing activities (including viewing, editing, transferring, or deleting) until the Privacy Officer and Incident Response Team authorize resumption. This action prevents further potential data leakage or corruption.
4. **Adherence to Containment Protocols:** Employees must fully cooperate and follow all established departmental containment procedures, which may include isolating affected systems, revoking temporary access credentials, and deploying forensic tools. The primary goal is to limit the scope of the breach and prevent further damage.

7. Appeals and Review Process7.1 Internal Review Mechanism

7.1.1 Client Right to Request Review

Any client who is dissatisfied with a decision, outcome, or service delivery has the right to request a formal internal review of their case. This request must be submitted in writing, detailing the grounds for the appeal and providing any relevant supporting documentation, within **30 calendar days** of the date the original decision or outcome was communicated to the client.

7.1.2 Review Timeline and Procedure

Upon receipt of a valid internal review request, the relevant department or designated internal review committee will undertake a thorough and impartial examination of the client's case and the original decision-making process. The internal review, including the communication of the final determination, must be completed and communicated back to the client within **20 business days** from the date the request was formally lodged. If the review cannot be completed within this timeframe, the client will be notified of the delay and provided with an estimated completion date.

7.2 Escalation to External Appeal Body

7.2.1 Unresolved Disputes

Should the client remain dissatisfied following the completion of the internal review process, or if the internal review was not completed within the stipulated timeframe, the client retains the right to escalate the unresolved dispute to an independent third-party adjudicative body. This external body is officially recognized as the **External Administrative Tribunal (EAT)**. The client must adhere to the EAT's own submission requirements and deadlines for external appeal.

7.2.2 Employee Guidance Scope

Employees of the organization are permitted and encouraged to provide clients with general information regarding the procedure for escalating their dispute to the External Administrative Tribunal (EAT), including directing them to the EAT's official submission guidelines and contact information. However, employees **must not** provide the client with any form of legal advice, interpretation of legal statutes, or opinions on the probable success or merits of the client's case before the EAT, as this falls outside the scope of their professional expertise and mandate.