

**ONTARIO TRANSFER PAYMENT AGREEMENT**  
Portable Housing Benefit – Special Priority Policy (PHB-SPP) Program

**THE AGREEMENT**, effective as of \_\_\_\_\_, 2018 (the “**Effective Date**”),

**B E T W E E N:**

**Her Majesty the Queen in right of Ontario as represented by  
the Minister of Housing (“MHO”) and the Minister of Finance (“MOF”)  
(collectively “Ontario”)  
- and -**

**The Corporation of the City of London**

(the “**Service Manager**” of “**SM**”)

**BACKGROUND**

The Service Manager has agreed to participate in the delivery and administration of the Portable Housing Benefit – Special Priority Policy (PHB-SPP) Program.

MHO wishes to provide Funds to the Service Manager for the Program.

**CONSIDERATION**

In consideration of the mutual covenants and agreements contained in this Agreement and for other good and valuable consideration, the receipt and sufficiency of which is expressly acknowledged, Ontario and the Service Manager (the “**Parties**”) agree as follows:

**1.0 ENTIRE AGREEMENT**

1.1 This agreement (the “**Agreement**”), including:

- Schedule “A” - General Terms and Conditions
- Schedule “B” - Program Specific Information and Additional Provisions
- Schedule “C” - Program Description and Timelines
- Schedule “D” - Program Guidelines
- Schedule “E” - Reporting
- Schedule “F” - Payment Plan
- Schedule “G” - Personal Information Sharing Provisions

any amending agreement entered into as provided for below, constitutes the entire agreement between the Parties with respect to the subject matter contained in this Agreement and supersedes all prior oral or written representations and agreements.

## **2.0 CONFLICT OR INCONSISTENCY**

2.1 **Conflict or Inconsistency.** In the event of a conflict or inconsistency between the Additional Provisions and the provisions in Schedule “A”, the following rules will apply:

- (a) the Parties will interpret any Additional Provisions in so far as possible, in a way that preserves the intention of the Parties as expressed in Schedule “A”, and
- (b) where it is not possible to interpret the Additional Provisions in a way that is consistent with the provisions in Schedule “A”, the Additional Provisions will prevail over the provisions in Schedule “A” to the extent of the inconsistency.

## **3.0 COUNTERPARTS**

3.1 The Agreement may be executed in any number of counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument.

## **4.0 AMENDING THE AGREEMENT**

4.1 Subject to the remainder of this section, the Agreement may only be amended by a written agreement duly executed by MHO and the Service Manager. MHO may amend the Program Guidelines from time to time by Notice to the Service Manager. If an amendment is to be made to Schedule “G” or is one that would affect MOF’s role or responsibilities under this Agreement, the amendment may only be made by a written amendment of MHO, MOF and the Service Manager, signed by persons occupying the positions of the signatories to the Agreement.

## **5.0 ACKNOWLEDGEMENT**

5.1 The Service Manager:

- (a) acknowledges that it has read and understands the provisions contained in the entire Agreement; and
- (b) agrees to be bound by the terms and conditions contained in the entire Agreement.

5.2 The Parties acknowledge that MHO and MOF have executed a Memorandum of Understanding under which MOF has agreed to provide services to assist MHO with the administration of the Program.

5.3 The Parties further acknowledge that it is not the responsibility of MOF to respond to Program enquiries and complaints from, including but not limited to, individuals, MPPs, municipal councillors, Office of the Ombudsman, the Human Rights Commission, and in

respect of any of any action, suit, prosecution or other legal proceedings related to the Program. In the case where the inquiry or complaint is received by MOF, it will be forwarded by MOF to the respective signatories for MHO and the SM as set out below.

**IN WITNESS WHEREOF**, the Parties have executed the Agreement on the dates set out below.

<b>HER MAJESTY THE QUEEN IN RIGHT OF ONTARIO as represented by the Minister of Housing</b>	
Name:	
Title:	
Date:	

<b>THE CORPORATION OF THE CITY OF LONDON</b>	
Name:	
Title:	
Date:	
Name:	
Title:	
Date:	

The Ministry of Finance agrees to and is bound by only the terms and conditions under Schedule “G” – Personal Information Sharing Provisions.

<b>MINISTRY OF FINANCE</b>	
Name:	
Title:	
Date:	

**SCHEDULE “A”**  
**GENERAL TERMS AND CONDITIONS**

---

**1.0 INTERPRETATION AND DEFINITIONS**

1.1 **Interpretation.** For the purposes of interpretation:

- (a) words in the singular include the plural and vice-versa;
- (b) words in one gender include all genders;
- (c) the headings do not form part of the Agreement; they are for reference only and will not affect the interpretation of the Agreement;
- (d) any reference to dollars or currency will be in Canadian dollars and currency; and
- (e) “include”, “includes” and “including” denote that the subsequent list is not exhaustive.

1.2 **Definitions.** In the Agreement, the following terms will have the following meanings:

“**Additional Provisions**” means the terms and conditions referred to in section 8.1 and as specified in Schedule “C”.

“**Agreement**” means this agreement entered into by MHO, MOF and the Service Manager, all of the Schedules listed in Section 1.1 of the main body of the Agreement, and any amendments made in accordance with the terms set out herein.

“**Benefit Period**” means each period for which MOF, on initial intake or annual reassessment, approves a participating Eligible SPP Household to receive a Monthly Benefit.

“**Business Day**” means any working day, Monday to Friday inclusive, excluding statutory and other holidays, namely: New Year’s Day; Family Day; Good Friday; Easter Monday; Victoria Day; Canada Day; Civic Holiday; Labour Day; Thanksgiving Day; Remembrance Day; Christmas Day; Boxing Day and any other day on which MHO has elected to be closed for business.

“**Eligible SPP Household**” means,

- (i) a household that:
  - (i) is participating in the SDV-PHB Pilot; and
  - (ii) has applied for a Monthly Benefit under the Program and provided all necessary information for the calculation of the benefit; or

- (ii) a household that:
  - (i) is on a social housing waiting list and has been included in the special priority household category under O. Reg. 367/11 under the HSA;
  - (ii) except in the case of an Interim Participant, has agreed to being removed from the social housing waiting list if it is approved for and begins to receive a Monthly Benefit; and
  - (iii) has applied for a Monthly Benefit under the Program and provided all necessary information for the calculation of the benefit.

**“Event of Default”** has the meaning ascribed to it in section 14.1.

**“Expiration Date”** means the date on which this Agreement will expire and is the date set out in Schedule “B”.

**“FIPPA”** means the Freedom of Information and Protection of Privacy Act.

**“Fiscal Year”** means:

- (a) in the case of the first Fiscal Year, the period commencing on the Effective Date and ending on the following March 31; and
- (b) in the case of Fiscal Years subsequent to the first Fiscal Year, the period commencing on April 1 following the end of the previous Fiscal Year and ending on the following March 31.

**“Funds”** means the money MHO provides to the Service Manager pursuant to the Agreement.

**“HSA”** means the Housing Services Act, 2011.

**“Indemnified Parties”** means Her Majesty the Queen in right of Ontario, Her ministers, agents, appointees and employees.

**“Interim Participant”** means a household participating in the SDV-PHB Pilot that chooses to participate in the Program only until June 30, 2019 so that it may be added back to or remain on the social housing waiting list as set out in the Program Guidelines.

**“Maximum Funds”** means the maximum amount MHO will provide the Service Manager under the Agreement as set out in Schedule “B”.

**“MFIPPA”** means the Municipal Freedom of Information and Protection of Privacy Act.

**“MOF”** means the Ministry of Finance.

**“Monthly Benefit”** means the monthly benefit calculated and paid to Program participants in accordance with the Program Guidelines.

**“Notice”** means any communication given or required to be given pursuant to the Agreement.

**“Notice Period”** means the period of time within which the Service Manager is required to remedy an Event of Default, and includes any such period or periods of time by which MHO considers it reasonable to extend that time.

**“Party”** means either MHO or the Service Manager.

**“Program”** means the Portable Housing Benefit – Special Priority Policy (PHB-SPP) Program described in Schedule “C” and the Program Guidelines.

**“Program Guidelines”** means the means the guidelines for the Program, including the Q’s and A’s, attached as Schedule “D” as amended by MHO from time to time.

**“Reports”** means the reports described in Schedule “E”.

**“SDV-PHB Pilot”** means the Survivors of Domestic Violence Portable Housing Benefit Pilot that was launched in September 2016 and that ends on June 30, 2018.

## **2.0 REPRESENTATIONS, WARRANTIES AND COVENANTS**

**2.1 General.** The Service Manager represents, warrants and covenants that:

- (a) it has full power to fulfill its obligations under the Agreement;
- (b) it has, and will continue to have for the term of the Agreement, the experience and expertise necessary to carry out the Program;
- (c) it is in compliance, and will continue to comply with, all federal and provincial laws and regulations, all municipal by-laws, and any other orders, rules and by-laws related to any aspect of the Program, the Funds or both; and
- (d) unless otherwise provided for in the Agreement, any information the Service Manager provided to MHO in support of its request for funds (including information relating to any eligibility requirements) was true and complete at the time the Service Manager provided it and will continue to be true and complete for the term of the Agreement.

**2.2 Execution of Agreement.** The Service Manager represents and warrants that it has:

- (a) the full power and authority to enter into the Agreement; and
- (b) taken all necessary actions (including the adoption of any authorizing by-law) to authorize the execution of the Agreement.

2.3 **Governance.** The Service Manager represents, warrants and covenants that it has, and will maintain, in writing for the period during which the Agreement is in effect:

- (a) a code of conduct and ethical responsibilities for all persons at all levels of the Service Manager's organization;
- (b) procedures to ensure the ongoing effective functioning of the Service Manager;
- (c) decision-making mechanisms for the Service Manager;
- (d) procedures to enable the Service Manager to manage Funds prudently and effectively;
- (e) procedures to enable the Service Manager to complete the Program successfully;
- (f) procedures to enable the Service Manager, in a timely manner, to identify risks to the completion of the Program, and strategies to address the identified risks;
- (g) procedures to enable the preparation and delivery of all Reports required pursuant to Article 6.0; and
- (h) procedures to enable the Service Manager to deal with such other matters as the Service Manager considers necessary to ensure that the Service Manager carries out its obligations under the Agreement.

2.4 **Supporting Documentation.** Upon request, the Service Manager will provide MHO with proof of the matters referred to in this Article 2.0.

### 3.0 **TERM OF THE AGREEMENT**

3.1 **Term.** The term of the Agreement will commence on the Effective Date and will expire on the Expiration Date unless terminated earlier pursuant to Article 12.0, Article 13.0 or Article 14.0.

### 4.0 **FUNDS AND CARRYING OUT THE PROGRAM**

4.1 **Funds Provided.** MHO will:

- (a) provide the Service Manager up to the Maximum Funds for the purpose of assisting with the delivery and administration of the Program;
- (b) subject to adjustment in accordance with this Agreement, provide the Funds to the Service Manager in accordance with the Payment Plan set out in Schedule "F"; and
- (c) deposit the Funds into a separate account designated by the Service Manager provided that the account:
  - (i) resides at a Canadian financial institution; and

(ii) is in the name of the Service Manager.

4.1.1 **Adjustment.** Despite section 4.1, in order to more accurately reflect the Service Manager's need for Funds, MHO may adjust the amount of the Funds to be provided, and any instalment of Funds, based upon the information provided by MOF to MHO in accordance with Schedule "F".

4.2 **Limitation on Payment of Funds.** Despite section 4.1:

- (a) MHO is not obligated to provide any Funds to the Service Manager until the Service Manager provides the insurance certificate or other proof as MHO may request pursuant to section 11.2;
- (b) MHO is not obligated to provide instalments of Funds until it is satisfied with the progress of the Program;
- (c) MHO may adjust the amount of Funds it provides to the Service Manager in any Fiscal Year based upon MHO's assessment of the information provided by the Service Manager pursuant to section 6.1; and
- (d) if, pursuant to the *Financial Administration Act* (Ontario), MHO does not receive the necessary appropriation from the Ontario Legislature for payment under the Agreement, MHO is not obligated to make any such payment, and, as a consequence, MHO may:
  - (i) reduce the amount of Funds and, in consultation with the Service Manager, change the Program; or
  - (ii) terminate the Agreement pursuant to section 13.1.

4.3 **Use of Funds.** The Service Manager will:

- (a) administer and deliver the Program in accordance with the terms and conditions of this Agreement, including Schedule "C", Schedule "G" and the Program Guidelines;
- (b) use the Funds only for the purpose of administering and delivering the Program;
- (c) spend the Funds only in accordance with Schedule "C";
- (d) spend Funds provided for administration costs only on the costs of administering the Program;
- (e) use the Funds provided for first and last months' rent only to reimburse the Service Manager for funds paid to Eligible SPP Households that:
  - (i) are approved by MOF for a Monthly Benefit;



- (ii) are approved by the Service Manager for a contribution towards first and last months' rent based on demonstrated need; and
- (iii) were not participants under the SDV-PHB Pilot; and
- (f) not use the Funds to cover any specific cost that has or will be funded or reimbursed by any third party, including other ministries, agencies and organizations of the Government of Ontario.

4.4. **No Changes.** The Service Manager will not make any changes to the Program that are contrary to those in Schedule "C" and the Program Guidelines without the prior written consent of MHO.

4.5 **Interest Bearing Account.** If MHO provides Funds to the Service Manager before the Service Manager's immediate need for the Funds, the Service Manager will place the Funds in an interest bearing account in the name of the Service Manager at a Canadian financial institution.

4.6 **Interest.** If the Service Manager earns any interest on the Funds, MHO may:

- (a) deduct an amount equal to the interest from any further instalments of Funds; or
- (b) demand from the Service Manager the repayment of an amount equal to the interest.

4.7 **Maximum Funds.** The Service Manager acknowledges that the Funds available to it pursuant to the Agreement will not exceed the Maximum Funds.

4.8 **Rebates, Credits and Refunds.** The Service Manager acknowledges that the amount of Funds available to it pursuant to the Agreement is based on the actual costs to the Service Manager, less any costs (including taxes) for which the Service Manager has received, will receive, or is eligible to receive, a rebate, credit or refund.

4.9 **Funding, Not Procurement.** For greater clarity, the Service Manager acknowledges that it is receiving funding from MHO for the Program and is not providing goods or services to MHO.

4.10 **Program Over Budget.** The Service Manager acknowledges that should the Service Manager's Program expenses exceed the amount of the Funds, MHO is not responsible for any additional funding and the Service Manager undertakes to incur all further costs necessary to carry out its responsibilities under the Program.

## 5.0 CONFLICT OF INTEREST

5.1 **No Conflict of Interest.** The Service Manager will administer and deliver the Program and use the Funds without an actual, potential or perceived conflict of interest.

5.2 **Conflict of Interest Includes.** For the purposes of this Article, a conflict of interest includes any circumstances where:

- (a) the Service Manager; or
- (b) any person who has the capacity to influence the Service Manager's decisions, has outside commitments, relationships or financial interests that could, or could be seen to, interfere with the Service Manager's objective, unbiased and impartial judgment relating to the Program, the use of the Funds, or both.

5.3 **Disclosure to MHO.** The Service Manager will:

- (a) disclose to MHO, without delay, any situation that a reasonable person would interpret as an actual, potential or perceived conflict of interest; and
- (b) comply with any terms and conditions that MHO may prescribe as a result of the disclosure.

## 6.0 **REPORTING, ACCOUNTING AND REVIEW**

6.1 **Preparation and Submission.** The Service Manager will:

- (a) submit to MHO at the address referred to in section 18.1, all Reports in accordance with the timelines and content requirements set out in Schedule "E", or in a form as specified by MHO from time to time;
- (b) submit to MHO at the address referred to in section 18.1, any other reports as may be requested by MHO in accordance with the timelines and content requirements specified by MHO;
- (c) ensure that all Reports and other reports are completed to the satisfaction of MHO; and
- (d) ensure that all Reports and other reports are signed on behalf of the Service Manager by an authorized signing officer.

6.2 **Record Maintenance.** The Service Manager will keep and maintain:

- (a) all financial records (including invoices) relating to the Funds or otherwise to the Program in a manner consistent with generally accepted accounting principles; and
- (b) all non-financial documents and records relating to the Funds or otherwise to the Program.

6.3 **Inspection.** MHO, its authorized representatives or an independent auditor identified by MHO may, at its own expense, upon twenty-four hours' Notice to the Service

Manager and during normal business hours, enter upon the Service Manager's premises to review the progress of the Program and the Service Manager's allocation and expenditure of the Funds and, for these purposes, MHO, its authorized representatives or an independent auditor identified by MHO may take one or more of the following actions:

- (a) inspect and copy the records and documents referred to in section 6.2;
- (b) remove any copies made pursuant to section 6.3(a) from the Service Manager's premises; and
- (c) conduct an audit or investigation of the Service Manager in respect of the expenditure of the Funds and/or the Program.
- (d) MHO may conduct an annual audit in respect of the information addressed in this section 6.3.

6.4 **Disclosure.** To assist in respect of the rights set out in section 6.3, the Service Manager will disclose any information requested by MHO, its authorized representatives or an independent auditor identified by MHO, and will do so in the form requested by MHO, its authorized representatives or an independent auditor identified by MHO, as the case may be.

6.5 **No Control of Records.** No provision of the Agreement will be construed so as to give MHO any control whatsoever over the Service Manager's records.

6.6 **Auditor General.** For greater certainty, MHO's rights under this Article are in addition to any rights provided to the Auditor General pursuant to section 9.1 of the *Auditor General Act* (Ontario).

## 7.0 COMMUNICATIONS REQUIREMENTS

7.1 **Acknowledge Support.** Unless otherwise directed by MHO, the Service Manager will acknowledge the support of MHO in a form and manner as directed by MHO.

7.2 **Publication.** The Service Manager will indicate, in any of its Program-related publications, whether written, oral, or visual, that the views expressed in the publication are the views of the Service Manager and do not necessarily reflect those of MHO.

## **8.0 FURTHER CONDITIONS**

- 8.1 **Additional Provisions.** The Service Manager will comply with any Additional Provisions.
- 8.2 **Open Data.** The Service Manager agrees that MHO may publicly release the following information, whether in hard copy or in electronic form, on the internet or otherwise: Service Manager name, Service Manager contact information, Service Manager address, amount of Maximum Funds and/or Funds, Program description, Program objectives/goals, Program location, and Program results reported by the Service Manager. However, MHO and the Service Manager agree that such permission does not apply to the personal information of individuals in Eligible SPP Households.
- 8.3 **Announcements.** The Service Manager shall not publicly announce receiving the Funds or anything to do with the Agreement, including requesting the presence of the Minister of Housing at one or more Program events, until permitted by MHO.

## **9.0 FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY**

- 9.1 **FIPPA.** The Service Manager acknowledges that MHO and MOF are bound by FIPPA and that any information provided to MHO and MOF in connection with the Program or otherwise in connection with the Agreement may be subject to disclosure in accordance with that Act.
- 9.2 **MFIPPA.** MHO and MOF acknowledge that the Service Manager is bound by MFIPPA and that any information provided to the Service Manager in connection with the Program or otherwise in connection with the Agreement may be subject to disclosure in accordance with that Act.

## **10.0 INDEMNITY**

- 10.1 **Indemnification.** The Service Manager hereby agrees to indemnify and hold harmless the Indemnified Parties from and against any and all liability, loss, costs, damages and expenses (including legal, expert and consultant fees), causes of action, actions, claims, demands, lawsuits or other proceedings, by whomever made, sustained, incurred, brought or prosecuted, in any way arising out of or in connection with the Program or otherwise in connection with the Agreement, unless solely caused by the negligence or wilful misconduct of MHO.

## **11.0 INSURANCE**

- 11.1 **Service Manager's Insurance.** The Service Manager represents and warrants that it has, and will maintain for the term of the Agreement, at its own cost and expense, with insurers having a secure A.M. Best rating of B+ or greater, or the equivalent, all the necessary and appropriate insurance that a prudent person carrying out a Program similar to the Program would maintain, including commercial general liability insurance

on an occurrence basis for third party bodily injury, personal injury and property damage, to an inclusive limit of not less than the amount set out in Schedule “B” per occurrence. The policy will include the following:

- (a) the Indemnified Parties as additional insureds with respect to liability arising in the course of performance of the Service Manager’s obligations under, or otherwise in connection with, the Agreement;
- (b) a cross-liability clause;
- (c) contractual liability coverage; and
- (d) a 30 day written notice of cancellation.

11.2 **Proof of Insurance.** The Service Manager will provide MHO with certificates of insurance, or other proof as may be requested by MHO, that confirms the insurance coverage as provided for in section 11.1. Upon the request of MHO, the Service Manager will make available to MHO a copy of each insurance policy.

## 12.0 TERMINATION ON NOTICE

12.1 **Termination on Notice.** MHO may terminate the Agreement at any time without liability, penalty or costs upon giving at least 30 days’ Notice to the Service Manager.

12.2 **Consequences of Termination on Notice by MHO.** If MHO terminates the Agreement pursuant to section 12.1, MHO may take one or more of the following actions:

- (a) cancel further instalments of Funds;
- (b) demand the repayment of any Funds remaining in the possession or under the control of the Service Manager; and
- (c) determine the reasonable costs for the Service Manager to wind down the Program, and do either or both of the following:
  - (i) permit the Service Manager to offset such costs against the amount owing pursuant to section 12.2(b); and
  - (ii) subject to section 4.8, provide Funds to the Service Manager to cover such costs.

## 13.0 TERMINATION WHERE NO APPROPRIATION

13.1 **Termination Where No Appropriation.** If, as provided for in section 4.2(d), MHO does not receive the necessary appropriation from the Ontario Legislature for any payment MHO is to make pursuant to the Agreement, MHO may terminate the

Agreement immediately without liability, penalty or costs by giving Notice to the Service Manager.

**13.2 Consequences of Termination Where No Appropriation.** If MHO terminates the Agreement pursuant to section 13.1, MHO may take one or more of the following actions:

- (a) cancel further instalments of Funds;
- (b) demand the repayment of any Funds remaining in the possession or under the control of the Service Manager; and
- (c) determine the reasonable costs for the Service Manager to wind down the Program and permit the Service Manager to offset such costs against the amount owing pursuant to section 13.2(b).

**13.3 No Additional Funds.** For greater clarity, if the costs determined pursuant to section 13.2(c) exceed the Funds remaining in the possession or under the control of the Service Manager, MHO will not provide additional Funds to the Service Manager.

#### **14.0 EVENT OF DEFAULT, CORRECTIVE ACTION AND TERMINATION FOR DEFAULT**

**14.1 Events of Default.** It will constitute an Event of Default if, in the opinion of MHO, the Service Manager breaches any representation, warranty, covenant or other material term of this Agreement, including failing to do any of the following in accordance with the terms and conditions of the Agreement:

- (a) administer and deliver the Program in accordance with this Agreement;
- (b) comply with its obligations set out in Schedule "C";
- (c) use or spend Funds only as authorized herein; or
- (d) provide, in accordance with section 6.1, Reports or such other reports as may have been requested pursuant to section 6.1(b).

**14.2 Consequences of Events of Default and Corrective Action.** If an Event of Default occurs, MHO may, at any time, take one or more of the following actions:

- (a) initiate any action MHO considers necessary in order to facilitate the successful continuation or completion of the Program;
- (b) provide the Service Manager with an opportunity to remedy the Event of Default;
- (c) suspend the payment of Funds for such period as MHO determines appropriate;
- (d) reduce the amount of the Funds;

- (e) cancel further instalments of Funds;
- (f) demand from the Service Manager the repayment of any Funds remaining in the possession or under the control of the Service Manager;
- (g) demand from the Service Manager the repayment of an amount equal to any Funds the Service Manager used, but did not use in accordance with the Agreement;
- (h) demand from the Service Manager the repayment of an amount equal to any Funds MHO provided to the Service Manager; and
- (i) terminate the Agreement at any time, including immediately, without liability, penalty or costs to MHO upon giving Notice to the Service Manager.

**14.3 Opportunity to Remedy.** If, in accordance with section 14.2(b), MHO provides the Service Manager with an opportunity to remedy the Event of Default, MHO will provide Notice to the Service Manager of:

- (a) the particulars of the Event of Default; and
- (b) the Notice Period.

**14.4 Service Manager not Remediating.** If MHO has provided the Service Manager with an opportunity to remedy the Event of Default pursuant to section 14.2(b), and:

- (a) the Service Manager does not remedy the Event of Default within the Notice Period;
- (b) it becomes apparent to MHO that the Service Manager cannot completely remedy the Event of Default within the Notice Period; or
- (c) the Service Manager is not proceeding to remedy the Event of Default in a way that is satisfactory to MHO,

MHO may extend the Notice Period, or initiate any one or more of the actions provided for in sections 14.2(a), (c), (d), (e), (f), (g), (h) and (i).

**14.5 When Termination Effective.** Termination under this Article will take effect as set out in the Notice.

## **15.0 FUNDS AT THE END OF A FISCAL YEAR**

**15.1 Funds at the End of a Fiscal Year.** Without limiting any rights of MHO under Article 14.0, if the Service Manager has not spent all of the Funds provided to it for the Fiscal Year, MHO may take one or both of the following actions:

- (a) demand from the Service Manager the return of the unspent Funds; and
- (b) adjust the amount of any further instalments of Funds accordingly.

For greater certainty, the Service Manager may not carry Funds over from one Fiscal Year to the next. Should a planned commitment for Funds under the Program fall through, the Funds may only be recommitted and spent within the same Fiscal Year.

## **16.0 FUNDS UPON EXPIRY**

**16.1 Funds Upon Expiry.** The Service Manager will, upon expiry of the Agreement, return to MHO any Funds remaining in its possession or under its control.

## **17.0 DEBT DUE AND PAYMENT**

**17.1 Payment of Overpayment.** If at any time during the term of the Agreement, MHO provides Funds in excess of the amount to which the Service Manager is entitled under the Agreement, MHO may:

- (a) deduct an amount equal to the excess Funds from any further instalments of Funds; or
- (b) demand that the Service Manager pay an amount equal to the excess Funds to MHO.

**17.2 Debt Due.** If, pursuant to the Agreement:

- (a) MHO demands from the Service Manager the payment of any Funds or an amount equal to any Funds from the Service Manager; or
- (b) the Service Manager owes any Funds or an amount equal to any Funds to MHO, whether or not their return or repayment has been demanded by MHO,

such Funds or other amount will be deemed to be a debt due and owing to MHO by the Service Manager, and the Service Manager will pay or return the amount to MHO immediately, unless MHO directs otherwise.

**17.3 Interest Rate.** MHO may charge the Service Manager interest on any money owing by the Service Manager at the then current interest rate charged by MHO of Ontario on accounts receivable.

**17.4 Payment of Money to MHO.** The Service Manager will pay any money owing to MHO by cheque payable to the "Ontario Minister of Finance" and delivered to MHO at the address referred to in section 18.1.

**17.5 Failure to Repay.** Without limiting the application of section 43 of the *Financial Administration Act* (Ontario), if the Service Manager fails to repay any amount owing



under the Agreement, Her Majesty the Queen in right of Ontario may deduct any unpaid amount from any money payable to the Service Manager by Her Majesty the Queen in right of Ontario.

## **18.0 NOTICE**

18.1 **Notice in Writing and Addressed.** Notice will be in writing and will be delivered by email, postage-prepaid mail, personal delivery or fax, and will be addressed to MHO and the Service Manager respectively as set out in Schedule “B”, or as either Party later designates to the other by Notice.

18.2 **Notice Given.** Notice will be deemed to have been given:

- (a) in the case of postage-prepaid mail, five Business Days after the Notice is mailed; or
- (b) in the case of email, personal delivery or fax, one Business Day after the Notice is delivered.

18.3 **Postal Disruption.** Despite section 18.2(a), in the event of a postal disruption:

- (a) Notice by postage-prepaid mail will not be deemed to be received; and
- (b) the Party giving Notice will provide Notice by email, personal delivery or by fax.

18.4 **Notice by MHO.** The Service Manager will comply with all Notices given by MHO.

## **19.0 CONSENT BY MHO AND COMPLIANCE BY SERVICE MANAGER**

19.1 **Consent.** When MHO provides its consent pursuant to the Agreement, it may impose any terms and conditions on such consent and the Service Manager will comply with such terms and conditions.

## **20.0 SEVERABILITY OF PROVISIONS**

20.1 **Invalidity or Unenforceability of Any Provision.** The invalidity or unenforceability of any provision of the Agreement will not affect the validity or enforceability of any other provision of the Agreement. Any invalid or unenforceable provision will be deemed to be severed.

## **21.0 WAIVER**

21.1 **Waivers in Writing.** Either Party may, in accordance with the Notice provision set out in Article A18.0, ask the other Party to waive an obligation under the Agreement.

21.2 **Waiver Applies.** Any waiver a Party grants in response to a request made pursuant to section A21.1 will:

- (a) be valid only if the Party granting the waiver provides it in writing; and

(b) apply only to the specific obligations referred to in the waiver.

## **22.0 INDEPENDENT PARTIES**

22.1 **Parties Independent.** The Service Manager acknowledges that it is not an agent, joint venturer, partner or employee of MHO, and the Service Manager will not represent itself in any way that might be taken by a reasonable person to suggest that it is, or take any actions that could establish or imply such a relationship.

## **23.0 ASSIGNMENT OF AGREEMENT OR FUNDS**

23.1 **No Assignment.** The Service Manager will not, without the prior written consent of MHO, assign any of its rights, or obligations under the Agreement.

23.2 **Agreement Binding.** All rights and obligations contained in the Agreement will extend to and be binding on the Parties' respective heirs, executors, administrators, successors and permitted assigns.

## **24.0 GOVERNING LAW**

24.1 **Governing Law.** The Agreement and the rights, obligations and relations of the Parties will be governed by and construed in accordance with the laws of the Province of Ontario and the applicable federal laws of Canada. Any actions or proceedings arising in connection with the Agreement will be conducted in the courts of Ontario, which will have exclusive jurisdiction over such proceedings.

## **25.0 FURTHER ASSURANCES**

25.1 **Agreement into Effect.** The Service Manager will provide such further assurances as MHO may request from time to time with respect to any matter to which the Agreement pertains, and will otherwise do or cause to be done all acts or things necessary to implement and carry into effect the terms and conditions of the Agreement to their full extent.

## **26.0 RIGHTS AND REMEDIES CUMULATIVE**

26.1 **Rights and Remedies Cumulative.** The rights and remedies of MHO under the Agreement are cumulative and are in addition to, and not in substitution for, any of its rights and remedies provided by law or in equity.

## **27.0 FAILURE TO COMPLY WITH OTHER AGREEMENTS**

27.1 **Other Agreements.** If the Service Manager:

- (a) has failed to comply (a "**Failure**") with any term, condition or obligation under any other agreement with Her Majesty the Queen in right of Ontario or one of Her agencies;
- (b) has been provided with notice of such Failure in accordance with the requirements of such other agreement;

- (c) has, if applicable, failed to rectify such Failure in accordance with the requirements of such other agreement; and
- (d) such Failure is continuing,

MHO may suspend the payment of Funds for such period as MHO determines appropriate.

## **28.0 SURVIVAL**

28.1 **Survival.** The following Articles and sections, and all applicable cross-referenced sections and schedules, will continue in full force and effect for a period of seven years from the date of expiry or termination of the Agreement: Article 5 of the main body of the Agreement; Article 1.0 and any other applicable definitions, section 4.2(d), sections 4.3, 4.6, 4.7 and 4.10, Article 5, section 6.1 (to the extent that the Service Manager has not provided the Reports to the satisfaction of MHO), sections 6.2, 6.3, 6.4, 6.5, 6.6, Article 7.0, Article 8.0, Article 10, Article 11.0, section 12.2, sections 13.2 and 13.3, sections 14.1, 14.2 (a), (d), (e), (f), (g) and (h), Article 16.0, Article 17.0, Article 18.0, Article 20.0, section 23.2, Article 24.0, Article 26.0, Article 27.0, Article 28.0 and Article 29.0 of Schedule “A”; the use of Funds provisions of Schedule “C” and Articles 4 and 6 of Schedule “G”.

## **29.0 PERSONAL INFORMATION AND PARTICIPATION BY MINORS**

- 29.1 **Permissions.** The Service Manager represents warrants and covenants that it has or will receive permission to disclose the personal information of all individuals whose personal information is disclosed during the Program and/or in Reports or other reports, and, in the case of minors, the legal guardian or parent has provided such permission on behalf of the minor.
- 29.2 **Consent of Legal Guardian.** The Service Manager acknowledges that it is the responsibility of the Service Manager to obtain express written consent from the legal guardian of any minors who are involved in any way with the Program.

**- END OF GENERAL TERMS AND CONDITIONS -**

## SCHEDULE "B"

### PROGRAM SPECIFIC INFORMATION AND ADDITIONAL PROVISIONS

<b>Maximum Funds</b>	<p>For the first Fiscal Year of the Program, the lesser of the amount MHO determines to be payable in accordance with Schedule "F" for the Fiscal Year and \$3 million.</p> <p>For subsequent Fiscal Years of the Program, the lesser of the amount MHO determines to be payable in accordance with Schedule "F" for the Fiscal Year and \$2 million.</p> <p>Funds are also subject to availability and an overall Program maximum of \$10 million the first Fiscal Year of the Program and \$15 million in subsequent Fiscal Years of the Program.</p>
<b>Expiration Date</b>	<p>Subject to the termination rights in the Agreement, the date indicated in a Notice provided by the MHO to the Service Manager as being the Expiry Date.</p>
<b>Insurance</b>	<p>\$ 2,000,000.00</p>
<b>Contact information for the purposes of Notice to MHO</b>	<p>Name: Director, Housing Programs Branch, Housing Division</p> <p>Address: 777 Bay Street, 14<sup>th</sup> Floor, Toronto, Ontario, M5G 2E5</p> <p>Fax: 416-585-6588</p> <p>Email: <a href="mailto:Housing.Program.MAH@ontario.ca">Housing.Program.MAH@ontario.ca</a></p>
<b>Contact information for the purposes of Notice to the Service Manager</b>	<p>Name: Sandra Datars Bere</p> <p>Position: Managing Director, Housing, Social Services and Dearness Home</p> <p>Address: 355 Wellington Street, 2nd floor, London, ON N6A 3N7</p> <p>Attention: Sandra Datars Bere</p> <p>Fax: 519-661-4466</p> <p>Email: <a href="mailto:sdatarsb@london.ca">sdatarsb@london.ca</a></p> <p>Telephone: 519-661-2489 ext 5337</p>

<b>Contact information for the senior financial person in the Service Manager organization (e.g., CFO, CAO) to respond as required to requests from MHO related to the Agreement</b>	Name: Dave Purdy Position: Manager, Housing Services Address: 355 Wellington St. Suite 248, 2nd Floor, London ON N6A 3N7 Fax: 519-661-4466 Email: <a href="mailto:dpurdy@london.ca">dpurdy@london.ca</a> Telephone: 519-661-2489 ext 5596
--	--

Additional Provisions relating to the Program are set out in Schedule "C".

## SCHEDULE “C”

### PROGRAM DESCRIPTION AND TIMELINES

---

#### C.1 BACKGROUND

The Portable Housing Benefit – Special Priority Policy (PHB-SPP) Program will provide up to \$10 million in 2018-19 and up to \$15 million in 2019-20, and ongoing, for housing assistance for, among others, households included in the special priority category under the Housing Services Act, 2011.

The Program is to be administered and delivered by the Ministry of Housing, with assistance from the Service Manager and the Ministry of Finance.

Through the Program, the Ministry of Housing aims to provide SPP households with additional options to meet their housing needs and alleviate pressure on the social housing system. Instead of staying in shelters or other precarious housing situations until a social housing unit becomes available, this Program would provide survivors of domestic violence or human trafficking with the option to receive a portable housing benefit so they can quickly find housing in their community.

A portable housing benefit is a subsidy provided to a low-income household to help with housing costs. The subsidy gives a household the freedom to choose where to live since it is not tied to a specific unit like most rent-geared-to-income social housing. The Ministry of Finance will provide the portable housing benefit directly to the person who applies for the benefit on behalf of the SPP household or their landlord.

#### C.2 PROGRAM OBJECTIVE

The Program has three objectives:

- To increase support for those experiencing domestic violence or human trafficking to obtain and retain housing;
- To decrease wait times for housing assistance for SPP households on the chronological wait list for social housing and others who have participated in the SDV-PHB Pilot; and
- To expand housing choice for SPP households.

#### C.3 SCOPE OF PROGRAM

##### 1.0 DEFINITIONS

1.1 In this Schedule, capitalized terms have the meaning given to them in Schedule “A” and the following terms have the following meanings:

“**Adjusted Family Net Income**” has the meaning given to it under the Program Guidelines.

**“Applicant”** means a household that the Service Manager confirms as qualifying under the definition of “Eligible SPP Household” as set out in Schedule “A” to this Agreement.

**“Application Form”** means an application form for the Program in the form provided to the Service Manger by MHO.

**“Renewal Form”** means an application form to be completed by Program participants in each Benefit Period following the initial Benefit Period in order to continue to receive a Monthly Benefit.

**“ServiceOntario”** means the part of the Ministry of Government and Consumer Services that is designated under section 1 of O. Reg. 475/07 under the the Ministry of Government Services Act as a service provider organization.

## **2.0 RESPONSIBILITIES OF MHO**

- 2.1 MHO shall be responsible for overall Program policy and shall carry out the Program as set out in the Program Guidelines and Schedule “G”.
- 2.2 MHO shall be responsible for obtaining the services to be provided by MOF to assist with Program administration.

## **3.0 RESPONSIBILITIES OF THE SERVICE MANAGER**

- 3.1 During the term of the Agreement, the Service Manager will:
  - (a) comply with, administer and deliver the Program in accordance with this Agreement, including the Program Guidelines;
  - (b) provide information about the Program, including Program requirements under the Program Guidelines, and distribute initial Application Forms to:
    - (i) households on their social housing waiting list that have been included in the special priority household category under O. Reg. 367/11 under the HSA; and
    - (ii) households that are participating in the SDV-PHB Pilot.
  - (c) ensure that all Applicants comply with the criteria set out in the definition of “Eligible SPP Household”;
  - (d) assist Applicants with filling out their Application Forms for the initial Benefit Period;
  - (e) if requested by Applicants, collect and send completed Application Forms to MOF for processing for the initial Benefit Period;
  - (f) with the exception of Interim Participants, ensure that all Eligible SPP Households who are on their social housing waiting list consent to being

removed from and are removed from the list if the household is approved for and begins to receive a Monthly Benefit;

- (g) provide funding for first and last months' rent calculated in accordance with Schedule "F" to Eligible SPP Households that:
  - (i) are approved by MOF for a Monthly Benefit;
  - (ii) are approved by the Service Manager for a contribution towards first and last months' rent based on demonstrated need; and
  - (iii) were not participants under the SDV-PHB Pilot;
- (h) for Applicants entering the Program who have not filed income tax return(s); whose most recent income tax return(s) do not reflect the household's current financial circumstances,
  - (i) calculate the household's Adjusted Family Net Income,
  - (ii) facilitate an income tax verification exemption for the Applicant, and
  - (iii) verify each household member's net income using the best available information,

all as required under the Program Guidelines;

- (i) promptly communicate the results of any calculation and verification under clause (h) to MOF;
- (j) inform all participating Eligible SPP Households that they must complete a Renewal Form prior to each annual review, file all required income tax returns each year by April 30, and qualify to continue to receive a Monthly Benefit each year in accordance with the Program Guidelines;
- (k) inform all participating Eligible SPP Households of the ongoing eligibility criteria under the Program Guidelines;
- (l) inform all participating Eligible SPP Households that they must provide ServiceOntario with notice of the following within 30 days of the date on which they occur:
  - (i) any permanent change in household composition;
  - (ii) any change of address;
  - (iii) if a member of household begins to receive or stops receiving assistance under the Ontario Works Act, 1997 or the Ontario Disability Support Program Act, 1997,
  - (iv) any acceptance of a rent-geared-to-income unit;



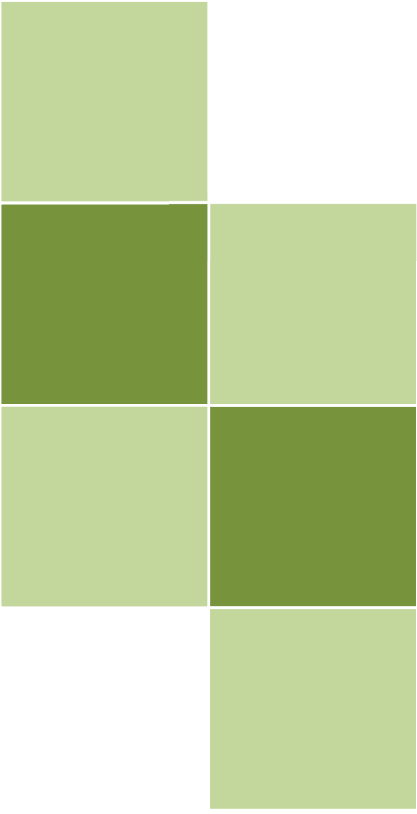
- (v) any acceptance of another government funded housing benefit;
  - (vi) any failure to dispose of a home suitable for year-round occupancy (within or outside Ontario) in accordance with the Program Guidelines;
  - (vii) any acceptance of basic income under the Ontario Basic Income Pilot;
  - (viii) ceasing to be a renter household.
- (m) inform all participating Eligible SPP Households that they must provide ServiceOntario with notice of any request for an in-year reassessment;
  - (n) assist MHO and MOF with the development of Program materials, such as application forms, letters and communication materials;
  - (o) complete and distribute T5007 tax forms (Statement of Benefits) to participants who received first and last month's rent assistance; and,
  - (p) participate in the Program evaluation as directed by MHO.

#### **4.0 USE OF FUNDS**

4.1 The Service Manager shall use the Funds solely as follows:

- (a) All Funds provided for first and last month's rent must be used to reimburse the Service Manager for funds paid to an Eligible SPP Household that:
  - (i) is approved by MOF for a Monthly Benefit;
  - (ii) is approved by the Service Manager for a contribution towards first and last months' rent based on demonstrated need; and
  - (iii) was not a participant under the SDV-PHB Pilot;
- (b) All Funds provided for administration costs must be used to offset Program administration costs.

**SCHEDULE "D"**  
**PROGRAM GUIDELINES**  
**SEE ATTACHED**



# Portable Housing Benefit - Special Priority Policy (PHB-SPP)

Program Guidelines



# TABLE OF CONTENTS

List of Acronyms.....	1
Highlights .....	2
Introduction .....	3
Scope of the Guidelines .....	3
Provincial Context.....	3
Program Description.....	6
Objectives .....	6
Outcomes .....	6
Funding.....	6
Timeframe.....	7
Eligibility Criteria: Applicants .....	7
Eligibility Criteria: Ongoing .....	8
Portability .....	9
Program Delivery .....	10
SDV-PHB Pilot Program (2016-2018) Recipients .....	10
Application and Annual Renewal Process.....	11
Service Level Standards.....	12
Payments to Applicants.....	13
Calculation of Portable Housing Benefit.....	13
Interaction with Social Assistance .....	15
Automated Income Verification .....	15
Exemption from Automated Income Verification .....	16
First and Last Month's Rent.....	16
In-Year Changes .....	16
Monthly Payments .....	17
Direct Deposit .....	18
T5007 Tax Forms .....	18
Accountability and Reporting.....	19
Memoranda of Understanding .....	19
Transfer Payment Agreements.....	19
Quarterly Reports .....	19
French Language Services Act Compliance .....	20
Roles and Responsibilities .....	20
Important Dates.....	22
Appendix A: Ministry of Housing Contacts .....	23
Appendix B: Ministry of Community and Social Services Contacts .....	25

## **LIST OF ACRONYMS**

- AFNI – adjusted family net income
- AMR – Average Market Rent
- CMHC – Canada Mortgage and Housing Corporation
- CRA – Canada Revenue Agency
- LTAHS – Long-Term Affordable Housing Strategy
- MCSS – Ministry of Community and Social Services
- MHO – Ministry of Housing
- MOF – Ministry of Finance
- PHB – portable housing benefit
- PHB Framework – Portable Housing Benefit Framework
- PHB-SPP – Portable Housing Benefit - Special Priority Policy
- RGI – rent-g geared-to-income
- SPP – Special Priority Policy
- SDV-PHB – Survivors of Domestic Violence - Portable Housing Benefit

## HIGHLIGHTS

Ontario is launching the Portable Housing Benefit - Special Priority Policy program to provide rental assistance to households who qualify for the Special Priority Policy category prescribed in Ontario Regulation 367/11 under the *Housing Services Act, 2011*.

Eligible applicants who would prefer to live in private rental housing rather than wait for social housing are able to apply for monthly portable housing benefit payments under this program. Eligible applicants may also receive funds directly from Service Managers for first and last month's rent.

Monthly payments to participants are calculated based on household income, as reported on households' latest Canada Revenue Agency notice(s) of assessment, or as verified by Service Managers in certain circumstances. The Ministry of Finance will pay the benefit to participants each month, recalculate the benefit as required, and verify continued eligibility annually.

As the monthly housing benefit is fully portable within Ontario, participants will continue receiving a benefit if they move to a rental unit in another Service Manager area.

Service Managers will help deliver this program by providing program information to eligible applicants and supporting the application process. Service Managers will receive an administration payment for each application approved for their service area and will be reimbursed for funding provided to eligible applicants for first and last month's rent.

## INTRODUCTION

The 2017 Ontario Budget announced the province will invest \$30 million over the next three years in the Portable Housing Benefit - Special Priority Policy (PHB-SPP) program to eventually support up to 3,000 survivors of domestic violence and provide them with the flexibility to choose where they want to live. This ongoing program was announced on November 28, 2017.

A portable housing benefit (PHB) is a monthly subsidy (housing allowance) provided to a low-income household to assist with housing costs. Unlike other forms of housing assistance, the benefit is tied to the household and not a physical housing unit, allowing the benefit to move with the household to any Service Manager area in Ontario. As a result, recipients will have more flexibility to choose where they live to be closer to family, social support networks, schools and employment opportunities.

The PHB-SPP program will provide households who qualify for the Special Priority Policy (SPP) category prescribed in Ontario Regulation 367/11 under the *Housing Services Act, 2011* with an additional option to meet their housing needs while also alleviating pressure on the broader social housing system. This program will provide these households with the option to receive a PHB to help them obtain or retain housing, rather than staying in shelters or other precarious housing situations until a social housing unit becomes available. Households who are approved to receive benefits under this program will not remain on the social housing waiting list of their local Service Manager, with the exception of certain households transitioning from the Survivors of Domestic Violence - Portable Housing Benefit (SDV-PHB) Pilot program.

## Scope of the Guidelines

These guidelines form part of the PHB-SPP Transfer Payment Agreements between the province and Service Managers. They provide a framework for the PHB-SPP program and are designed to assist Service Managers with their administration of the program in their local communities.

The Ministry of Housing (MHO) recognizes that changes to the program design may be necessary in the future; as such, the guidelines may be updated as needed, and any updates will be communicated to Service Managers.

## Provincial Context

The province has undertaken a number of related strategic initiatives to tackle the challenges of housing and homelessness. The PHB-SPP program complements the government's efforts to improve responses to households experiencing violence, such as:

- "It's Never Okay: An Action Plan to Stop Sexual Violence and Harassment";
- "Walking Together: Ontario's Long-Term Strategy to End Violence Against Indigenous Women";
- and
- Ontario's Strategy to End Human Trafficking.

The PHB-SPP program is informed by the following initiatives:

### 1. Special Priority Policy (SPP)

The SPP provides priority access to social housing for eligible households leaving abusive situations, including survivors of domestic violence and survivors of human trafficking. The policy is intended to

ensure that housing is not an inhibiting factor for a household to leave an abusive situation in circumstances where they cannot afford private market accommodation.

As set out in Ontario Regulation 367/11 of the *Housing Services Act, 2011*, Service Managers are required to provide households eligible for the SPP category priority placement on the centralized waiting list for rent-geared-to-income (RGI) assistance above all other applicants.

Recently, amendments were made to the SPP to expand the policy to include survivors of human trafficking, improve the application process for households, and better ensure the policy is culturally inclusive to Indigenous groups and reflective of the complex cycle of abuse experienced by some households.

Aligning with the roll-out of the PHB-SPP program, all Service Managers were required to comply with the SPP regulatory amendments by April 1, 2018.

## 2. Long-Term Affordable Housing Strategy (LTAHS) Update

In March 2016, the province released the LTAHS Update, which reflects new research and best practices that support Ontario's transformation towards a better housing system, including the design and administration of this program.

The LTAHS Update is guided by an updated vision:

**Every person has an affordable, suitable and adequate home to provide the foundation to secure employment, raise a family and build strong communities.**

The vision is associated with two overarching outcomes:

- Decreasing the number of people who are homeless; and
- Increasing the number of families and individuals achieving housing stability.

As part of the updated LTAHS, Ontario committed to developing a framework for a PHB. Traditionally, Ontarians in need of housing assistance have relied primarily on receiving RGI assistance and been required to live in specific housing units to receive this assistance.

The Portable Housing Benefit Framework (PHB Framework or "the Framework") – which is now reflected in regulation under the *Housing Services Act, 2011* – creates the opportunity for Service Managers to use a PHB as an alternative means towards meeting their service level standards if it is delivered in accordance with the regulation.

A PHB provides a monthly subsidy to low-to-moderate income households to assist with housing costs. Unlike RGI assistance, a PHB is tied to an applicant instead of a physical housing unit.

A PHB has multiple benefits for recipients:

- It gives people on a social housing waiting list a potential option to receive a housing benefit that would give them more flexibility and choice about where they live, so they could choose to live closer to employment, child care, schools or family.
- It may help applicants who like where they are living but face affordability challenges to remain where they live.
- Relative to the RGI calculation, the PHB calculation is simplified and reassessed annually using income tax information; by moving to an annual benefit calculation, recipients have an



incentive to earn income as they do not experience an increase in rent with every change in income.

The PHB Framework also provides Service Managers with the opportunity to create more vibrant mixed-income communities due to a greater ability to diversify their housing options.

The LTAHS Update also included priority investments into the province's housing and homelessness systems, including a two-year PHB pilot program for households eligible for the SPP category (SDV-PHB Pilot program).

### **3. SDV-PHB Pilot Program (2016-2018)**

In September 2016, MHO launched the SDV-PHB Pilot program in 22 Service Manager areas. Similar to the PHB-SPP program, eligibility to participate in the Pilot was first determined by whether a household qualified for the SPP category. If households were included in the SPP category, applied and agreed to participate in the SDV-PHB Pilot, they were provided with an alternative form of housing assistance through a PHB. The purpose of the Pilot program was to explore how the benefit could address issues of lengthy wait times, lack of choice, and pressures related to social housing waiting lists among some Service Managers.

Service Managers had the flexibility under the Pilot program to design their own local PHB programs for eligible applicants. These flexibilities included determining PHB amounts as well as the option to offer additional funds for first and last month's rent.

Key findings and lessons learned from the Pilot program highlighted the significant and immediate positive impact it had on the ability of households to quickly find safe, stable and affordable housing, and the strong support of participants to recommend the program to other households.

An important element in the success of the Pilot program was the fact that Service Managers worked very closely with third-party service providers in their areas, such as Violence Against Women support providers and homeless shelters. These agencies provide support services and refer applicants to Service Managers for assistance. The Ministry of Community and Social Services (MCSS) has continued to work closely with the Violence Against Women sector and helped promote the program to that sector through its network of regional offices and the Violence Against Women Stakeholder Advisory Group.

Based on the experience gained in the Pilot program, Service Managers are encouraged to continue working closely with the Violence Against Women sector, and MHO and MCSS regional offices, to promote the expanded PHB-SPP program and ongoing supports available to applicants applying for the SPP category.

## **PROGRAM DESCRIPTION**

### **Objectives**

The PHB-SPP program has three objectives:

- To provide households who qualify for the SPP category with housing support;
- To decrease wait times for housing assistance; and
- To expand housing choice for households who are eligible for the SPP category.

### **Outcomes**

The PHB-SPP program will deliver outcomes to recipients over the immediate, short, intermediate and long term, including:

- Receiving housing assistance more quickly than households in the SPP category who are waiting for RGI assistance;
- Having more choice of suitable housing (e.g., housing type, quality, location);
- Having a reduced rent burden (lower percentage of income spent on shelter costs);
- Being less likely to return to an emergency shelter;
- Experiencing improved household financial well-being; and
- Having improved quality of life.

MHO will develop and use an evaluation framework to assess the effectiveness of the program.

### **Funding**

Subject to annual budget approvals, the province is committed to providing stable, ongoing funding for the program. Up to \$10 million in 2018-19 and up to \$15 million in 2019-20 is available for eligible applicants approved for the program, including households participating in the SDV-PHB Pilot program on March 31, 2018. Due to the PHB-SPP program budget, the ministry cannot guarantee funding of all eligible applicants.

Service Managers will provide eligible households with the option to apply for the PHB-SPP program to help them obtain or retain housing rather than wait for a social housing unit to become available. Households across the province who qualify for the SPP category, apply for the program, and are approved will be provided with a monthly subsidy to assist with the costs of renting a unit of their choosing in the private market.

Service Managers will not receive annual funding allocations. All Service Managers are eligible to receive funding from MHO on a quarterly basis:

- Towards administration costs related to supporting the program; and
- To be reimbursed for first and last month's rent assistance provided to applicants who are approved for the program, as appropriate.

Service Managers will receive a one-time administration payment of \$250 for each application from their service area that is approved for the program. Administration payments will be made quarterly based on the number of eligible applicants approved for the program in each service area, as reported by the Ministry of Finance (MOF) through an online portal.

Details related to Service Managers providing approved applicants with funding for first and last month's rent are included in the "First and Last Month's Rent" section on page 16.

In order to receive funding, Service Managers are required to sign a Transfer Payment Agreement with MHO and MOF that sets out the roles and responsibilities of the parties and the accountability framework for the program, including the terms for funding and reporting requirements. Funding is conditional upon MHO receiving the required quarterly reports from Service Managers. For more information, see the "Transfer Payment Agreements" section on page 19.

## Timeframe

Service Managers delivering the SDV-PHB Pilot program will continue making monthly payments until June 30, 2018, and are responsible for helping Pilot participants transition into the PHB-SPP program. MOF begins payments to PHB-SPP program recipients, including households who have transitioned from the SDV-PHB Pilot, in July 2018.

## Eligibility Criteria: Applicants

Applicants who are not participating in the SDV-PHB Pilot program must meet the following criteria to be eligible to begin receiving a PHB-SPP benefit:

- Reside in Ontario;
- Be on a social housing waiting list and eligible for the SPP category set out in Ontario Regulation 367/11 under the *Housing Services Act, 2011*;
- Be a renter household or fleeing an abusive situation;
- Not be in receipt of, or part of a household in receipt of, RGI assistance, a PHB-SPP benefit, or any other government-funded housing benefit, with the exception of social assistance shelter payments; and
- Consent to being removed from the social housing waiting list of the Service Manager that designated the household under the SPP, once a PHB-SPP benefit is received.

**Note:** For the purpose of this program, household members include the applicant; applicant's spouse or partner (if applicable) and any dependents who reside in the household. If an applicant is sharing his or her household with an individual that is not a household member as defined above (e.g., friend or roommate), the individual is not included as a household member.

All households participating in the SDV-PHB Pilot program as of March 31, 2018 are eligible to apply to receive assistance under the PHB-SPP program. See the "SDV-PHB Pilot Program (2016-2018) Recipients" section on page 10 for information on the application process for Pilot participants.

No member of a household receiving a PHB-SPP benefit may receive, or be part of a household that receives, RGI assistance, more than one PHB-SPP benefit, or another government-funded housing benefit (e.g., housing allowance under the Investment in Affordable Housing program) at the same time, with the exception of social assistance shelter payments.

Service Managers may provide Community Homelessness Prevention Initiative funding to recipients of the PHB-SPP program who need emergency assistance, since that assistance is not intended to be ongoing.

A household receiving a PHB-SPP benefit may reside in a unit that received assistance under a government program (e.g., the Canada-Ontario Affordable Housing Program), where that assistance was attached to the unit and not the household members.

All eligibility criteria will be clearly listed on the application form provided to program applicants.

In addition to the eligibility criteria outlined, participation of new eligible applicants in the program each year is on a first-come, first-served basis, and is subject to annual provincial budget approvals.

### **IMPORTANT NOTE:**

As set out in paragraphs 3 and 4 of section 60 of Ontario Regulation 367/11 under the *Housing Services Act, 2011*, when reviewing RGI eligibility, Service Managers are prohibited from requesting information or documents with respect to a household that was included in the SPP category when the household began to receive RGI assistance if a member of the household believes that he or she or any member of the household will be at risk of abuse if they obtain the information or documents.

This rule also applies when a household is initially applying for a benefit under this program. It could affect obtaining information needed to file taxes or information related to changes in income, which if not accessible by any other means, may require interaction with the abusing individual or the individual engaged in trafficking and put a person at risk of further abuse. In such a case, income would be calculated by the Service Manager based on the best available information. See the "Exemption from Automated Income Verification" section on page 16 for details on this process.

### **Eligibility Criteria: Ongoing**

Annually each Spring, households receiving monthly program benefits must complete an annual renewal form to confirm their ongoing eligibility and to update MOF of any changes to household composition, address and other relevant information.

By the time of the **first renewal**, and each year thereafter, household members must meet the following criteria annually to remain eligible for the program:

- Reside in Ontario;
- Be a renter household; and
- Not be in receipt of, or part of a household in receipt of, RGI assistance, more than one PHB-SPP benefit, or any other government-funded housing benefit, with the exception of social assistance shelter payments.

Recipients who do not confirm their eligibility by submitting an annual renewal form within 120 days of the annual renewal deadline will no longer be eligible for the PHB-SPP program.

In addition to the above criteria, all household members must meet the following criterion by the time of the **second renewal**, and each year thereafter, to remain eligible for the program:

- Do not own a home suitable for year-round occupancy (within or outside Ontario).

By the time of the second renewal, all members of the household with a legal or beneficial interest in a residence (either in or outside Ontario) that is suitable for year-round occupancy must divest (i.e. sell)

their interest and notify MOF in writing, or be ineligible to be included in the household, except in extenuating circumstances.

Households receiving a nil benefit payment for 24 consecutive months will lose their eligibility under the program, receive a notice of their ineligible status, and exit the program.

## **Portability**

The PHB-SPP benefit is fully portable across Ontario. Participants can continue to receive a monthly benefit when they move to a rental unit in another Service Manager area. When a participant moves to a different Service Manager area, the amount of the monthly benefit may change, based on the new Average Market Rent (AMR) for the corresponding size of unit in the new community. See the “In-Year Changes” section on page 16 for more information.

## **PROGRAM DELIVERY**

MHO has overall responsibility for the policy and oversight of the PHB-SPP program; Service Managers provide program information to eligible households and support the application process; MOF processes applications for the PHB-SPP program, monthly benefit payments and ongoing eligibility; and ServiceOntario operates the program's Information Centre (call centre). For a full list of activities and responsibilities, see the "Roles and Responsibilities" section on page 20.

Benefits under the PHB-SPP program will be delivered consistent with, but with appropriate modifications to, the PHB Framework set out in Schedule 4.1 of Ontario Regulation 367/11 under the *Housing Services Act, 2011*.

Delivering the program consistent with the PHB Framework, with necessary modifications to accommodate this program's design, will provide a number of benefits, including:

- Ensuring a similar calculation of the benefit across the province and a consistent programmatic approach, while being responsive to local conditions;
- Enabling households to retain in-year increases in income; and
- Allowing applicants to live in communities that best suit their needs (e.g., education, child care, employment opportunities, community engagement).

## **SDV-PHB Pilot Program (2016-2018) Recipients**

All households receiving assistance under the SDV-PHB Pilot program are eligible to apply for the PHB-SPP program. Service Managers delivering the SDV-PHB Pilot program should provide applications for the PHB-SPP program to all Pilot participants when they become available in May 2018.

Service Managers that provided Pilot benefits to households through Direct Delivery will continue to provide monthly housing benefits to eligible households between April 1, 2018 and June 30, 2018.

Where Pilot recipients transitioning to the PHB-SPP program have demonstrated to the Service Manager a need to receive additional support to bridge the gap between Pilot benefits typically received at the beginning of the month and the first PHB-SPP benefit payment in late July 2018, Service Managers may provide the recipients with an additional benefit payment. Service Managers should reflect the total assistance they will provide to Pilot households in their Take-Up Plan for the period of April 1, 2018 to June 30 2018.

Households receiving assistance under the Pilot as of March 31, 2018 who apply for the expanded PHB-SPP program may choose to:

- Transition to the ongoing program and be removed from the social housing waiting list of the Service Manager that designated the household under the SPP; or
- Remain on the social housing waiting list in the Service Manager area that designated the household under the SPP and approved their participation in the Pilot until June 30, 2019, or until they accept an offer of RGI assistance, whichever is sooner.

These households will:

- Be eligible to receive monthly assistance until June 30, 2019 in either the amount they received under the Pilot as of March 31, 2018 or the amount calculated for the PHB-SPP benefit, whichever is greater; and

- Not be eligible for first and last month's rent assistance under the PHB-SPP program.

As of July 1, 2019, all former Pilot participants receiving assistance under the PHB-SPP program will have the amount of their monthly assistance calculated in accordance with the PHB-SPP program guidelines.

## **Application and Annual Renewal Process**

1. The Service Manager provides PHB-SPP program information to households it has determined are eligible for the SPP category, including:
  - The criteria for assessing the initial and continued eligibility of an applicant for the PHB-SPP benefit;
  - The method used in calculating the benefit at the time of application, for annual reviews and for in-year reassessments;
  - How RGI assistance would be calculated if the household received an offer of RGI assistance;
  - The effect of the receipt of a PHB-SPP benefit or RGI assistance on social assistance payments that a member of the household is receiving or is entitled to receive under Ontario Works or the Ontario Disability Support Program; and
  - Advising the applicant that they may be contacted by MOF to provide and receive additional information on the benefit.

To support the applicant's informed consent and decision to apply for a PHB-SPP benefit, the Service Manager must include in this communication any support persons that the applicant requests and consents to being involved.

2. The Service Manager provides a PHB-SPP application form to an interested eligible applicant.
3. The Service Manager assists the applicant with the completion of the application form and applicable schedules.
4. The Service Manager will determine household net income and adjusted family net income (AFNI) for applicants, and complete the Schedule 2 (Income Tax Filing Exemption), if:
  - The household has not filed the required income tax return(s) in the previous calendar year; or
  - The most recent income tax return(s) does not reflect the household's current financial circumstances.

See the "Exemption from Automated Income Verification" section on page 16 for details on this process.

5. The applicant (or Service Manager, if requested by the applicant) submits the completed application form to MOF by mail, along with the necessary schedules (e.g., Schedule 1: Additional Income Earners), if applicable, and the Service Manager-completed Schedule 2 (Income Tax Filing Exemption), if applicable. The application form includes written consent permitting the CRA to disclose taxpayer information to MOF for the purpose of administering the PHB-SPP program, and for the applicant to be contacted at a later date as part of a program evaluation.

6. MOF processes the application and verifies the application is complete. If the application is not complete, MOF follows up with the applicant, or the Service Manager where necessary, to request additional information.
7. MOF reviews completed applications and confirms eligibility based on the criteria set out in these guidelines and availability of funding.
  - If eligible, MOF calculates the benefit amount either based on the Service Manager calculation of net income and AFNI or its own determination, verifies income where the Service Manager has not done so, and provides the applicant with a Notice of Entitlement.
  - If ineligible, MOF informs the applicant and Service Manager of the ineligibility determination and answers applicant enquiries.

ServiceOntario handles initial enquiries from applicants regarding the application form, with MOF following up as necessary.

8. MOF begins making monthly payments to participants according to the Notice of Eligibility. With respect to how long a client would have to wait before their first monthly payment is received, MOF will make every effort to ensure that applications received by the relevant monthly cut-off date are processed for the upcoming payment date. In the event of incomplete information on an application or information that is inconsistent with CRA, the processing time may be delayed.
9. When MOF approves an applicant for the PHB-SPP program, the Service Manager provides first and last month's rent to the applicant (as appropriate), and removes the applicant from its social housing waiting list (as necessary).
10. Each Spring, MOF provides program participants with an annual renewal form. Households complete and submit the annual renewal form by the deadline included in the form to confirm they comply with ongoing eligibility requirements and inform of any changes (e.g., household composition, address).
11. Annually by April 30, participants must submit a federal income tax return to the CRA to enable MOF to calculate the monthly benefit based on household income.
12. Based on the updated calculation of the household's monthly benefit, MOF provides participants with a Notice of Entitlement including the benefit amount and proceeds to make monthly payments by direct deposit. Payments will be made by direct deposit only, except for extenuating circumstances.

Participants may contact the ServiceOntario Information Centre for more information on the calculation of the monthly benefit, or to request a redetermination of their benefit amount based on changes to the information submitted to MOF with the annual renewal form.

## **Service Level Standards**

Applicants assisted under the program do not count towards meeting Service Managers' service level standards. Service level standards identify the minimum number of low income households required to receive RGI assistance (or approved alternative assistance) in Service Manager areas, as set out in the *Housing Services Act, 2011*.



## PAYMENTS TO APPLICANTS

MOF provides benefit payments by direct deposit each month to the individual who applied for the benefit on behalf of the household and signed the application form. Alternatively, the applicant can choose to have the funds deposited directly to a landlord by submitting a Schedule 6 form (Landlord Consent to Receive Payment). Payments will be made by direct deposit only, except for extenuating circumstances.

Service Managers provide payments directly to applicants for first and last month's rent in accordance with the program guidelines and as outlined in the "First and Last Month's Rent" section on page 16.

## Calculation of Portable Housing Benefit

The benefit is calculated using a formula that is generally consistent with Schedule 4.1 of Ontario Regulation 367/11 under the *Housing Services Act, 2011*. The formula includes AMR and adjusted family net income (AFNI).

$$\text{Monthly Portable Housing Benefit} = (\text{AMR} \times 80\%) - \left[ \frac{(\text{AFNI} \times 30\%)}{12} \right]$$

This formula is responsive to changes in:

- Household income, through the use of AFNI;
- Household composition, through selecting the AMR for the type of housing associated with the family composition; and
- Local housing markets, through the use of local AMR.

For information on the benefit calculation for social assistance recipients, see the "Interaction with Social Assistance" section on page 15.

## Average Market Rent (AMR)

The amount of a PHB is based on the difference between 80 per cent of the Canada Mortgage and Housing Corporation (CMHC) AMR for an appropriately sized rental unit, based on household composition, and 30 per cent of annual household AFNI divided by 12. AMR is defined as the average expense of market rent in the relevant service area, as provided by CMHC to MHO based on CMHC's annual rental survey. AMR is a standard measure used in other housing programs and MHO updates AMR information on its website annually.

The PHB-SPP program only uses AMRs for unit sizes of one bedroom, two bedrooms and three bedrooms. Recipients will receive a monthly benefit based on a calculation using a unit size no smaller than one bedroom and no larger than three bedrooms. Households requiring more than three bedrooms will receive a benefit based on a calculation using AMR for three bedrooms.

MOF will use a uniform set of occupancy standards to calculate the amount of a monthly benefit based on the appropriate unit size for each eligible household, as follows:

- Spouses/partners will be designated one bedroom; and
- Every other person in the household will be designated a separate bedroom.

Households may reside in any size of accommodation they choose, regardless of the number of bedrooms determined by the occupancy standards.

### **Adjusted Family Net Income (AFNI)**

The AFNI of a household is based on the income of each member of the household who is at least 17 years old, excluding those who are in full-time attendance at a recognized educational institution. Benefits received under this program are exempted as income for the purpose of calculating the monthly PHB-SPP benefit.

When an applicant applies to the program, household net income and AFNI will be determined by MOF if the relevant tax information is available for each household member whose income is to be included in the calculation. Household net income and AFNI will be determined by the Service Manager for new applicants if:

- The household has not filed the required income tax return(s) in the previous calendar year; or
- The most recent income tax return(s) does not reflect the household's current financial circumstances.

Where the relevant tax information is available for each household member whose income is to be included in the calculation, household net income is determined by MOF using the latest annual CRA notice(s) of assessment. MOF will use the net income for relevant household members indicated on line 236 of the latest notice(s) of assessment issued under the *Income Tax Act* (Canada) for the most recent taxation year that ended before the application is considered, adjusted as follows, or if no notice of assessment has been issued, the amount that would appear on that line had the notice of assessment been issued, adjusted as follows:

- By subtracting from that amount any payments from a registered disability savings plan received by the member in that taxation year and any payment of a PHB received by the member in that taxation year; and
- By adding to that amount any payments from a registered disability savings plan repaid by the member in that taxation year.

Where the Service Manager is determining household net income and AFNI of new applicants for the reasons outlined above, the net income of each household member whose income is to be included in the calculation is determined by the Service Manager using:

- The best information available; and
- The amount that best approximates each member's net income adjusted as outlined above and based on the Service Manager's projections of income and deductions for the 12-month period beginning on the first day of the month following the month in which the application is considered.

The Service Manager provides the calculated amount on Schedule 2 (Income Tax Filing Exemption) of the application.

The maximum monthly benefit payable is 80 per cent of AMR less \$85. The minimum monthly benefit payable is \$10. Any monthly benefit calculated as an amount less than \$10 will be considered a nil (\$0) payment.

During each annual review, the benefit is calculated by MOF using the latest household notice(s) of assessment for the most recent taxation year, as indicated above. However, households with significant decreases in income or other changes (e.g., changes to household composition) may require an in-year reassessment, as outlined in the “In-Year Changes” section on page 16.

Using AFNI to define income is consistent with other modern forms of assistance, such as the Ontario Child Benefit.

## **Interaction with Social Assistance**

Under Ontario Works and the Ontario Disability Support Program, recipients receive a shelter allowance as a portion of their monthly entitlement up to a maximum amount based on actual shelter costs and household size. Social assistance recipients are eligible to receive the maximum shelter amount if their shelter costs exceed the maximum.

The *Ontario Works Act, 1997* and the *Ontario Disability Support Program Act, 1997* allow for housing benefits to be exempted as income, where approved by the Director of Ontario Works or the Ontario Disability Support Program, up to the difference between actual shelter costs (e.g., rent) and the actual shelter allowance payable (which is capped at maximum shelter costs). This exemption was approved for the SDV-PHB Pilot program.

For social assistance recipients, consistent with the PHB Framework, the same PHB calculation formula applies to determine the maximum benefit amount for a household. The social assistance shelter allowance will be provided in the normal fashion, however the PHB will fill the gap between the social assistance shelter allowance and actual shelter costs, up to the maximum PHB amount.

If actual shelter costs increase or a recipient moves to a unit with higher rent, the PHB amount paid will increase but remain subject to the maximum PHB amount. In addition, if a recipient no longer receives social assistance, the maximum PHB amount will be paid to the household.

As a result, recipients receiving social assistance are required to contact the ServiceOntario Information Centre to report any changes (increases or decreases) in their shelter costs to allow MOF to adjust their PHB-SPP benefit accordingly.

Recipients receiving social assistance do not need to report month-to-month changes in utilities because shelter costs are averaged over a year.

## **Automated Income Verification**

MOF conducts annual Automated Income Verification using CRA income tax information. For instance, for the 2019 to 2020 benefit period (July 1, 2019 to June 30, 2020), 2018 income tax information would be used for Automated Income Verification. As a result, households receiving a PHB-SPP benefit must submit CRA income tax return(s) each year by April 30. Failure to submit the required income tax return(s) may result in a delay in benefit payments.

## **Exemption from Automated Income Verification**

Applicants entering the PHB-SPP program may be exempted from Automated Income Verification for their initial benefit calculation where:

- The household has not filed the required income tax return(s) in the previous calendar year; or
- The most recent income tax return(s) does not reflect the household's current financial circumstances.

In this situation, Service Managers will manually calculate and verify household net income and AFNI, as outlined in the "Adjusted Family Net Income (AFNI)" sub-section of the "Calculation of Portable Housing Benefit" section that begins on page 13.

If information is not available for an initial benefit calculation because a member of the household believes that he or she or any member of the household will be at risk of abuse if the information is obtained, the Service Manager will calculate and verify household net income and AFNI based on the best available information. See the "Important Note" in the "Eligibility Criteria: Applicants" section that begins on page 7 for more information.

During that year of exemption, household members will be required to submit annual income tax returns to the CRA by April 30. Households who were initially exempt will be required to have Automated Income Verification based on their annual notice(s) of assessment going forward.

## **First and Last Month's Rent**

For applicants approved for the program by MOF, Service Managers may provide funding directly for first and last month's rent, where the applicant has demonstrated to the Service Manager a need to receive the payment. Where Service Managers have a method for determining household need under the Community Homelessness Prevention Initiative Program, a similar process should be applied.

The amount of first and last month's rent shall not exceed the lesser of:

- Twice the amount of the actual rent paid by the approved household; or
- Twice the amount of 100 per cent of the CMHC AMR for an appropriately sized rental unit, based on household composition.

MHO will flow these funds to Service Managers on a quarterly basis retroactively, in accordance with Service Manager quarterly reports.

## **In-Year Changes**

As indicated on the application form, participants must report any changes in personal information (e.g., household composition, address) as soon as possible to the ServiceOntario Information Centre. Subject to the following, recipients are not required to report an increase in income during the year or undergo a reassessment of the monthly benefit due to an increase in income.

MOF will perform an in-year reassessment of recipient eligibility and/or monthly benefits under the following circumstances:

- A recipient contacts the ServiceOntario Information Centre to request a reassessment due to a significant decrease of at least 20 per cent in household income (limited to one in-year reassessment each year).

- A recipient contacts the ServiceOntario Information Centre to advise of a move to a different Service Manager area (this may affect AMR and therefore the monthly benefit received).
- A recipient contacts the ServiceOntario Information Centre to advise of a permanent change to household composition.
- A recipient contacts the ServiceOntario Information Centre to advise that they have started or stopped receiving assistance under the *Ontario Works Act, 1997* or the *Ontario Disability Support Program Act, 1997*.
- A recipient who is receiving social assistance contacts the ServiceOntario Information Centre to advise of a change (increase or decrease) in shelter costs.
- A Service Manager or recipient advises the ServiceOntario Information Centre that they have ceased to be eligible on certain grounds for continued eligibility (e.g., the recipient is receiving another government-funded housing benefit).

When performing an in-year review, MOF will request the necessary information from the recipient to reassess eligibility and/or recalculate the monthly benefit, as appropriate.

Where an in-year reassessment results in a change in a PHB-SPP benefit, the change will be processed at the time of the in-year reassessment.

As noted, recipients may request only one in-year reassessment between annual reviews due to a significant decrease of at least 20 per cent in household income. Where a recipient has requested an in-year reassessment due to a decrease in household income, net income and AFNI is determined by MOF using the amount that best approximates the household's income, calculated and adjusted as outlined in the "Adjusted Family Net Income (AFNI)" sub-section of the "Calculation of Portable Housing Benefit" section that begins on page 13. The calculation is based on MOF's projections of income and deductions for the 12-month period beginning on the first day of the month following the month in which the review is considered.

## Monthly Payments

When MOF receives a completed application form or annual renewal form by the relevant monthly cut-off date or the annual renewal deadline, payment is processed on a go-forward basis according to the effective start date in the Notice of Eligibility for new applicants or the first payment date of the next benefit period for existing recipients.

If an application form is not submitted by the monthly cut-off date or is incomplete, new applicants will be paid retroactively from the effective start date in the Notice of Eligibility, not the application date, once all required information has been submitted.

If an annual renewal form is not submitted by the annual renewal deadline or is incomplete, recipients will be paid retroactively from the beginning of the new benefit year once all required information has been submitted.

Existing recipients who do not confirm their ongoing eligibility by submitting an annual renewal form within 120 days of the annual renewal deadline will no longer be eligible for the PHB-SPP program, as outlined in the "Eligibility Criteria: Ongoing" section on page 8.

If a household is absent from Ontario for more than 60 consecutive days, the household's PHB-SPP benefit may be suspended.

## **Direct Deposit**

All applicants, including those who are transferring from other programs, must submit direct deposit information with their applications, such as void cheques or direct deposit forms from their bank. MOF uses this information to set up monthly payments to applicants. Payments will be made by direct deposit only, except for extenuating circumstances.

## **T5007 Tax Forms**

MOF is required to issue a T5007 tax form, known as a Statement of Benefits, to all program participants by the end of February each year. The forms report PHB-SPP monthly benefits provided to recipients as income for tax purposes. MOF issues T5007 forms to participants even in cases where payments are made directly to landlords. Benefits received under this program are exempted as income for the purpose of calculating the monthly PHB-SPP benefit.

Service Managers are required to issue T5007 tax forms to participants for first and last month's rent payments delivered directly to households. In addition, Service Managers will issue T5007 tax forms for any monthly benefits provided to SDV-PHB Pilot households between April 1, 2018 and June 30, 2018.

## ACCOUNTABILITY AND REPORTING

The province places a high degree of importance on accountability for its actions, decisions and policies with regard to the use of public funds for programs and services. The government has an obligation to demonstrate value for money and ensure that funds have been spent appropriately and in a timely manner. Accordingly, Service Managers must submit the following as accountability mechanisms for the PHB-SPP program:

- Transfer Payment Agreement with MHO and MOF;
- Quarterly Reports; and
- French Language Services Reports.

Service Managers will submit quarterly reports and French Language Services Reports as described in the respective sections of the PHB-SPP Transfer Payment Agreement.

Service Managers are required to use the Grants Ontario System to submit PHB-SPP reports. For assistance or questions regarding the Grants Ontario System, please contact the Grants Ontario – AIMS Support Desk at [AIMSupport@ontario.ca](mailto:AIMSupport@ontario.ca) or by telephone at 416-585-7070 or 1-866-417-5399 (toll-free).

## Memoranda of Understanding

Three memoranda of understanding govern the PHB-SPP program:

- **MHO and MOF Memorandum of Understanding:** Sets out the responsibilities of the two ministries in relation to the PHB-SPP program
- **CRA and MOF Memorandum of Understanding:** Enables MOF to obtain household level tax information from the CRA in order to perform Automated Income Verification during eligibility determination and benefit calculation
- **MHO and ServiceOntario Memorandum of Understanding:** Arranges for ServiceOntario to operate the Information Centre to respond to program enquiries from applicants and request required information, as appropriate

## Transfer Payment Agreements

Service Managers must enter into a Transfer Payment Agreement with MHO and MOF for the PHB-SPP program. In accordance with the province's Transfer Payment Accountability Directive, the agreements will contain an accountability framework, outline the roles and responsibilities of the parties, and include the terms for funding and reporting requirements. The agreement will set out the role of Service Managers, MHO and MOF in relation to the sharing of household personal information.

## Quarterly Reports

Following the execution of Transfer Payment Agreements, Service Managers are required to submit quarterly reports to MHO including actual expenditures and households assisted for the previous quarter. Service Managers will also provide additional information, data and reports as needed by the ministry to report on progress made towards achieving program outcomes.

## French Language Services Act Compliance

Service Managers who are located in or servicing an area that is designated under the *French Language Services Act* are required to:

- Ensure services are provided in French; and,
- Make it known to the public (through signs, notices, other information on services, and initiation of communications in French) that services provided to and communications with the public in connection with the PHB-SPP program are available in French.

Services being provided directly to the public by Service Managers, or through the office of a sub-contractor (e.g., local non-profit agency), are required to comply with the *French Language Services Act*.

To demonstrate compliance, Service Managers are required to submit French Language Services Reports to MHO confirming that the requisite French language services are being provided. An initial report must be signed and submitted to MHO at the time of signing the Transfer Payment Agreement, and reports must be submitted annually thereafter by July 15.

Sample French Language Services Report templates are included as part of Transfer Payment Agreements.

## Roles and Responsibilities

MHO will undertake the following activities:

- Establish the PHB-SPP Program Guidelines;
- Help Service Managers connect with partner ministries and Violence Against Women support providers;
- Enter into Transfer Payment Agreements with MOF and Service Managers;
- Enter into Memoranda of Understanding with MOF and ServiceOntario;
- Provide program funding to MOF;
- Provide funding for administration costs and first and last month's rent to Service Managers;
- Develop, review and approve quarterly reports; and
- Arrange for ServiceOntario to operate the Information Centre to respond to program enquiries as appropriate.

Service Managers will undertake the following activities:

- Enter into Transfer Payment Agreements with MHO and MOF;
- Explain the program and eligibility criteria to eligible applicants;
- Distribute PHB-SPP program application forms to eligible applicants;
- Ensure interested applicants have been informed of the benefits and risks of the program;
- Ensure interested applicants have consented on the program application to the disclosure of their personal information to MHO, MOF, Ministry of Government and Consumer Services, ServiceOntario, MCSS, CRA, and the Service Manager;
- Collect required information on intake;
- Submit required reports to MHO;
- Provide first and last month's rent payments to eligible applicants as appropriate (to be reimbursed by MHO);



- Complete and distribute T5007 tax forms (Statement of Benefits) to participants for first and last month's rent payments delivered directly to households and for any monthly benefits provided to SDV-PHB Pilot households between April 1, 2018 and June 30, 2018; and
- Calculate and provide applicant income information to MOF at the time of initial application, as required.

MOF will undertake the following activities:

- Enter into Memoranda of Understanding with MHO and CRA;
- Enter into Transfer Payment Agreements with MHO and Service Managers;
- Distribute application forms to Service Managers to be provided to eligible households;
- Receive and process applications, annual renewal forms, and in-year reassessment requests from participating households;
- Follow up with applicants to request information for incomplete applications, renewal forms and in-year assessments, as necessary;
- Determine eligibility for the PHB-SPP program and issue eligibility notices;
- Verify household income and AFNI using CRA tax return information;
- Calculate benefit amounts;
- Reassess eligibility and benefit amounts annually at renewal, in-year due to specific changes (e.g., change in household composition), and up to once per year for in-year reassessments due to a significant decrease in income;
- Issue benefit payments to program participants;
- Manage recovery of overpayments;
- Provide regular updates to MHO and Service Managers through an online portal (e.g., funding expended, the number of households assisted); and
- Complete and distribute T5007 tax forms (Statement of Benefits) annually to recipients to report PHB-SPP monthly benefits as income for tax purposes (in addition to the T5007 tax forms issued by Service Managers for first and last month's rent payments delivered directly to households).

ServiceOntario will undertake the following activities:

- Enter into a Memorandum of Understanding with MHO; and
- Operate the Information Centre to respond to program enquiries.

## IMPORTANT DATES

The benefit year for the PHB-SPP program is July 1 to June 30. The PHB-SPP program will be delivered according to the following timelines:

Activity	Date
Program announcement	November 30, 2017
Guidelines and support materials released to Service Managers with MHO teleconference	February – March 2018
Service Managers delivering SDV-PHB Pilot program sign amendments to Pilot funding agreements to extend Service Manager payments to Pilot recipients until June 30, 2018	March – April 2018
Service Managers continue monthly benefit payments to SDV-PHB Pilot recipients	April 1, 2018 – June 30, 2018
MOF continues Shared Delivery payments to SDV-PHB Pilot recipients	April 1, 2018 – June 30, 2018
Transfer Payment Agreements for administration funding and first and last month's rent payments executed by MHO, Service Managers and MOF	May 2018
MOF provides an application form to Service Managers for distribution to eligible households	May 2018
MOF begins receiving applications	May 2018
MOF begins payments to PHB-SPP program recipients, including households who have transitioned from the SDV-PHB Pilot	July 2018 (first monthly payment date is July 28, 2018)
Service Manager Quarterly Reports due to MHO each year (annual deadlines)	Q1 (April to June): July 15 Q2 (July to September): October 15 Q3 (October to December): January 15 Q4 (January to March): March 15
Service Manager French Language Services Reports due to MHO	Initial report submitted at the time of signing the Transfer Payment Agreement and reports submitted annually thereafter by July 15

To obtain further information about the PHB-SPP program, Service Managers are encouraged to contact their respective regional staff contacts at MHO. For information on available support services, contact the respective regional staff contacts at MCSS. Contact information is included in the appendices.

## APPENDIX A: MINISTRY OF HOUSING CONTACTS

### MUNICIPAL SERVICES OFFICE – CENTRAL

Serving: Durham, Halton, Hamilton, Muskoka, Niagara, Peel, Simcoe, York

777 Bay Street 13<sup>th</sup> Floor  
Toronto, ON M5G 2E5  
General Inquiry: 416-585-6226  
Toll Free: 1-800-668-0230  
Fax: 416-585-6882

Contact: Ian Russell, Team Lead, Regional Housing Services  
Tel: 416-585-6965  
Email: [ian.russell@ontario.ca](mailto:ian.russell@ontario.ca)

### MUNICIPAL SERVICES OFFICE – EASTERN

Serving: Cornwall, Hastings, Kawartha Lakes, Kingston, Lanark, Leeds and Grenville, Lennox and Addington, Northumberland, Ottawa, Peterborough, Prescott and Russell, Renfrew

8 Estate Lane, Rockwood House  
Kingston, ON K7M 9A8  
General Inquiry: 613-545-2100  
Toll Free: 1-800-267-9438  
Fax: 613-548-6822

Contact: Mila Kolokolnikova, Team Lead, Regional Housing Services  
Tel: 613-545-2123  
Email: [mila.kolokolnikova@ontario.ca](mailto:mila.kolokolnikova@ontario.ca)

### MUNICIPAL SERVICES OFFICE – WESTERN

Serving: Brantford, Bruce, Chatham-Kent, Dufferin, Grey, Huron, Lambton, London, Norfolk, Oxford, St. Thomas, Stratford, Waterloo, Wellington, Windsor

659 Exeter Road, 2<sup>nd</sup> Floor  
London, ON N6E 1L3  
General Inquiry: 519-873-4020  
Toll Free: 1-800-265-4736  
Fax: 519-873-4018

Contact: Cynthia Cabral, Senior Housing/Planning Advisor  
Tel: 519-873-4520  
Email: [cynthia.cabral@ontario.ca](mailto:cynthia.cabral@ontario.ca)

**MUNICIPAL SERVICES OFFICE – NORTHERN (SUDBURY)**

Serving: Algoma, Cochrane, Greater Sudbury, Manitoulin-Sudbury, Nipissing, Parry Sound, Sault Ste. Marie, Timiskaming

159 Cedar Street, Suite 401  
Sudbury, ON P3E 6A5  
General Inquiry: 705-564-0120  
Toll Free: 1-800-461-1193  
Fax: 705-564-6863

Contact: Cindy Couillard, Team Lead, Regional Housing Services  
Tel: 705-564-6808  
Email: [cindy.couillard@ontario.ca](mailto:cindy.couillard@ontario.ca)

**MUNICIPAL SERVICES OFFICE – NORTHERN (THUNDER BAY)**

Serving: Kenora, Rainy River, Thunder Bay

435 James Street, Suite 223  
Thunder Bay, ON P7E 6S7  
General Inquiry: 807-475-1651  
Toll Free: 1-800-465-5027  
Fax: 807-475-1196

Contact: Peter Boban, Team Lead, Regional Housing Services  
Tel: 807-473-3017  
Email: [peter.boban@ontario.ca](mailto:peter.boban@ontario.ca)

**HOUSING PROGRAMS BRANCH – TORONTO**

Serving: Toronto

777 Bay Street, 14<sup>th</sup> Floor  
Toronto, ON M5G 2E5  
Fax: 416-585-7003

Contact: Walter Battello, Account Manager, Regional Services Delivery Unit  
Tel: 416-585-6480  
Email: [walter.battello@ontario.ca](mailto:walter.battello@ontario.ca)

## **APPENDIX B: MINISTRY OF COMMUNITY AND SOCIAL SERVICES CONTACTS**

### **CENTRAL REGION**

Serving: Dufferin, Halton, Peel, Simcoe, Waterloo, Wellington, York

6733 Mississauga Road, Suite 200  
Mississauga, ON L5N 6J5  
Tel: (905) 567-7177  
Fax: (905) 567-3215  
Toll Free: 1-877-832-2818

17310 Yonge Street  
Newmarket, ON L3Y 7R8  
Tel: (905) 868-8900  
TTY: (905) 715-7759  
Fax: (905) 895-4330  
Toll Free: 1-877-669-6658

### **EAST REGION**

Serving: Cornwall, Durham, Hastings, Kawartha Lakes, Kingston, Lanark, Leeds & Grenville,  
Lennox & Addington, Northumberland, Ottawa, Peterborough, Prescott & Russell, Prince  
Edward County, Renfrew

347 Preston Street, 3rd Floor  
Ottawa, ON K1S 2T7  
Tel: (613) 234-1188  
Fax: (613) 783-5958  
Toll Free: 1-800-267-5111

11 Beechgrove Lane  
Kingston, ON K7M 9A6  
Tel: (613) 545-0539  
Fax: (613) 536-7272  
Toll Free: 1-800-646-3209  
TTY: (613) 536-7304

**WEST REGION**

Serving: Brantford, Bruce, Chatham-Kent, Grey, Hamilton, Huron, Lambton, London, Niagara, Norfolk, Oxford, St. Thomas, Stratford, Windsor

217 York Street, Suite 203  
P.O. Box 5217  
London, ON N6A 5R1  
Tel: (519) 438-5111  
Fax: (519) 672-9510  
Toll Free: 1-800-265-4197  
TTY: (519) 663-5276  
119 King Street West  
Hamilton, ON L8P 4Y7  
Tel: (905) 521-7280  
Fax: (905) 546-8277  
Toll Free: 1-866-221-2229  
TTY: (905) 546-8276

**NORTH REGION**

Serving: Algoma, Cochrane, Kenora, Manitoulin-Sudbury, Nipissing, Parry Sound, Rainy River, Sault Ste. Marie, Sudbury, Thunder Bay, Timiskaming

199 Larch Street  
10th Floor, Suite 1002  
Sudbury, ON P3E 5P9  
Tel: (705) 564-4515  
Fax: (705) 564-2163  
Toll Free: 1-800-461-1167  
TTY: (705) 564-3233

621 Main Street West  
North Bay, ON  
P1B 2V6  
Tel: (705) 474-3540  
Fax: (705) 474-5815  
Toll Free: 1-800-461-6977  
TTY: (705) 474-7665

**TORONTO**

Serving: Toronto

375 University Avenue, 5th Floor  
Toronto, ON M7A 1G1  
Tel: (416) 325-0500  
Fax: (416) 325-0565  
TTY: (416) 325-3600

**SCHEDULE “E”  
REPORTING**

SCHE

Name of Report	Due Date
1. Quarterly Report(s): Quarter 1 Report Quarter 2 Report Quarter 3 Report Quarter 4 Report	On July 15 in each Fiscal Year. On October 15 in each Fiscal Year. On January 15 in each Fiscal Year. On March 15 in each Fiscal Year.
2. French Language Services Report	On July 15 in each Fiscal Year.
3. Reports as specified from time to time	On a date or dates specified by MHO.

**Report Due Date**

The Reporting period is based on the Fiscal Year.

Except as noted below, if the due date of any Report falls on a non-Business Day, the due date is deemed to be the next Business Day.

**Submission of Reports**

All Reports are to be submitted through the Grants Ontario System (GOS) unless MHO notifies the Service Manager otherwise. Reports attached to this Schedule are samples of the Reports required under GOS.

**Report Details**

1. The Quarterly Reports shall be substantially in the form of Appendix “A” and shall be subject to the approval of MHO.

The Quarterly Reports shall set out:

- (a) actual households and the target group of the household approved by MOF under the Program in each completed quarter of each Fiscal Year;
- (b) the amount that the Service Manager paid to Eligible SPP Households for first and last months’ rent in accordance with this Agreement and the Program Guidelines in each completed quarter of the Fiscal Year; and
- (c) confirmation that funding provided for administration costs were spent on administration costs.

Through the Quarterly Report and other Program reports, MHO will obtain information on the performance indicators set out below to demonstrate that the Program objectives set out in the Program Guidelines are being met:

- Number of households approved under the Program;
  - Increased housing affordability of households approved under the Program; and
  - Increased housing stability of households approved under the Program.
2. The French Language Services Report will be in the form of Appendix “B” and shall set out whether the Service Manager has complied with the French Language Services (FLS) requirements of the Agreement.
  3. MHO will specify the timing and content of any other reports as may be necessary.



**APPENDIX "A"**  
**QUARTERLY REPORT**  
**SEE ATTACHED.**

# Portable Housing Benefit - Special Priority Policy

## QUARTERLY REPORT

Household Identifier	# Bedrooms Required	Total amount paid to households for First/Last Month's Rent	Payment Date (if first/last paid)	SPP Eligibility	
				HT	DV
	#	\$	date		

\*Add rows as needed

*I confirm, to the best of my knowledge, that the information in this Portable Housing Benefit - Special Priority Policy Quarterly Report is correct.*

<b>Prepared By:</b>	Print Name & Title	Signature	Date
<b>Approved By:</b> (Delegated Service Manager Authority)	Print Name & Title	Signature	Date

## APPENDIX "B"

### FRENCH LANGUAGE SERVICES REPORT

Please complete and submit this Report on an annual basis by July 15th of each year.

Service Manager: \_\_\_\_\_

Service Manager Address: \_\_\_\_\_

Service Manager Contact: \_\_\_\_\_

Name: \_\_\_\_\_

Number: \_\_\_\_\_

Email: \_\_\_\_\_

This report is to confirm that the \_\_\_\_\_ [Service Manager name] is providing services under the Portable Housing Benefit – Special Priority Policy (PHB-SPP) Program and has an office(s) located in or serving an area designated in the Schedule to the French Language Services Act ("FLSA").

The \_\_\_\_\_ [Service Manager name] confirms that it is:

- Providing PHB-SPP Program services to the public in French in all of its offices (including the offices of sub-contractors) located in or serving an area designated in the Schedule to the FLSA as described in Schedule A; and,
- Making it known to the public, including by way of signs, notices, other information on services, and initiation of communications in French, that services provided to and communications with the public in connection with the PHB-SPP Program are available in French.

I declare that the above information is true and complete.

Service Manager Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

I have the authority to bind \_\_\_\_\_ [Service Manager name]

Dated at \_\_\_\_\_ this \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_.

As a Service Manager providing services under the PHB-SPP Program and having offices (including the offices of sub-contractors) located in or serving an area designated in the Schedule to the French Language Services Act, please complete the section below. A list of designated areas is attached.

Service Manager Name: \_\_\_\_\_

Name of Designated Area(s): \_\_\_\_\_

Description of Services: \_\_\_\_\_

Please select all items that apply to the services you are providing under the PHB-SPP Program in an office (or the office of a sub-contractor) that is located in or services a designated area.

- Signage and visibility of available services in French
- Over-the-counter services are available in French
- Written correspondence and telephone service are available in French
- Translation of written material produced for public use is available in French
- Other \_\_\_\_\_ [please specify]

Please list any services or locations in designated areas where these French language services are not being provided. Please explain.

---

---

---

---

---

---

---

List of Designated Areas under the French Language Services Act

Service Manager	Designated Area(s)
City of Toronto	All
Central Region	
Regional Municipality of York	City of Markham (As of July 1, 2018)
Regional Municipality of Peel	City of Mississauga; City of Brampton
County of Simcoe	Town of Penetanguishene; Townships of Tiny and Essa
Eastern Region	
City of Cornwall	County of Glengarry; Township of Winchester; County of Stormont
City of Kingston	City of Kingston
City of Ottawa	All
United Counties of Prescott and Russell	County of Prescott; County of Russell
County of Renfrew	City of Pembroke; Townships of Stafford and Westmeath
Western Region	
Municipality of Chatham-Kent	Town of Tilbury; Townships of Dover and Tilbury East
City of Hamilton	All of the City of Hamilton as it exists on December 31, 2000
City of London	City of London
Regional Municipality of Niagara	City of Port Colborne; City of Welland
City of Windsor	City of Windsor; Towns of Belle River and Tecumseh; Townships of Anderdon, Colchester North, Maidstone, Sandwich South, Sandwich West, Tilbury North, Tilbury West and Rochester
Northeast Region	
Algoma District Services Administration Board	District of Algoma
Cochrane District Social Services Administration Board	All
City of Greater Sudbury	All
Manitoulin-Sudbury District Services Board	District of Sudbury
District of Nipissing Social Services Administration Board	District of Nipissing
District of Parry Sound Social Services Administration Board	Municipality of Callander
District of Sault Ste. Marie Social Services Administration Board	The part of the District of Algoma that is part of the district for the District of Sault Ste. Marie Social Services Administration Board
District of Timiskaming Social Services Administration Board	All
Northwest Region	

Kenora District Services Board	Township of Ignace
District of Thunder Bay Social Services Administration Board	Towns of Geraldton, Longlac and Marathon; Townships of Manitouwadge, Beardmore, Nakina and Terrace Bay

**SCHEDULE “F”  
PAYMENT PLAN**

SCHE

Payment	Due Date
<p>For administration costs, \$250 for each new Eligible SPP Household that MOF confirms to MHO as participating in the Program and that is reflected as participating in the Program in a Quarterly Report, all to the extent approved by MHO.</p>	<p>Within 30 days of MHO approving the confirmation by MOF and the relevant Quarterly Report.</p>
<p>For each Eligible SPP Household that complies with the criteria set out in clause 4.1(a) of Schedule “C”, the lesser of:</p> <ul style="list-style-type: none"> <li>a) twice the amount of actual rent paid by the household; and</li> <li>b) twice the amount of 80% of the Canada Mortgage and Housing Corporation Average Market Rent for an appropriately sized unit for the household, based on household composition,</li> </ul> <p>as reflected as having been paid by the Service Manager but not yet reimbursed in an MHO approved Quarterly Report.</p>	<p>Within 30 days of MHO approving the relevant Quarterly Report.</p>

## **SCHEDULE "G"**

### **PERSONAL INFORMATION SHARING PROVISIONS**

#### **1.0 DEFINITIONS**

1.1 In this Schedule, capitalized terms have the meaning given to them in Schedules "A" and "C" and the following terms have the following meanings:

**"FOI"** means Freedom of Information;

**"Party"** means MHO, MOF or the Service Manager and "Parties" means all of them;

**"PI"** means personal information as defined under FIPPA and MFIPPA;

**"Records"** has the same meaning as that term is defined in FIPPA and MFIPPA.

1.2 For the purposes of Articles 3 and 5 of this Schedule "G", the term "Applicant" shall include each other household member reflected on the Application Form and, for greater certainty, "Application Form" shall include all Schedules thereto; where applicable, "Application Form" shall include a Renewal Form and all schedules thereto.

#### **2.0 FOI REQUESTS, FIPPA, and MFIPPA**

2.1 MHO, MOF and the Service Manager acknowledge and agree that:

- (a) Records of Canada Revenue Agency taxpayer information in the custody of MHO and MOF shall not be considered to be within the custody or control of the Service Manager;
- (b) MHO, MOF and the Service Manager shall comply with FIPPA and/or MFIPPA as required and will cooperate in handling each Program related FOI request under FIPPA or MFIPPA that it receives in accordance with the applicable legislation;
- (c) As between MHO and MOF, FIPPA requests shall be addressed as set out in the Memorandum of Understanding between them relating to the Program; and
- (d) Each party will advise the other parties of any Program related breaches of FIPPA or MFIPPA immediately after they occur as set out in sections 4.7 and 4.8.



### **3.0 PI SHARING**

- 3.1 MHO and the Service Manager will provide to MOF only PI that MOF requires for the provision of its services to assist MHO in the administration of the Program. In the case of the Service Manager, this may include completed Application Forms and Applicant income information with respect to which the Applicant(s) has completed and signed the certification and consent area of the Application Form.
- 3.2 MOF will provide to MHO and the Service Manager only PI that is related to an Applicant who has completed and signed the certification and consent area of the Application Form, and that MHO and the Service Manager require for the administration of the Program.
- 3.3 MHO will collect from MOF and the Service Manager only PI that (i) is related to an Applicant who has completed and signed the certification and consent area of the Application Form; (ii) the disclosure of which to MHO is authorized by the certification and consent; and (iii) MHO requires for the administration of the Program.
- 3.4 MHO will provide to the Service Manager only PI that (i) is related to an Applicant who has completed and signed the certification and consent area of the Application, (ii) is authorized by the certification and consent, (iii) the Service Manager requires for the administration of the Program, and (iv) is listed on Appendix "A-1".
- 3.5 MOF will provide to MHO and the Service Manager a list of Applicants that have completed and signed the certification and consent area of the Application Form and may update this list from time to time.
- 3.6 The Service Manager will provide to MHO only PI that (i) is related to the Applicants reflected on the list provided to it under section 2.5, (ii) MHO or MOF require for the administration of the Program and (iii) is listed on Appendix "A-2".
- 3.7 The means of transmitting PI between MHO and the Service Manager will be either bonded courier or encrypted email.
- 3.8 MHO and the Service Manager may provide PI to one another by such other means as may be agreed to by both parties.

### **4.0 CONFIDENTIALITY AND SECURITY OF PI**

- 4.1 The PI collected, used or disclosed under this Agreement is confidential and shall not be shared beyond the Parties to this Agreement.

- 4.2 MHO, MOF and the Service Manager will each take all reasonable measures to ensure the confidentiality and integrity of the PI that it may receive under this Agreement and to safeguard the PI against accidental or unauthorized access, disclosure, use, modification and deletion. All Parties agree to comply with their internal security safeguards to protect PI against loss or theft, as well as unauthorized access, disclosure, copying, use or modification of the format in which it is held or retained.
- 4.3 MHO and MOF each agree that it will follow the guidelines set out in the Office of the Chief Information and Privacy Officer, Ministry of Government and Consumer Services, "Taking the Right Steps - A Guide to Managing Privacy and Privacy Breaches" attached as Appendix "B-1", the OPS Corporate Policy on Protection of Personal Information dated July 25, 2011 attached as Appendix B-2, and each Party's policies and guidelines governing the protection of PI. The Service Manager agrees that it will also, to the extent possible, follow these guidelines even though they are drafted for institutions under FIPPA and not MFIPPA. The Service Manager will also use reasonable efforts to comply with the document entitled "IPC Practices No. 26: Safe and Secure Disposal Procedures for Municipal Institutions" attached as Appendix "B-3".
- 4.4 MHO, MOF and the Service Manager will each store any PI it receives under this Agreement in encrypted files on password-protected computer systems.
- 4.5 MHO, MOF and the Service Manager may store any PI they receive under this Agreement by such other means as may be agreed to by all Parties.
- 4.6 Access to the PI will be limited to persons who need to know the PI for the purposes of administering the Program and who are authorized by an MHO, MOF or Service Manager designated official identified in Appendix "C" to access the PI for the purposes of administering the Program. The parties acknowledge that the persons identified in Appendix "D" have such a need to know and are so authorized. All Parties will put the appropriate procedures in place to ensure that the PI is accessed only by such persons.
- 4.7 MHO, MOF and the Service Manager will immediately give notice to the other of any loss, suspected loss, unauthorized access to or unauthorized use or disclosure of the PI provided under this Agreement. This notice must be provided to the relevant official identified in Appendix "C" and must include:
- (a) a description of the relevant PI;
  - (b) the date on which and the place at which the PI was lost or subject to unauthorized access or disclosure;

- (c) the circumstances surrounding the loss or unauthorized access or disclosure;
- (d) the extent of the known or probable loss, or unauthorized access or disclosure, and the identities of any unauthorized persons who had or are believed to have had access to PI;
- (e) the actions taken or contemplated to remedy the loss or unauthorized access or disclosure; and
- (f) any other relevant details.

MOF and MHO will also provide this notice to their own Freedom of Information and Privacy Co-ordinators. The Service Manager will provide the notice to their own Municipal Freedom of Information and Privacy Co-ordinator. MHO will provide notice to the Information and Privacy Commissioner. The affected Party shall immediately take reasonable steps to prevent the recurrence of any loss or unauthorized use, access or disclosure of the information.

- 4.8 A written follow-up report on an event described above is to be forwarded as soon as possible by MHO, MOF or the Service Manager to the others as applicable. The report will outline the results of any investigation conducted following the initial search and notification. The report shall include the steps taken to prevent the loss from recurring. Follow-up may also include telephone or written communication between MHO, MOF, the Service Manager and the IPC.

## **5.0 CONDITIONS AND PROCEDURES FOR THE PROVISION OF PI**

5.1 In order to maintain the confidentiality of PI, MHO, MOF and the Service Manager agree that:

- (a) prior to requesting or disclosing PI, all Parties will ensure that the Applicant has properly completed and signed the certification and consent area of the Application Form;
- (b) except with respect to the PI referred to in the second sentence of section 3.1, prior to requesting or disclosing PI, all Parties will ensure that the Applicant is reflected on the most current list provided under section 3.5;
- (c) requests by any party for PI from any other party must be made in writing or by email by a designated official of the requesting Party and a designated official must authorize the release of the PI;
- (d) the PI shared will be disclosed and used solely for the purpose of administering the Program; and
- (e) only authorized persons who need to know the PI for the purposes of administering the Program will have access to and use PI obtained under this Agreement.

5.2 MHO, MOF and the Service Manager shall each ensure that the information provided to the other under this Agreement will be as accurate and complete as possible. However, all Parties recognize that complete accuracy cannot be guaranteed and that neither party shall hold the other responsible for incomplete or inaccurate transmission of information.

## **6.0 RETENTION AND SECURITY**

6.1 MHO, MOF and the Service Manager will each retain the PI that it receives from the other for only the minimum period that is legally and administratively required for the Program. MHO, MOF and the Service Manager will destroy the PI at the end of the retention period in accordance with FIPPA and MFIPPA, as applicable, and the best practices and guidelines listed in section 4.3.

6.2 The following principles will govern the physical destruction of the PI:

- (a) record disposal and destruction should be carried out in a way that protects the confidentiality of any information it contains and in accordance with FIPPA and MFIPPA, as applicable, and the best practices and guidelines listed in section 4.3; and

- (b) where a record is authorized for destruction, all copies of it, including security and backup copies, must be destroyed.

## **7.0 DESIGNATED OFFICIALS**

- 7.1 MHO, MOF and Service Manager officials responsible for the overall administration and security of this Schedule are identified in Appendix "C".

## **8.0 COMPLIANCE LETTER**

- 8.1 Upon request, the Service Manager will provide MHO with a letter signed by the designated official of the Service Manager identified under Appendix "C" (i) outlining the Service Manager's protections and procedures relating to the security and confidentiality of the PI related to this Agreement and (ii) confirming that the Service Manager is in compliance with the PI related provisions of this Agreement.

## **9.0 STATUTORY AUTHORITIES**

- 9.1 The statutory authorities for personal information sharing under this Schedule are set out in Appendix "E".

**APPENDIX “A”**  
**PERSONAL INFORMATION TO BE EXCHANGED**

**“A-1”**

MHO may provide the following information to the Service Manager:

- Applicant’s First Name and Last Name
- Application Number
- Application Status (e.g. pending, to be determined, ineligible, eligible, etc.)
- Applicable occupancy standards
- Any other personal information related to an Applicant or client to resolve any program related issues (e.g. duplicate application, temporary shelter issues, suspensions, etc.)

**“A-2”**

The Service Manager may provide the following information to MHO:

- Applicant’s First Name and Last Name
- Application Number
- Whether an Applicant qualifies for the special priority category status and is on a the social housing waiting list or is in the SDV-PHB Pilot
- The amount provided to the Applicant in respect of first and last month’s rent, its method of calculation and the date it was provided
- Any other personal information related to an Applicant or client to resolve any Program related issues (e.g. duplicate application, temporary shelter issues, suspensions, etc.)

**APPENDIX “B-1”**

**OFFICE OF THE CHIEF INFORMATION AND PRIVACY OFFICER, MINISTRY  
OF GOVERNMENT SERVICES, “TAKING THE RIGHT STEPS – A  
GUIDE TO MANAGING PRIVACY AND PRIVACY BREACHES”**

**SEE ATTACHED**



**Information, Privacy & Archives  
Ministry of Government and Consumer Services**

# **Taking the Right Steps – A Guide to Managing Privacy and Privacy Breaches**

**Revised Document**

**April 18, 2007**





# TABLE OF CONTENTS

- About This Guide ..... 1
  - Purpose ..... 1
  - Context ..... 1
  
- What is a Privacy Breach? ..... 2
  - Definition..... 2
  - Examples..... 2
  
- Part 1 – Privacy Management ..... 3
  - Prevent Privacy Breaches ..... 5
    - Privacy Audit ..... 6
    - Privacy Impact Assessment ..... 6
    - Threat/Risk Assessment ..... 6
  - Prepare for Privacy Breaches ..... 7
    - 1. Privacy Breach Response Plan..... 7
    - 2. Privacy Breach Response Coordinator ..... 7
    - 3. Privacy Breach Response Team..... 8
    - 4. Third Parties..... 8
  
- Part 2 – Privacy Breach Response Protocol ..... 8
  - Key Players in Responding to Privacy Breaches ..... 8
  - Additional Resources ..... 9
  - Four-Step Protocol..... 10
    - Step 1 – Respond and Contain ..... 11
    - Step 2 – Notify..... 17
    - Step 3 – Investigate ..... 22
    - Step 4 – Implement Change ..... 24
  
- Helpful Resources ..... 26
  
- Appendix 1 - Checklists..... 27

# ABOUT THIS GUIDE

## Purpose

The purpose of this Guide is to help institutions under the Freedom of Information and Protection of Privacy Act prevent, prepare for and respond to any incident involving unauthorized disclosure of personal information (i.e., a privacy breach).

The Guide is divided into two parts:

**Part 1** places the need to address privacy breaches within the broader context of privacy management. Your ability to address privacy breaches will be enhanced if you have a coordinated program designed to protect personal information. A key objective of this Part is to help you manage privacy breaches by providing guidance on how to prevent and prepare for privacy breaches.

This Part will be of particular interest to Chief Administrative Officers and Delegated Decision-Makers responsible for the protection of privacy within institutions.

**Part 2** provides advice on what to do when a breach has occurred. The key objectives of this Part are to help your institution address privacy breaches by:

- increasing awareness of what constitutes a privacy breach;
- creating a standard response process or protocol to enhance consistency of approach across the Ontario Public Service; and
- defining who to notify when a privacy breach has occurred, and providing best practices regarding the timing, method and contents of the notice to the individuals affected by a breach.

This Part will be of particular interest and use to institutions' Freedom of Information and Privacy Coordinators (Coordinators) and Program Managers responsible for responding to privacy breaches.

## Context

This Guide does not replace legislative or other requirements or diminish your responsibility for complying with them. It is intended to supplement the following requirements:

- **Freedom of Information and Protection of Privacy Act (FIPPA):** Institutions subject to FIPPA are required to follow the legislation's rules regarding the collection, use, retention, disclosure and disposal of personal information in their custody or control. Of particular relevance to this Guide are the responsibilities FIPPA places on institutions to secure personal information and protect it from unauthorized access or disclosure.
- **Personal Health Information Protection Act (PHIPA):** PHIPA applies to any institution that is a health information custodian and collects, uses and discloses personal health information. Among other obligations, PHIPA requires custodians to take reasonable steps to protect personal health information from theft, loss, unauthorized use, copying, modification, disposal or disclosure. PHIPA also requires custodians to notify individuals at the first reasonable opportunity if their personal health information is stolen, lost, or accessed by unauthorized persons.
- **Corporate Directives and Guidelines:** In addition to the statutory obligations, institutions are required to follow rules related to privacy, information management, information technology, and security defined in corporate directives, and are encouraged to follow best practices outlined in related guidelines.<sup>1</sup>

## WHAT IS A PRIVACY BREACH?

### Definition

For the purposes of this Guide, a privacy breach is defined as an incident involving unauthorized disclosure of personal information in the custody or control of an institution covered by FIPPA. This would include personal information being stolen, lost, or accessed by unauthorized persons.

### Examples

Circumstances that could lead to a privacy breach include:

- personal information faxed to a wrong number or mailed to a wrong address or person;

---

<sup>1</sup> The Ontario Government's directives, guidelines, standards and policies regarding information management and security may be found on the iNetwork Intranet site at: <https://intra.sse.gov.on.ca/inetwork/resourcecentre/Pages/subject.aspx>, and on the Cyber Security Intranet site at: [http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/\(vwReadPagesByRefId\\_Content\)/sec2006.04.27.13.50.07.NWV\\_page?open](http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/(vwReadPagesByRefId_Content)/sec2006.04.27.13.50.07.NWV_page?open).

- loss or theft of equipment containing personal information (e.g., memory sticks, disks, laptops, filing cabinets, photocopiers, fax machines or other devices with memory capabilities);
- disposal of equipment without secure destruction of the personal information it contains;
- use of laptops, disks, memory sticks, briefcases or other equipment to store or transport personal information outside of your office without adequate security measures;
- inappropriate use of electronic devices to transmit personal information (e.g., unsecured personal digital assistants, cell phones, or fax machines);
- intrusions into your buildings, file storage containers, or computer systems and networks;
- insufficient controls to protect personal information; and
- insufficient restrictions on access or editing rights to personal information.

## PART 1 – PRIVACY MANAGEMENT

Protection of personal information is a core business function that needs to be effectively managed. Privacy management applies common management principles (e.g., planning, directing, controlling, evaluating) to the personal information collected, used, disclosed, retained and destroyed by institutions. It involves establishing and following disciplined and consistent practices for the management of personal information. To be effective, it also requires leadership and a commitment to privacy protection at all levels of your organization.

An effective privacy management program will:

- **Define Roles and Responsibilities:** The head of an institution is accountable for compliance with FIPPA. In most institutions, some or all of the powers or duties of a head will have been delegated to an officer or officers (e.g., Delegated Decision-Makers and Coordinators). However, the management of privacy needs to be an institution-wide initiative, engaging staff at all levels. Your staff are accountable for protecting the personal information in their custody and control.
- **Align Business Practices:** Integrate the protection of personal information into your programs, systems, and policies and use tools (e.g., Privacy Impact Assessments) that require you to consider privacy on a proactive basis. The public expects government services to be provided on a cost-effective basis. It is easier and less expensive to build privacy protective measures into technology, contracts,

programs, practices and business continuity plans from the beginning, than to retrofit them after privacy breaches occur. Therefore, consider privacy when identifying your strategic priorities, deliverables and performance measures. Privacy should not be an after-thought.

- **Educate and Enhance Awareness:** Education about privacy, as well as FIPPA's requirements, will help your staff understand why privacy is important and how to protect it. Education and awareness are vital to creating a culture of privacy.<sup>2</sup>
- **Monitor and Evaluate Privacy Management Program:** Proper oversight is crucial to the success of any program. Therefore, periodically review your privacy policies and practices, and commit to ongoing improvement in compliance.

Privacy management programs will differ according to institutions' needs and capacity. An institution with limited personal information holdings will have different needs than an institution with a high volume of transactions involving sensitive personal information. This customization of approach is necessary and useful to enable your institution to meet the specific needs of your clients and programs.

Addressing privacy breaches is an important part of your institution's privacy management programs. When a privacy breach occurs, both the individuals affected by the breach and the institutions involved are potentially vulnerable to adverse consequences:

**Individuals:** Unauthorized disclosure of personal information violates an individual's privacy. It creates the potential for harm, including identity theft and other forms of fraud, physical safety issues such as stalking or harassment, financial loss, adverse impact on employment or business opportunities, and damage to reputation.

**Institutions:** In addition to not meeting the legal requirements of FIPPA, there are other consequences, including:

- reduced productivity as staff respond to a breach or deal with a complaint;
- lost public trust and confidence due to public disclosure of a major privacy breach;
- cost of emergency measures necessary to control a breach; and
- replacement costs of hardware, software and data affected by the breach.

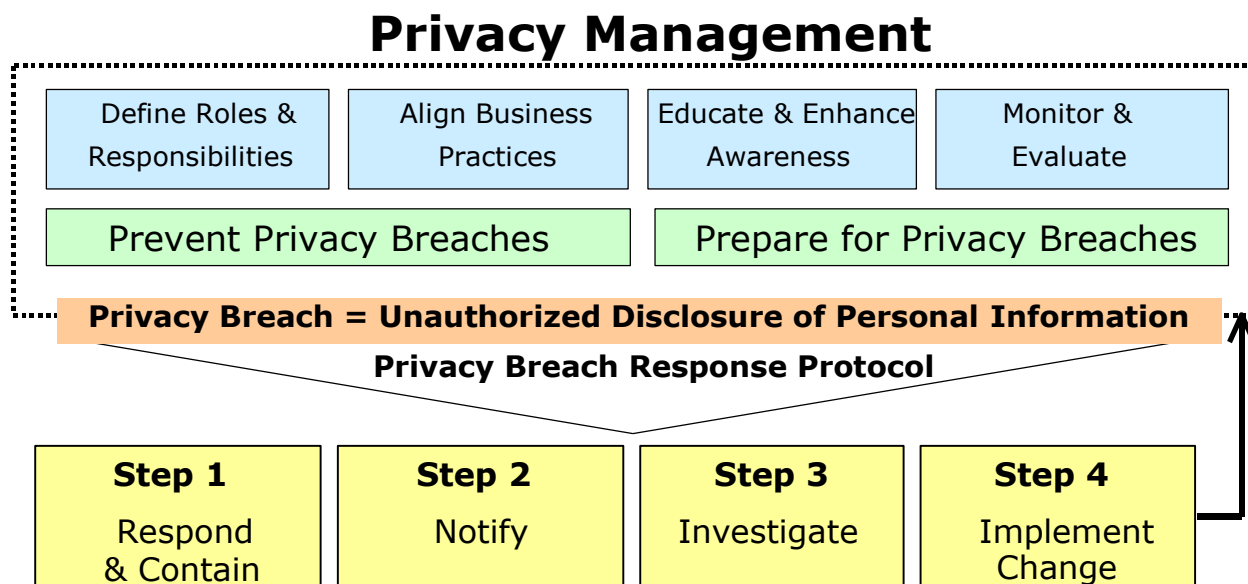
Preventing privacy breaches, and preparing to respond to them, are critical components of privacy management.

---

<sup>2</sup> The Centre for Learning and Leadership offers several classroom and e-learning courses on privacy.

Figure 1 illustrates how an over-arching privacy management program helps you address privacy breaches.

Figure 1 – Privacy Breach Response Protocol within Privacy Management Context



## Prevent Privacy Breaches

Three areas are of particular importance to your efforts to prevent privacy breaches:

- **Education:** Staff (at all levels) need to understand their responsibilities to comply with FIPPA, and how to protect personal information in their work activities.
- **Security:** An effective security program is essential to prevent privacy breaches. As threats to security are ever-changing, there is no one type of security program that would mitigate the risks of all types of privacy breaches. Physical, technical and procedural safeguards appropriate to your programs and the scope and nature of the personal information in your custody and control need to be included in your security program.<sup>3</sup>
- **Third Parties:** If third party service providers collect, use, retain, disclose or destroy any personal information on your behalf, require them to implement and maintain appropriate security and privacy safeguards. Take reasonable steps to monitor and enforce their compliance with the privacy and security requirements defined in your contracts or service agreements.<sup>4</sup>

<sup>3</sup> See Office of the Information and Privacy Commissioner/Ontario (IPC) Order HO-004 for discussion of security regarding mobile computing devices at: [http://www.ipc.on.ca/images/Findings/up-3ho\\_004.pdf](http://www.ipc.on.ca/images/Findings/up-3ho_004.pdf).

<sup>4</sup> See the Guidelines for the Protection of Information When Contracting for Services for additional information at:

The use of the tools outlined below will help you prevent privacy breaches by identifying inappropriate information management practices and inadequate security and privacy measures. [Appendix 1](#) contains a checklist of key questions to help you identify areas, policies and practices that need to be improved in order to prevent privacy breaches.

## **Privacy Audit**

The purpose of a privacy audit, which is a self-assessment tool, is to identify:

- your personal information holdings;
- the information needs of your program areas or corporate functions; and
- your existing privacy and information management policies, practices and procedures.

A privacy audit will help you determine the extent to which personal information in your institution's custody and control is maintained in accordance with FIPPA (i.e., identify short-falls).<sup>5</sup>

## **Privacy Impact Assessment**

The purpose of a Privacy Impact Assessment is to help you identify the:

- internal and external risks to privacy of a proposed initiative (e.g., new technology, information system, or program) in advance of implementation; and
- measures to address those risks – one of which could be a privacy breach if the initiative proceeds without sufficient safeguards in place.<sup>6</sup>

## **Threat/Risk Assessment**

The purpose of a Threat/Risk Assessment is to:

- assess security threats and vulnerabilities;
- document your existing security measures; and

---

<https://intra.sse.gov.on.ca/inetwork/resourcecentre/Documents/Guidelines%20for%20the%20Protection%20of%20Information%20when%20Contracting%20for%20Services.pdf>.

<sup>5</sup> The Guide and Checklist for Managing Personal Information is available on the IPA Intranet site: <https://intra.sse.gov.on.ca/inetwork/resourcecentre/Documents/Guide%20and%20Checklist%20for%20Managing%20Personal%20Information.pdf>.

<sup>6</sup> The Privacy Impact Assessment guides and tools are available on the IPA Intranet site at: <https://intra.sse.gov.on.ca/inetwork/managinginformation/privacy/Pages/pia.aspx>.

- recommend appropriate and necessary security safeguards.

This tool will help you identify security issues that could have bearing on the protection of personal information and contribute to a privacy breach.<sup>7</sup>

## **Prepare for Privacy Breaches**

Despite your best efforts, privacy breaches will occur and, in order for you to be able to respond in a timely and effective manner, planning is essential. Focus your efforts on the four areas, outlined below, when preparing to respond to privacy breaches.

To help you prepare to respond to a privacy breach in a timely and effective manner, consider and answer the questions outlined in checklist in [Appendix 1](#).

### **1. Privacy Breach Response Plan**

Develop a plan that documents how the four steps of the privacy breach response protocol, outlined in Part 2 of this Guide, are adapted and applied in your institution. The creation of a response plan may involve documenting your existing practices for dealing with privacy breaches.

One of the key components of a response plan is defining when a privacy breach needs to be reported to your Deputy Minister's Office. The Deputy Minister is responsible for determining if a breach needs to be reported to your Minister's Office.

Having such a plan will enable you to respond to privacy breaches in a coordinated manner. As part of your privacy management program, evaluate the effectiveness of your response plan annually and implement changes, as necessary.

### **2. Privacy Breach Response Coordinator**

Designate one person as responsible and accountable for developing your privacy breach response plan and for coordinating the implementation of that plan. Having this coordinating role helps rationalize planning and preparation, as well as enhances continuity and consistency of approach for privacy breaches.

In most institutions, the Freedom of Information and Privacy Coordinator would be the logical choice for coordinating the development and implementation of a privacy breach response plan given their knowledge and experience.

---

<sup>7</sup> Information about the Threat/Risk Assessment is available on the Cyber Security Intranet at: [http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/\(vwReadPagesByRefId\\_Content\)/sec2006.06.26.09.57.49.JDN\\_page?open](http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/(vwReadPagesByRefId_Content)/sec2006.06.26.09.57.49.JDN_page?open).



### **3. Privacy Breach Response Team**

Identifying key players or creating a “response team” in advance of a privacy breach will help you prepare. If you already have a privacy working group or committee, involve them in preparing for and responding to privacy breaches.

The roles and responsibilities of the players involved in responding to a privacy breach are interdependent. All players responding to a breach need to work in a co-ordinated manner as a team. Strong communication amongst the players and consistent practices makes the handling of a privacy breach more effective and efficient.

Part 2 of this Guide outlines the key players that need to be involved in all privacy breaches.

### **4. Third Parties**

Under FIPPA, your institution need not have custody of personal information to be responsible for its protection. As with prevention, if third party service providers collect, use, retain, disclose or destroy personal information on your behalf, in your contracts and service agreements require them to:

- be prepared to respond to privacy breaches in a manner consistent with your privacy breach response plan; and
- immediately report breaches to a designated contact at your institution.

## **PART 2 – PRIVACY BREACH RESPONSE PROTOCOL**

While Part 1 focuses on privacy management and the need for your institution to take action to prevent and prepare for privacy breaches, this Part of the Guide focuses on what you need to do once a privacy breach has occurred.

### **Key Players in Responding to Privacy Breaches**

The areas and positions needed to respond to a privacy breach will vary according to the nature of the institution and the type of breach. However, the following players need to be involved when your institution responds to any privacy breaches. The allocation of responsibilities may shift depending upon an institution’s business practices.

**Staff:** Staff, in all areas and at all levels of your institution, will play key roles in identifying, documenting and containing a breach. Staff dealing with clients or the public on a regular basis (e.g., Call Centre personnel) need to be aware of what to do if a privacy breach is reported by an external source.

**Program Manager:** Program Managers will be responsible for alerting the Coordinator of a breach or suspected breach and working with the Coordinator to implement the four steps of the response protocol. They need to be familiar with this Guide, your institution's privacy breach response plan, the identity and contact information of the Coordinator and delegates, and fully understand their own role and responsibilities in the process.

**Freedom of Information and Privacy Coordinator:** The Coordinator will play a central role in your institution's response to a privacy breach by:

- identifying the privacy implications of a breach and providing advice to the area(s) affected by the breach;
- ensuring the appropriate players are notified or involved in responding to the breach; coordinating your institution's activities, products and communications; and
- acting as the point of contact for the Office of the Information and Privacy Commissioner/Ontario (IPC) and the Information, Privacy and Archives Division (IPA), Ministry of Government and Consumer Services (MGCS).

**Delegated Decision-Maker:** In most institutions, the responsibility for protecting the personal information affected by the privacy breach will have been delegated to an identified position, known as a Delegated Decision-Maker. These individuals are key decision-makers in responding to privacy breaches and, therefore, need to be familiar with your institutions' response plan and their role and responsibilities.<sup>8</sup>

**Third Party Service Provider:** Increasingly, institutions use third parties to carry out or manage programs or services on their behalf. In such circumstances, institutions usually retain responsibility for protecting personal information in accordance with FIPPA. Therefore, third party service providers need to know their roles and responsibilities if a privacy breach occurs when they have custody of personal information. Require your service providers to inform you of all actual and suspected privacy breaches.

## Additional Resources

Depending upon the nature of a breach, it may be appropriate for your Coordinator or the Program Manager of the area affected by the breach to consult with or involve other appropriate areas, such as the following:

---

<sup>8</sup> If your institution does not have a Delegated Decision-Maker, the Director or Manager of the program area could assume this role.

**Legal Services:** The legal ramifications of a privacy breach need to be identified, including the impact on contracts with third party service providers. Seek legal guidance if there is reason to believe a breach is the result of a criminal act and law enforcement needs to be contacted.

**Information Technology:** Information technology staff have the technical skills necessary to identify a privacy/security breach, analyze what has happened and what needs to be done to contain the breach, as well as to implement short- and long-term measures to protect personal information (e.g., changing access controls, strengthening firewalls, taking systems off-line, etc.).

**Issues Management/Communications:** Involve this area if there is a need to develop and implement an issues management strategy (i.e., if a breach has or is likely to become a matter of public interest), or to inform the media and, by extension, the public (within the constraints imposed by FIPPA, security needs and law enforcement interests).

**Contingency/Disaster Planning:** If a privacy breach occurs as part of a larger incident within your institution or across institutions, your Coordinator will work with the appropriate areas or individuals responsible for contingency or disaster planning. Human Resources: Involve your human resources area when a staff member is the possible target of an incident or is suspected of causing a privacy breach.

**Physical Security/Facility Management:** Involve your physical security and facilities management areas if a privacy breach occurs as a result of a failure of physical security measures, or if access to facilities is necessary (e.g., a compromised workstation is locked in an office).

**Emergency Management and Security:** This area is responsible for administering the personnel screening checks and needs to be notified if a privacy breach has implications on a security clearance (e.g., theft of personal information by a contractor).

**IPA/Other Coordinators:** For advice on how to respond, consult the IPA or other institutions' Coordinators with experience managing privacy breaches.

## Four-Step Protocol

Given the diversity of institutions and the varied nature of privacy breaches, no “one size fits all” response protocol is possible or practical. You will need to tailor your actions to ensure they are proportional and appropriate to each privacy breach. There are, however, a number of essential steps to be followed when any privacy breach occurs:

1. Respond and Contain
2. Notify

### 3. Investigate

### 4. Implement Change

These steps may need to take place simultaneously, or in rapid succession, depending upon the circumstances. Each step does not have to be completed before beginning the next.

Each step of the protocol is described below and includes suggested roles and responsibilities for the key players. [Appendix 1](#) contains a checklist of key questions to consider and answer when determining if you have taken adequate or appropriate measures to complete each step.

## **Step 1 – Respond and Contain**

Initiate this step as soon as a privacy breach, suspected breach or attempt at unauthorized access has been discovered. Within this one step, five actions are critical:

1. report the privacy breach to key players within the institution, to the IPA and, if necessary, to law enforcement;
2. assess the situation to determine if a breach has occurred and what needs to be done;
3. contain the privacy breach;
4. document the breach and containment activities; and
5. brief senior management.

### **1. Report**

**Internal Reporting:** A privacy breach or suspected breach needs to be reported to the Program Manager of the area affected by the breach, your institution's Coordinator, and the Delegated Decision-Maker responsible for the area involved in the privacy breach.<sup>9</sup>

**IPA, MGCS:** Your Coordinator needs to inform the IPA of all privacy breaches within 24 hours of discovery. In addition, alert the IPA if you plan to report a privacy breach to your Deputy Minister's Office.<sup>10</sup>

---

<sup>9</sup> Notify the Program Area Director if there is no Delegated Decision-Maker.

<sup>10</sup> The IPA acts as an advisor to the minister responsible for the administration of FIPPA and, therefore, needs to be aware of any escalating privacy issues.

**Law Enforcement:** If you think a privacy breach involves illegal activities, the Program Manager or Coordinator needs to report the breach to the appropriate law enforcement agency. Consult your Legal Services Branch and Deputy Minister’s Office prior to contacting law enforcement.

Key Players	Suggested Responsibilities
Staff	<p>Inform your Manager immediately upon becoming aware of a breach or suspected breach.</p> <p>Provide the Manager with as much information as known at the time (e.g., what happened, when, how breach was discovered, and if any corrective action has already been taken).</p> <p>If Manager is unavailable, escalate reporting of breach to the next level of management.</p>
Program Manager	<p>Alert the Coordinator and provide as much information about the breach or suspected breach as is currently available.</p> <p>After appropriate consultation, contact law enforcement, if necessary.</p>
Coordinator	<p>If a privacy breach is identified by external source (e.g., individual, other institution, third party service provider, or IPC), contact appropriate area(s) to respond to the breach.</p> <p>Report breach and provide updates to the IPA.</p>
Third Party Service Provider	<p>Inform designated party at institution as soon as a privacy breach or suspected breach discovered.</p> <p>Fulfill contractual obligations.</p>

## 2. Assess

Once an incident or suspected incident has been reported to your Program Manager and Coordinator, they need to immediately determine if a privacy breach has occurred. In making this assessment, two important questions need to be answered:

### Is personal information involved?

Not all data in the custody or control of an institution is personal information. Therefore, the first part of your assessment is to identify the type of information affected by the incident.

**Definition:** Personal information is defined in subsection 2(1) of FIPPA as recorded information about an identifiable individual (i.e., natural person) and includes, but is not limited to: race, nationality, religion, age, sex, marital status, education, medical or criminal history, financial information, identifying numbers, address, telephone number, fingerprints, blood type, and opinions. The definition of personal information is not exhaustive – an institution may have other types of personal information in its custody or control.

Personal information may include information that is not recorded (e.g., a verbal disclosure). Also, if there is a reasonable expectation that an individual can be identified from the information disclosed (either alone or when combined with other information), such information will likely qualify as personal information.

### Has an unauthorized disclosure occurred?

Unauthorized disclosure, whether it is intentional, inadvertent, or as a result of a criminal activity, is the defining activity for privacy breaches. It is the “threshold” or “trigger” mechanism for the application of this Guide.

If the answer to both questions is “yes”, a privacy breach has occurred and you need to follow the rest of the privacy breach response protocol outlined in this Guide.

**Note:** Institutions have a responsibility to protect personal information and to secure general records, particularly sensitive records.<sup>11</sup> Respond to security breaches involving general records in accordance with established rules and regulations. Report incidents involving unauthorized collection, use, retention or disposal of personal information to your Coordinator.

Key Players	Suggested Responsibilities
Program Manager and Coordinator	<p>Work together to:</p> <ul style="list-style-type: none"> <li>▪ Obtain all available information about the nature of the breach or suspected breach (e.g., when, where, whose personal information involved, how much personal information involved, verbal disclosure or hard copies involved, etc.).</li> <li>▪ Determine what happened (e.g., did a privacy breach actually occur, what personal information was involved, etc.?) and what needs to be done.</li> <li>▪ Answer questions in Step 1 Checklist related to</li> </ul>

<sup>11</sup> The Information Security & Privacy Classification Policy and the Information Security & Privacy Classification Operating Procedures are available at: [http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/\(vwReadPagesByRefId\\_Content\)/sec2006.06.26.12.06.06.LVU\\_page?open](http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/(vwReadPagesByRefId_Content)/sec2006.06.26.12.06.06.LVU_page?open)

Key Players	Suggested Responsibilities
	assessing a privacy breach.

### 3. Contain

Take immediate action to contain a privacy breach and to alleviate its consequences for both the individuals whose personal information was involved in the incident and your institution.

Key Players	Suggested Responsibilities
Program Manager	Work with Coordinator to: <ul style="list-style-type: none"> <li>▪ Undertake all appropriate action to contain breach and mitigate its impact.</li> <li>▪ Answer questions in Step 1 Checklist related to containing a privacy breach.</li> </ul>
Coordinator	Involve all appropriate parties in responding to privacy breach (e.g., Legal Services, Information Technology, Human Resources, Facility Management, etc.).  Provide advice on appropriate steps to respond to a privacy breach.  Work with the IPA, as required, if privacy breach impacts multiple institutions.
Third Party Service Provider	Take all necessary action to immediately contain the privacy breach.  Fulfill contractual obligations.

### 4. Document

Documenting the details of a privacy breach and your containment activity allows you to implement the correct remedial measures, respond to an investigation by the IPC, and evaluate your institution's response. Such an evaluation is an important part of privacy management.

Key Players	Suggested Responsibilities
Staff	<p>Document what happened (e.g., staff disclosed personal information without authority, intruder, third party service provider alert, equipment containing personal information lost or stolen, etc.), when, how breach was discovered, and what corrective action was taken.</p> <p>If breach identified by external source (e.g., individual, other institution, or third party service provider), document information provided, including contact information for follow-up, and any instructions given to reporting party (e.g., asking caller to mail back documents sent to wrong address). Immediately report breach to Manager.</p>
Program Manager	Ensure details of breach and corrective action are appropriately documented.
Third Party Service Provider	<p>Document what happened (e.g., staff disclose personal information without authority, intruder, equipment containing personal information lost or stolen, etc.), when, how breach was discovered, and what corrective action was taken.</p> <p>Fulfill contractual obligations.</p>

## 5. Brief

Briefing senior management and, potentially, your Minister's Office is another crucial part of internal reporting, and needs to be done at the discretion of your Coordinator, Delegated Decision-Maker and Deputy Minister's Office. The Deputy Minister will determine if briefing your Minister's Office is necessary.

It is recommended you report any privacy breach to your Deputy Minister's Office in the following circumstances:

- There is reasonable expectation of risk of harm to the individuals whose personal information is involved in the breach.
- The personal information at issue in the breach is very sensitive (e.g., personal health information).
- The scope of the breach is large in terms of the number of individuals affected or the amount of personal information disclosed.
- The scope of the breach is unknown and, therefore, you cannot immediately implement the steps necessary to contain it.



- The breach is the result of an unlawful act and law enforcement needs to be notified.
- The breach was identified to your institution by the media or the IPC.
- The breach is likely to result in media coverage.

When briefing your senior management or Deputy Minister’s and Minister’s Offices, include the following information:

- The nature and scope of the privacy breach (e.g., how many people are affected, what type of personal information is involved, the extent to which you have contained the breach) or, if the nature and scope are not known at the time of the briefing, that they are still to be determined.
- What steps you have already taken, or will be taking, to manage the privacy breach.
- Your plans to notify the individuals affected by the privacy breach and, if appropriate, the IPC and other parties.
- Your timetable for providing senior management with regular updates about the breach and your ongoing management of it.

Depending upon the nature of the privacy breach and your institution, it may be appropriate to brief your senior management, Deputy Minister’s and Minister’s Offices early in the response process. This will enable them to know what has occurred and how you are managing the privacy breach (i.e., what actions you are taking and planning, and when they will be updated on developments). This initial briefing may need to occur before you have fully completed your investigation.

Keeping senior management and the Deputy Minister’s and Minister’s Offices informed throughout the life cycle of a privacy breach will help them understand how your institution is addressing the breach and mitigating its consequences.

Key Players	Suggested Responsibilities
Program Manager and Coordinator	Work together to: <ul style="list-style-type: none"> <li>▪ Evaluate the circumstances of the privacy breach (outlined on pages 19 and 20) to determine its severity and scope, in consultation with Legal Services and Issues Management/Communications.</li> <li>▪ Develop briefing materials, including recommendations on:               <ul style="list-style-type: none"> <li>- response activities to manage the breach;</li> <li>- notice to the individuals affected by the breach</li> </ul> </li> </ul>

Key Players	Suggested Responsibilities
	<p>and the IPC; and</p> <ul style="list-style-type: none"> <li>- need to report the breach to the Deputy Minister's Office.</li> </ul> <ul style="list-style-type: none"> <li>▪ Brief Delegated Decision-Maker(s) responsible for protection of the personal information involved in the privacy breach, as appropriate throughout the course of your institution's response.</li> </ul>
Coordinator	If a privacy breach is to be reported to your Deputy Minister's Office, inform the IPA.
Delegated Decision-Maker (if other than the Deputy Minister)	<p>Brief senior management and, if appropriate, the Deputy Minister's Office, as necessary.</p> <p><b>Note:</b> The Deputy Minister will determine if briefing the Minister's Office is necessary.</p>

## **Step 2 – Notify**

In addition to the reporting outlined in Step 1, there is a need to notify other parties of the privacy breach, including, most importantly, the individuals whose personal information was involved in the incident (i.e., the data subject).

### ***Data Subject***

Notifying the data subject of a privacy breach should be your default course of action when one has occurred. The purpose of providing notice of a privacy breach to the individuals whose personal information was involved in the incident is to provide them with sufficient information about:

- what happened;
- the nature of potential or actual risks of harm; and
- appropriate action to take to protect themselves against harm.

Such notice supports the purposes of FIPPA and your responsibility to protect the privacy of individuals with respect to personal information. It is also consistent with the fair information practices of openness and accountability.

Key Players	Suggested Responsibilities
Program Manager and Coordinator	Work together to: <ul style="list-style-type: none"> <li>▪ Determine if there is a compelling reason for not notifying the data subjects of the privacy breach.</li> <li>▪ If no, determine content, timing and method of notice in accordance with the best practices (below).</li> <li>▪ Ensure notice is undertaken in an approved and coordinated manner.</li> <li>▪ Ensure there is adequate support available to notified individuals.</li> <li>▪ Answer questions in Step 2 Checklist related to notifying data subjects.</li> </ul>
Delegated Decision-Maker	Approve all decisions regarding notice to all external parties (e.g., data subject or IPC).
Third Party Service Provider	Participate in notifying the individuals affected by the breach in accordance with contractual obligations.

Below are listed best practices regarding the timing, method and content of notices to the individuals affected by a privacy breach.

### Timing of Notice

- Notify as soon as reasonably practicable.
- Do not compound the potential harm caused by a privacy breach by providing premature notice based on incomplete facts or taking any action that might make identity theft or other harm more likely to occur as a result.
- Delay notice if:
  - law enforcement determines immediate notice would impede a criminal investigation; or
  - the breach resulted from a security or information system failure, restore and test the integrity of the system before disclosing details of the breach.
- Provide notice to the data subjects as soon as the reason for delay has been resolved.

## **Method of Notice**

- Make every reasonable effort to directly notify each individual of the privacy breach if identities and contact information of the individuals affected by a privacy breach are known.
- Ensure notice is provided to correct individual and avoid false positives (i.e., when the notice is given to individuals whose personal information was not involved in the breach). Document the process for determining who will be notified.
- Determine if personal representatives or other authorized parties need to be notified instead of the data subject due to issues of capacity, age, language, etc.
- Determine if the seriousness or scope of the privacy breach warrants some kind of indirect notice using public communications channels (e.g., website or media) if direct notification is not possible or reasonably practicable.

*If notifying by telephone or in person:*

- Develop a script so each data subject receives consistent and complete information.

*If notifying in writing:*

- Send written notice by mail to the last known mailing address, by another means that can prove receipt of the notice, or deliver it personally.
- Send or deliver notices separately from any other mailings from your institution.
- Identify your institution on the envelope.
- Format in manner that makes your notice readable, understandable and useful.

## **Content of Notice**

- Make every reasonable effort to provide consistent messaging, particularly when notice is to be provided verbally by multiple players.
- Include the following information in written or verbal notices to the individuals affected by a privacy breach:
  - clear identification of your institution and contact information (e.g., a toll-free telephone number, website and postal address) of the individual/area where notice recipient can make inquiries, verify validity of notice and obtain additional information about the breach;
  - a brief description of what happened and when;

- to the extent possible, a generic description of the types of personal information involved in the breach, including if any unique identifiers or sensitive personal information were involved in the breach.
- a description of what you have done or are doing to contain the breach, mitigate its impact, investigate the cause and protect against any further breaches;
- a brief explanation of the potential or actual risks or threats to individuals impacted by the breach;
- an explanation of what action individuals can take to protect themselves, given the nature of the privacy breach (e.g., if identity theft is a reasonable possibility, advise the data subjects to contact their bank, credit card company, credit reporting bureau to inform them of the breach; check and monitor all bank accounts, credit card and other financial statements for any suspicious activity; and obtain a copy of their credit report);
- identify sources where individuals can find more information on identify theft, if reasonably likely to occur, and where they can report occurrences;
- an explanation of the types of assistance available to individuals from the institution or other sources;
- an indication if you have contacted the IPC and if it is investigating the privacy breach;
- a brief explanation of the individual's right to complain to the IPC about your institution's handling of their personal information; and
- contact information for the IPC.

## **Exceptions**

Notifying the individuals affected by a privacy breach may not be appropriate, reasonably possible, or necessary in the following limited circumstances:

- law enforcement determines notice would impede a criminal investigation;
- notice is not in the individual's interest (e.g., notice could potentially endanger an individual or result in greater harm to the individual);

- notice would serve no useful purpose<sup>12</sup> (e.g., if all the personal information involved in the privacy breach is: already publicly available; recovered before an unauthorized party could possibly access it; or protected by technology, such as encryption, that would mean unauthorized access and use of the data is not reasonably possible); or
- it is not possible to provide notice (e.g., identity of individuals affected by breach is not known).

If you are considering not notifying the data subjects of a privacy breach, consultation with the IPA is recommended.

### **Office of the Information and Privacy Commissioner/Ontario**

Determine if notifying the IPC is appropriate. Notice to the IPC is recommended when privacy breaches involve sensitive personal information or large numbers of individuals, or when the risk of harm to the data subjects is high.

The IPC will be able to provide advice and support to your institution response to a breach.

<b>Key Players</b>	<b>Suggested Responsibilities</b>
Program Manager	Work with Coordinator to determine if IPC needs to be notified of privacy breach.
Coordinator	Contact IPC, if appropriate.

### **Other Parties**

Depending upon the nature of the incident, it may be necessary or appropriate to notify other external parties of a privacy breach (e.g., other institutions or jurisdictions, technology suppliers, etc.). The Program Manager, Coordinator and Delegated Decision-Maker will need to make this determination on a case-by-case basis. Involve Legal Services in this decision if legal or contractual obligations are affected by a privacy breach.

---

<sup>12</sup> In an order related to a specific privacy breach under PHIPA, the IPC found that, in the absence of evidence that any records were lost or stolen, notifying potentially thousands of patients whose records were abandoned but later recovered by the IPC, would serve no useful purpose. Notice in this case would be based on a remote possibility of unauthorized access rather than a probability. IPC Order HO-003, December 2006, pp. 9-10.

Key Players	Suggested Responsibilities
Delegated Decision-Maker	If privacy breach impacts other institutions, organizations, third parties or jurisdictions, notify appropriate parties in accordance with Memoranda of Understanding or other defined protocols, as necessary.

### **Step 3 – Investigate**

#### ***Internal***

Once you have contained the privacy breach:

- identify and analyze the events that led to the privacy breach;
- evaluate what you did to contain it; and
- recommend remedial action to help prevent future breaches.

In most circumstances it will be appropriate for you to investigate your own privacy breaches. Depending upon the nature and scope of the breach, you may want to involve your internal audit programs in this process.

Document the results of your internal investigation including:

- background and scope of your investigation;
- legislative implications;
- how you conducted the assessment (who did it, who was interviewed, what questions asked, what policies and practices considered, etc.);
- the source and cause of the privacy breach;
- an inventory of your systems and programs affected by the breach;
- determination of the adequacy of your existing security and privacy policies, procedures and practices;
- assessment of the effectiveness of your institution’s response to the breach (i.e., implementation of Step 1 and Step 2); and
- findings including a chronology of events and recommendations for remedial actions.

Inform your senior management of the results of the investigation so they can act upon the recommendations.

One of the most important outcomes of a privacy breach is for your institution to learn from the incident. A “lessons learned” meeting with all parties involved in the breach and response will help you evaluate your existing privacy/security measures and your incident-handling process, and identify necessary changes and improvements.

Each investigation will result in a set of documents outlining the chronology of the privacy breach, the analysis of your response, and the required remedial steps. Over time, this information will help you identify systemic privacy or security weaknesses and threats.

<b>Key Players</b>	<b>Suggested Responsibilities</b>
Program Manager and Coordinator	Work together to assess the privacy breach and your institution’s response, to document findings, and to answer questions in Step 3 Checklist related to investigating privacy breaches.  Involve other parties in investigation, as necessary.
Delegated Decision-Maker	Review internal investigation reports and approve required remedial action.
Third Party Service Provider	Undertake full assessment of privacy breach, in accordance with contractual obligations.

***Office of the Information and Privacy Commissioner/Ontario***

Depending upon the nature of a privacy breach, the IPC may investigate and publicly report on the incident. If this occurs, cooperate fully with the IPC.

Your Coordinator needs to play a key role in your institution’s activities, products and communications with the IPC.

<b>Key Players</b>	<b>Suggested Responsibilities</b>
Program Manager	Make all appropriate information and documents available.
Coordinator	Coordinate your institution’s activities and communication with IPC.
Delegated Decision-Maker	Review IPC investigation report and approve required remedial action.



## **Step 4 – Implement Change**

When determining what changes and remedial action needs to be implemented, consider if it is necessary to:

- review your relevant information management systems to enhance compliance with FIPPA;
- amend or reinforce your existing policies and practices for managing and safeguarding personal information;
- develop and implement new security or privacy measures;
- train your staff on legislative requirements, security and privacy policies, practices and procedures to reduce the potential of future breaches; or
- test and evaluate remedial actions to determine if they have been implemented correctly, and if your policies and practices need to be modified.

In addition, evaluate whether the notice to the data subjects and other relevant parties was effective (e.g., was it done in a reasonably timely manner, were the tone and content of the notice appropriate, and was there sufficient support provided to data subjects?).

<b>Key Players</b>	<b>Suggested Responsibilities</b>
Program Manager	<p>Ensure all appropriate remedial action is undertaken, including necessary modifications to privacy and security measures, policies, practices and procedures.</p> <p>Work with Coordinator to train staff in a timely and effective manner.</p> <p>Follow-up to assess effectiveness of remedial action. Make changes, as necessary.</p>
Coordinator	<p>Evaluate effectiveness of your institution’s response to particular breach, as well as your response plan, and implement improvements, as necessary.</p> <p>Work with Program Manager to answer questions in Step 4 Checklist related to remedial actions and their implementation.</p>
Delegated Decision-Maker	Monitor implementation of remedial action.

<b>Key Players</b>	<b>Suggested Responsibilities</b>
Third Party Service Provider	Take all necessary remedial action to decrease risk of future privacy breaches (e.g., training, enhanced security measures, etc.), in accordance with contractual obligations.

## HELPFUL RESOURCES

Access and Privacy Branch, Alberta Government Services, Conducting a Privacy Audit, December 2004.

British Columbia Medical Association, Office of the Information and Privacy Commissioner for British Columbia, and the British Columbia College of Physicians and Surgeons, Key Steps for Physicians in Responding to Privacy Breaches, June 2006.

British Columbia Medical Association, Office of the Information and Privacy Commissioner for British Columbia, and the British Columbia College of Physicians and Surgeons, Physicians and Security of Personal Information, June 2006.

Office of the Information and Privacy Commissioner for British Columbia, Key Steps in Responding to Privacy Breaches, December 2006.

Office of the Information and Privacy Commissioner for British Columbia, Guidelines for Handling a Privacy Breach, October 2005.

Office of the Information and Privacy Commissioner for British Columbia, Privacy Breach Reporting Form, November 2006.

Office of the Information and Privacy Commissioner/Ontario and Office of the Information and Privacy Commissioner for British Columbia, Breach Notification Assessment Tool, December 2006.

Office of the Information and Privacy Commissioner/Ontario, A Privacy Breach Has Occurred – What Happens Next?, Presentation, September 14, 2001.

Office of the Information and Privacy Commissioner/Ontario, Privacy Assessment: The University Health Network's Response to Recent Breaches of Patient Privacy, July 30, 2002.

Office of the Information and Privacy Commissioner/Ontario, What to do if a privacy breach occurs: Guidelines for government organizations, Revised December 15, 2006.

Office of the Information and Privacy Commissioner/Ontario, What to do When Faced With a Privacy Breach, Guidelines for the Health Sector, June 2006.

## APPENDIX 1 – CHECKLISTS

The following questions can help you identify areas, policies and practices that may need to be improved in order to effectively manage privacy and to prevent, prepare for and respond to privacy breaches.

<b>Prevent Privacy Breaches Checklist</b>
<p><b>Education</b></p> <p>How is staff trained on FIPPA and your institution’s policies, procedures and practices for protecting personal information? How is effectiveness of training determined?</p> <p>Is accountability for privacy protection understood by staff at all levels?</p> <p>How is privacy awareness promoted across your institution?</p> <p>How are the policies, procedures and practices for managing personal information communicated to staff?</p> <p>How is staff informed of new privacy and security issues to be addressed that result from internal reviews, privacy breaches, public complaints and court decisions, or from changes in technology and information management practices?</p>
<p><b>Security</b></p> <p>Are security responsibilities clearly defined and subject to performance evaluation?</p> <p>What are the reasonably foreseeable risks to the security of personal information? Are existing safeguards (physical, technical and procedural) effective at addressing those risks? If not, what needs to be done to implement adequate safeguards?</p> <p>Do the security measures, including policies, practices and procedures, meet the requirements of FIPPA (i.e., protect personal information from unauthorized access, collection, use, disclosure, copying, modification or destruction) and corporate directives and guidelines?</p>

## Prevent Privacy Breaches Checklist

Are intrusion detection technology, policies and procedures in place for identifying, documenting (e.g., audit trail), reporting and responding to security incidents (i.e., actual and attempted attacks or intrusions)?

Is access to personal information (internal and external) limited to users with legitimate needs, and are appropriate controls and authentication measures in place?

What safeguards are in place to ensure personal information is not removed from your offices unless necessary, and that appropriate precautions are in place to protect the security and integrity of the information when outside your offices?

Are appropriate security measures in place for the disposal of personal information and destruction of equipment that may store personal information (e.g., computers, disks, memory sticks, disks, laptops, cell phones, personal digital assistants, filing cabinets, photocopiers, fax machines or other devices with memory capabilities)?

Are appropriate security measures in place for mobile devices, remote access from external network connections, and transmission of personal information over the Internet or other public networks?

How are security safeguards evaluated and adjusted to address new or emerging threats, a material change to your institution's programs or systems, personal information holdings, or any other circumstance that may impact your institution's security program? How frequently are security measures tested or otherwise monitored to determine effectiveness?

See also Threat/Risk Assessments Checklist (below).

### Third Parties

Is personal information collected, used, retained, disclosed or destroyed by third party service providers on your behalf?

If so, are third party service providers required, by contract or other measures, to have privacy protection measures that are compliant with FIPPA and your institution's privacy management program? How do you verify the effectiveness of the third parties' privacy protection measures?

## **Prevent Privacy Breaches Checklist**

### **Privacy Audits**

Are adequate resources available for developing, implementing and maintaining a privacy management program?

How and why is personal information collected, used, and disclosed?

Is some personal information more sensitive than others? How is the sensitivity identified and are special privacy or security measures in place for this data?

Are the roles and responsibilities related to privacy protection identified and documented?

What steps are in place to minimize the amount of personal information collected, used and disclosed?

How and where does your institution store personal information?

How long do you retain personal information?

Who has access to the personal information and who actually needs to have that access?

Do information handling policies, practices and procedures comply with FIPPA? How are they maintained to keep pace with changes in technology and program needs? How is their effectiveness monitored, enforced and reported?

### **Privacy Impact Assessments (PIA)**

Is a Privacy Impact Assessment conducted when designing and implementing programs or systems that will require the collection, use or disclosure of personal information or when applying technology to personal information systems?

Is the flow of personal information for a proposed new program or system, or change to an existing program or system, understood and documented?

Is your institution following the requirements and process defined in the PIA guides and tools?

How is compliance with FIPPA assessed for a proposed initiative? How will it be verified and reviewed on a go-forward basis?

Have the IPC and stakeholders impacted by the proposed initiative been consulted? What are their concerns and have they been addressed? If not, why not?

## **Prevent Privacy Breaches Checklist**

### **Threat/Risk Assessments (TRA)**

Has a Security Plan been prepared for each of your programs that deal with information and information technology?

How are threats to and sensitivities and vulnerabilities of information identified, and the levels of potential harm and risk assessed?

What are the most likely or serious threats that could lead to a privacy breach (e.g., hacker attack, procedural error, eavesdropping at service counter, lost laptop, etc.)? What measures are in place to counter these threats? Are they effective?

Where are the areas/programs/systems in your institution where there is the greatest likelihood of a privacy breach (e.g., where there is a high volume of transactions involving personal information)?

Is your institution following the OPS TRA requirements and process?

## **Prepare for Privacy Breaches Checklist**

### **Privacy Breach Response Plan**

Do you have an existing privacy breach response plan? If not, how will a plan be developed and implemented?

If yes, when was it last reviewed and updated? Was it approved by all parties/areas that logically would be involved in dealing with most types of privacy breaches, as well as by senior management?

How has the privacy breach protocol outlined in this Guide been adopted and applied to your institution?

Does your privacy breach response plan define the circumstances when a breach will be reported to your Deputy Minister's Office?

Do staff, at all levels, know about your privacy breach response plan, what a privacy breach is, what to do if there is one (e.g., reporting requirements), and how to document details of a breach? If not, what training is required?

Are there templates and forms to facilitate prompt reporting of privacy breaches to appropriate parties?

How will the effectiveness of your response plan be evaluated, by whom and how frequently?

## **Prepare for Privacy Breaches Checklist**

How is your response plan revised to accommodate lessons learned from security incidents or privacy breaches, as well as new risks, technology and other developments? Who is responsible for this?

How are changes to your response plan communicated to players involved in responding to privacy breaches and to your staff?

### **Privacy Breach Response Coordinator**

Who is responsible and accountable for: 1) developing your response plan, and 2) coordinating your institution's response to a privacy breach?

How is the identity of this individual communicated to staff, at all levels?

Have delegates or back-ups been identified in case the Response Coordinator unavailable at time of a breach?

Is 24/7 contact information of the Response Coordinator and delegates known to staff?

### **Privacy Breach Response Team**

Who should be involved in: 1) preparing, reviewing and approving your response plan, and 2) responding to a privacy breach (i.e., who are the key players and what are their roles and responsibilities)?

Are response team members aware of their roles and responsibilities?

How is the effectiveness of your response to a privacy breach determined?

Have key players been designated to be available on 24/7 basis? Is their contact information known to staff?

### **Third Parties**

Do your contracts and service agreements require third party service providers to:

- be prepared to respond to privacy breaches in a manner consistent with your privacy breach response protocol; and
- immediately report breaches to a designated contact at your institution.



## Step 1 – Respond and Contain Checklist

### Report

Have staff reported the privacy breach or suspected breach to their Manager? When and by whom?

Has the Manager reported the privacy breach or suspected breach to Coordinator? When?

Has the Program Manager/Coordinator reported privacy breach to:

- Delegated Decision-Maker – when and by whom?
- Deputy Minister's Office – when and by whom?
- IPA – when and by whom?
- Legal Services – when and by whom?
- Police or other appropriate authorities – when and by whom?
- Other Parties – who, when and by whom?

### Assess

Did a privacy breach occur (i.e., unauthorized disclosure of personal information)?

If no, is there another type of incident report to be completed or action to be taken?

If yes, what happened – describe incident/facts – what (cause of breach such as inadvertent verbal disclosure or theft of a laptop computer), when (date and time of incident), how, where (location), who identified breach (data subject, self-identified or by IPC)?

Whose personal information was affected by the breach (e.g., to whom does the data likely belong)?

What type of personal information was involved (e.g., unique identifiers such as Social Insurance Numbers or Driver's Licence numbers, personal health information, sensitive data)?

Who had custody and control of the personal information involved (e.g., program area, health information custodian, third party service provider)?

If third party service providers involved, are there specific contractual obligations that must be followed?

What medium was the personal information (e.g., oral, electronic or hardcopy)?

What is the likely scope of the privacy breach (i.e., how many individuals/areas/institutions affected)? Are other jurisdictions involved?

## Step 1 – Respond and Contain Checklist

Is the breach the result of illegal activity? Should law enforcement be involved?

Was the privacy breach a one-time occurrence or is there a risk of ongoing or further exposure of the personal information (i.e., would the breach allow unauthorized access to any other personal information)? If the latter, what needs to be done immediately to end the breach and protect the data? Is there a likelihood that a similar, but as-yet-undiscovered, problem exists elsewhere in your institution?

Is there evidence the personal information involved in the breach has been acquired by an unauthorized person and is being, or likely will be, used for unauthorized purposes?

What steps have you already taken to control the breach and mitigate its consequences (e.g., suspend process/activity that caused breach, shut down website or computer system temporarily, change passwords or locks, retrieve copies of records, etc.)?

Are there specific legislative requirements that must be followed (e.g., PHIPA for privacy breaches involving personal health information and health information custodians)?

Have there been any similar or related incidents in the past?

Was the personal information involved in the privacy breach encrypted or protected by other safeguards that would prevent unauthorized access to the personal information?

What potential consequence/harm to the data subject may result from the breach?

- **Identify theft:** most likely to occur when the breach involves Social Insurance Numbers, credit card numbers, driver's licence numbers, personal health numbers, debit card numbers with PIN or any other information that can be used to commit financial fraud.
- **Safety:** when loss of personal information potentially jeopardizes the physical safety of an individual or there is a risk of stalking or harassment.
- **Reputation:** generally associated with loss of sensitive personal information (e.g., mental health records or data that may jeopardize business or employment/business opportunities).
- **Other:** such as when breach may result in a financial loss for the data subject.

What potential consequence/harm to your institution or the public may result from the privacy breach?

## Step 1 – Respond and Contain Checklist

- **Security:** is there the potential to jeopardize the physical safety of your employees, provide access to other assets, or result in future breaches due to similar technical failures?
- **Public health or safety:** does the breach put public health or safety at risk?
- **Public trust:** will the breach result in loss of public trust or confidence? Does the situation require issuing a public statement/notice to reduce fear, or to maintain trust, or to give those directly affected the means to protect themselves or mitigate their own risk or consequences of the breach?
- **Legal:** does the breach constitute a contravention of legislative (e.g., FIPPA or PHIPA) or contractual requirements (e.g., with third party service providers), or might it result in civil litigation?
- **Other:** will breach result in IPC investigation, financial consequences for your institution, questions in Legislative Assembly, media attention?

### Contain

What steps do you need to take immediately to contain/control the breach (e.g., suspend or isolate process/activity affected by breach, shut down website or computer system temporarily, change passwords or locks, etc.)?

Have you taken all necessary steps to retrieve personal information from all sources to which it was inappropriately disclosed (e.g., identify who had unauthorized access to personal information, retrieve hard copies, obtain assurances the parties have not make copies or will use or disclose the data, and document contact information of anyone who may have accessed the personal information involved in the privacy breach in case follow-up is required)?

Have appropriate staff been informed of the breach and provided with instructions on how to control the breach and prevent further unauthorized disclosures of personal information?

Do your policies, procedures, practices need to be changed immediately to contain breach or prevent further breaches?

How are the programs or systems affected by the breach to be monitored for signs of continued problems?

### Document

Are the details of the privacy breach and action taken to contain it and mitigate its consequences being documented? How, by whom and where located?

### Step 1 – Respond and Contain Checklist

#### Brief

Has the Program Manager/Coordinator/Delegated Decision-Maker undertaken all appropriate briefings? When and to whom?

Are any of the circumstances outlined on pages 19 and 20 present? Have you consulted with Legal Services and Issues Management/ Communications to evaluate the severity and scope of the privacy breach?

Does your Deputy Minister's Office need to be briefed?

If a privacy breach has been reported to your Deputy Minister's Office or Minister's Office, have you informed the IPA of this development?

### Step 2 – Notify Checklist

Is notice to be given to individuals affected by the breach? Yes/No

If no, why not? Who approved decision? Has the IPA been consulted on decision not to notify?

If yes, have the best practices related to written or verbal notice been followed? Who should give the notice, how, when? How is consistent notice to be ensured?

If direct notice to the data subject is not possible (e.g., contact information unavailable or identity of data subject unknown), is an alternative approach to notice appropriate?

Should notice been given to the IPC? If so, when and by whom?

Do other parties (e.g., other institutions or jurisdictions) need to be notified of the privacy breach?

Are details of notice process being documented? How and by whom?

**Note:** Institutions under FIPPA that also are health information custodians under PHIPA should follow the notice requirements under subsections 12(2) and 12(3) of PHIPA.

### **Step 3 – Investigate Checklist**

Are you investigating the privacy breach?

If yes, how, by whom, and how findings being documented?  
If no, why not? Is a third party conducting the investigation?

What caused the privacy breach (e.g., accident, deliberate action, internal or external action, insufficient knowledge or training of staff, inadequate security or privacy policies, procedures and practices)?

Does the privacy breach raise systemic issues that need to be addressed across your institution (e.g., lack of staff training, insufficient access controls, firewall deficiencies, etc.) or across government?

Had your institution taken reasonable steps to prevent the privacy breach?

Does your institution's privacy management plan need to be modified as a result of the privacy breach in order to help prevent future breaches and to prepare you to respond to breaches in a more timely and effective manner?

If so, what changes are recommended, how will these be undertaken, by whom and when?

### **Step 4 – Implement Change Checklist**

Were appropriate decision-makers and senior management briefed of results of investigation(s)? When and by whom?

Has implementing your investigation's recommendations been approved? When and by whom? If not, why not?

Is any additional follow-up/report back to the IPC necessary?

How are the recommended remedial measures to be implemented, by whom and when?

How is their effectiveness to be monitored and evaluated? By whom?

**APPENDIX "B-2"**

**OPS CORPORATE POLICY ON PROTECTION OF PERSONAL INFORMATION  
DATED JULY 25, 2011**

**SEE ATTACHED**



## Minister of Government Services

### Corporate Policy on Protection of Personal Information

July 25, 2011

**FINAL APPROVED**

## **TABLE OF CONTENTS**

---

Purpose .....	1
Authority .....	1
Application and Scope.....	1
Principles .....	2
Definitions.....	2
Mandatory Requirements .....	3
Management of Personal Information .....	3
Privacy Officers .....	4
Privacy Breaches .....	4
Privacy Impact Assessment .....	5
Matching of Personal Information.....	5
Contracting for Services .....	6
Information Sharing .....	7
Consultation with Information, Privacy and Archives Division .....	8
Internet Communications .....	9
Accountabilities .....	10
Responsibilities .....	10
Appendices.....	10
Contact Information .....	11



## **PURPOSE**

---

1. The purpose of this policy is to define and establish requirements consistent with the Freedom of Information and Protection of Privacy Act, 1990, for the protection of personal information in the custody or under the control of government.
2. For greater clarity, this policy does not establish and define requirements under the Personal Health Information Protection Act, 2004.

## **AUTHORITY**

---

3. This policy is made by the Minister of Government Services under authority of the Management and Use of Information and Information Technology Directive that gives the Minister responsibility to establish, amend, replace or rescind policies on the management of I&IT that are consistent with the Directive, setting out more detailed operational requirements for ministries, I&IT clusters and agencies.

## **APPLICATION AND SCOPE**

---

4. This policy applies to all ministries, to all advisory and adjudicative agencies, and to any other agency defined under the Agency Establishment and Accountability Directive that is subject, by Memorandum of Understanding or a schedule thereto, to sections 8.1 to 8.4 of the Management and Use of Information & Information Technology Directive.
5. Use of the word “ministry” in this policy includes I&IT clusters and applicable agencies.
6. Requirements under the Personal Health Information Protection Act, 2004, are not within the scope of this policy.
7. This policy does not apply to personal information excluded from the Freedom of Information and Protection of Privacy Act, 1990.

## PRINCIPLES

---

8. The protection of personal information in accordance with statute, regulation, policy and best practices:
  - a) respects the privacy of individuals whose information is collected, used and disclosed by government;
  - b) reduces privacy, organizational and legal risk and maintains the public's trust and confidence in government operations; and
  - c) is an integral part of business practices and the design of programs, services, systems and processes.

## DEFINITIONS

---

9. In this policy:

“business owner” means any program director or equivalent having authority and accountability under legislation, regulation, or policy or other instrument for particular business activities and for the business records relating to those activities;

“coordinator” means the freedom of information and privacy coordinator or equivalent or that person normally performing the role of the freedom of information and privacy coordinator;

“information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, retention, dissemination, disclosure or disposition of information;

“institution” means an institution as defined by the Freedom of Information and Protection of Privacy Act, 1990;

“government” means the Government of Ontario unless the context otherwise requires;

“Head” means the head of an institution as defined by the Freedom of Information and Protection of Privacy Act, 1990, or that officer delegated to carry out the powers and duties of the Head;

“personal information” means personal information as defined by the Freedom of Information and Protection of Privacy Act, 1990;

“Privacy Impact Assessment” means the process that reviews a new or existing information system or program to determine whether measures are necessary to ensure compliance with personal information protection requirements in statute and regulation and to address the broader privacy implications of the system or program;

“privacy officer” means that person designated by the business owner who is responsible for ensuring compliance by the program with this policy; and

“program” means those activities and related records over which a business owner has authority and which collects, uses or discloses personal information.

## **MANDATORY REQUIREMENTS**

---

### **Management of Personal Information**

10. Personal information shall be collected, used, disclosed and otherwise managed only in accordance with the Freedom of Information and Protection of Privacy Act, 1990, and associated regulations.
11. The business owner is accountable to the Head for ensuring that personal information is collected, used, disclosed and otherwise managed in accordance with the Freedom of Information and Protection of Privacy Act, 1990, and associated regulations, and for compliance with this policy.
12. For greater clarity, personal information that is a business record or part of a business record shall be managed in accordance with the Corporate Policy on Recordkeeping, in addition to the requirements of this policy.
13. Where a collection of personal information is authorized by the Freedom of Information and Protection of Privacy Act, 1990, it shall be limited to that personal information that is reasonably necessary to achieve the purposes of the program for which it is collected.
14. Access to personal information shall be restricted to those individuals or agents who require access to personal information in order to perform their duties and where access is necessary and proper for the administration of the program.
15. Staff and management who require access to personal information in order to perform their duties shall receive training to a level commensurate with the complexity and sensitivity of the information to which they have access.

16. A review of compliance with section 10 and sections 12-15 shall be conducted by a business owner periodically as appropriate or if required by the Chief Privacy Officer and Archivist of Ontario, using guidelines issued by Information, Privacy and Archives Division.

## **Privacy Officers**

17. The business owner may, in writing, designate an individual to perform the role of privacy officer in relation to the personal information over which the business owner has authority.
18. The privacy officer shall:
  - perform all of the things required to be performed by the business owner under this policy;
  - be responsible for ensuring that personal information is managed in accordance with the Freedom of Information and Protection of Privacy Act, 1990, and associated regulations; and
  - be responsible for compliance with this policy.

## **Privacy Breaches**

19. A privacy breach occurs where there is an internal or external disclosure of personal information that is not authorized by the Freedom of Information and Protection of Privacy Act, 1990, and may be deliberate or inadvertent.
20. When a privacy breach occurs, the business owner shall report the breach forthwith to the coordinator, and the coordinator shall forthwith report the breach to Information, Privacy and Archives Division.
21. The business owner, in consultation with the coordinator, shall ensure at a minimum that:
  - the breach is contained and assessed;
  - the breach is reported to any other relevant parties;
  - where appropriate, the individual or individuals whose personal information has been breached, as well as the Information and Privacy Commissioner, are notified;

- the cause or causes of the breach are investigated in a manner commensurate with the nature and severity of the breach; and
- corrective or remedial action is taken pursuant to the investigation to prevent further breaches and address related matters.

## **Privacy Impact Assessment**

22. A privacy impact assessment shall be conducted whenever there is a substantial change in the collection, use or disclosure of personal information, including the creation or substantial modification of an information system or database containing personal information.

## **Matching of Personal Information**

23. Matching of personal information is a computerized or automated process comparing two or more databases of personal information that were originally created for different purposes, that creates or merges information on identifiable individuals in order to identify matters of interest or to make decisions about the individuals to whom the matched information relates.
24. Personal information may be matched only where:
- it is the purpose or one of the purposes for which the personal information in each database was collected;
  - it is consistent with the purpose or purposes for which the personal information in each database was collected;
  - the individuals to whom the information to be matched relates have consented to the matching of the information; or
  - it is required by law or for the purposes of law enforcement.
25. Where the results of a matching of personal information may lead to a denial, termination, suspension or reduction of a benefit, entitlement or other assistance, the ministry shall:
- verify or ensure the accuracy of the results of the matching exercise in a manner that is independent of the matching system;
  - provide notice to the individual affected by the matching exercise; and

- allow the affected individual to challenge or respond to the results of the matching exercise.
26. The process referred to in section 25 must be documented and approved by the responsible Assistant Deputy Minister or equivalent.
27. Sections 25 and 26 do not apply where a substantially similar process is established in relation to a program by statute or regulation.
28. For greater clarity, the following activities are not considered to be a matching of personal information for the purpose of this policy:
- a matching of information that is not personal information;
  - a matching of personal information to ensure the information is accurate or current or to correct and update personal information or to reconcile financial information;
  - a matching or consolidation of information collected for the same purpose to administer a specific program;
  - a matching of personal information as part of an audit, evaluation or review of a program, where the information is not used to identify matters of interest or to make decisions about the individuals to whom the matched information relates;
  - a matching of anonymized or pseudonymized personal information for research, statistical or evaluation purposes where adequate safeguards are implemented to prevent re-identification of the individuals to whom the information relates; and
  - a matching that involves only personal information that is collected for the purpose of creating a record that is publicly available.

## **Contracting for Services**

29. A contract for service with an external service provider involving personal information shall at a minimum provide:
- for the retention of control by the contracting ministry over personal information transferred to the service provider;
  - for compliance by the service provider with applicable sections of Part III of the Freedom of Information and Protection of Privacy Act, 1990, and associated regulations;

- for the training of service provider staff and management who have access to personal information commensurate with the sensitivity of that information, and (where considered necessary) for the designation of a privacy officer by the service provider;
- for the safeguarding by the service provider of personal information in accordance with the corporate policy;
- for the return to the contracting ministry or the secure destruction of personal information in accordance with applicable procedures by the service provider during or on termination of the contract;
- for compliance by the service provider with any other section of this policy or with any other applicable policy or guideline; and
- for discretionary or periodic auditing of the service provider (or other compliance monitoring arrangement) for compliance with this section.

## **Information Sharing**

30. Information sharing is the disclosure of personal information (including sale) for a specific purpose, by the institution that collected the information, to another institution, to another government, to a person or group of persons or to an external organization.
31. Information sharing must be authorized under the Freedom of Information and Protection of Privacy Act, 1990, or other statute.
32. An information sharing agreement must be approved by the disclosing and receiving organizations prior to the disclosure taking place.
33. Approval of an information sharing agreement means approval in writing of at least the business owner of the personal information in the disclosing organization and of the business owner (or equivalent) receiving the information in the receiving organization.
34. An information sharing agreement shall at a minimum specify:
  - the purpose and scope of the information sharing exercise;
  - the legal authority for the information sharing exercise, including the authority to disclose and indirectly collect personal information, respectively;
  - the personal information to be shared;

- the use or uses of the personal information by the organization receiving the information;
  - unless there is an exemption for notice of collection or a waiver of notice has been obtained, how notice requirements will be addressed by both the originating and receiving organizations;
  - the method for sharing information, including the medium or means of exchange of information between organizations;
  - how the receiving organization will ensure accuracy and security of the personal information once received; and
  - the duration of the information sharing agreement and the disposition of exchanged personal information during and on termination of the agreement.
35. For greater clarity, sections 31-33 do not apply to the sharing of anonymized or pseudonymized personal information where adequate safeguards are implemented to prevent re-identification of the individuals to whom the information relates.

### **Consultation with Information, Privacy and Archives Division**

36. A business owner (or privacy officer where one has been appointed) shall consult with Information, Privacy and Archives Division:
- on any proposed amendment to a statute or regulation that affects the Freedom of Information and Protection of Privacy Act, 1990, or the Municipal Freedom of Information and Protection of Privacy Act, 1990, within a reasonable period of time prior to their consideration by Cabinet;
  - except where section 27 applies, on a proposed matching of personal information, within a reasonable period of time prior to the execution of the matching; and
  - on any matter with significant implications for individual privacy or the protection of personal information.



## Internet Communications

37. A link to a corporate privacy statement shall be available from every public-facing government Internet page and shall include at a minimum:
- a general description of the information collected when an individual visits a government Internet page and how this information is used;
  - a statement that government Internet pages may embed third-party pages, content or components, and that such third-party pages, content or components, if selected by the user, may not be subject to the same statutory privacy protections as government pages;
  - suggestions (or a link to information) on how an individual can further protect on-line activities through practices and settings; and
  - whom the individual might contact for further information.
38. Information stored in or forming part of server access logs or Internet traffic monitoring data, including Internet protocol addresses, shall not be used to track, identify or locate individuals unless required by law or for the purposes of law enforcement.
39. Section 38 does not apply to the administration of a service or transactional relationship through an identification and authentication scheme, or to development, with user consent, of a related service history or profile.
40. Interactive on-line communication with government (such as forums, bulletin boards or consultations) shall be monitored and require participants to consent to a terms of use that at a minimum:
- caution against improper use of the interactive communication and of loss of privileges in event of improper use;
  - caution against the posting of personal information by participants about themselves beyond views and opinions on the subject of the interactive communication;
  - instruct users not to post personal information about another identifiable individual or individuals; and
  - require users to accept the terms of use before the user is able to participate in the interactive communication.

41. Where a government Internet page uses an embedded third-party site, content or component, a clear indication shall be given on the page that such third-party site, content or component belongs to a third party and is not part of the government page.
42. Sections 37-41 apply with necessary modification to any Internet communication by or on behalf of government, including but not limited to Internet sites, services, applications and public messaging.

## **ACCOUNTABILITIES**

---

43. Business owners are accountable to ministry Heads for ensuring that personal information is collected, used, disclosed and otherwise managed in accordance with the Freedom of Information and Protection of Privacy Act, 1990, and associated regulations, and that programs comply with this policy.

## **RESPONSIBILITIES**

---

44. Privacy officers, where they have been appointed, are responsible for ensuring that personal information is collected, used, disclosed and otherwise managed in accordance with the Freedom of Information and Protection of Privacy Act, 1990, and associated regulations, and that programs comply with this policy.
45. The Chief Privacy Officer and Archivist of Ontario is responsible for the periodic review of this policy, for providing training on the policy, for developing a corporate privacy statement for government Internet pages, and for issuing guidelines or best practices to promote proper implementation of the policy.

## **APPENDICES**

---

46. Guidelines and best practices associated with this policy and issued by the Chief Privacy Officer and Archivist of Ontario, and relevant standards issued by a standard-setting authority, shall be listed in an appendix to this policy, and said appendix may be revised as needed by the Chief Privacy Officer and Archivist of Ontario without approval of the Minister of Government Services.

## **CONTACT INFORMATION**

---

Policy and Planning Branch  
Information, Privacy and Archives  
Ministry of Government Services

## **APPENDIX – LIST OF ASSOCIATED GUIDELINES**

---

Guidelines associated with this policy are under development.

The following guidance documents were developed and made available prior to the development of this policy, are under review and will be superseded by the new guidelines. However, they remain relevant and helpful.

[Guide and Checklist for Managing Personal Information, 2008](#)

[Guidelines for Protection of Information When Contracting for Services, 2008](#)

[Publication of Conviction Information About Individuals, 2008](#)

[Taking the Right Steps – A Guide to managing Privacy and Privacy Breaches, 2007](#)

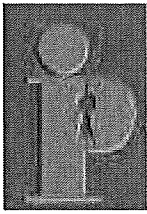
These guidance documents, and other useful publications, can be obtained from the Resource Center page of Policy and Planning Branch, Information, Privacy and Archives Division, Ministry of Government Services.

<https://intra.sse.gov.on.ca/inetwork/resourcecentre/Pages/subject.aspx>

**APPENDIX "B-3"**

**"IPC PRACTICES NO. 26: SAFE AND SECURE  
DISPOSAL PROCEDURES FOR MUNICIPAL INSTITUTIONS"**

**SEE ATTACHED**



NUMBER 26  
REVISED SEPTEMBER 1998



# IPC Practices

PUTTING ONTARIO'S INFORMATION AND PRIVACY LEGISLATION TO WORK  
INFORMATION AND PRIVACY COMMISSIONER/ONTARIO  
ANN CAVOUKIAN, Ph.D., COMMISSIONER

## Safe and Secure Disposal Procedures for Municipal Institutions

*All organizations should dispose of personal information in a safe and secure way when it is no longer needed. While provincial government organizations have been provided with guidance on this through Regulations and Directives, municipal organizations have not. This issue of IPC Practices offers guidance and practical suggestions on how municipal organizations can dispose of personal information in a safe and secure manner.*

### Background

To prevent unauthorized parties from accessing personal data, it is important to use care in the disposal and destruction of personal information.

Section 40(4) combined with Regulation 459 of the provincial *Freedom of Information and Protection of Privacy Act* (the provincial *Act*) deals with the disposal of personal information. Section 4(1) of Regulation 459 states:

Every head shall ensure that all reasonable steps are taken to protect the security and confidentiality of personal information that is to be destroyed, including protecting its security and confidentiality during its storage, transportation, handling and destruction.

Section 4(3) goes on to state:

In determining whether all reasonable steps are taken under subsection (1) or (2), the head shall consider the nature of the personal information to be destroyed or transferred.

Section 6 deals with the need for provincial organizations to keep a record of what personal information has been destroyed and states:

- 1) Every head of an institution shall ensure that the institution maintains a disposal record setting out what personal information has been destroyed or transferred to the Archives and the date of that destruction or transfer.
- 2) The head shall ensure that the disposal record maintained under subsection (1) does not contain personal information.

Section 30(4) of the *Municipal Freedom of Information and Protection of Privacy Act* (the municipal *Act*) deals with the disposal of personal information and states:

A head shall dispose of personal information under the control of the institution in accordance with the regulations.

Unlike the provincial *Act*, there are no equivalent regulations pursuant to section 30(4) of the municipal *Act*.

Thus, we have developed the following procedures to assist municipal organizations with the disposal of records.



## Recommended Procedures

### *Preparing disposal record*

A disposal record is a list indicating what records have been destroyed, when, by whom, and using what method of destruction. Records that have been kept or archived may also be tracked. It could be a simple list on paper, or part of an electronic records management system.

The disposal record applies to both paper and electronic (computer and video) records, and must not contain personal information. Referring to the record "type" rather than the contents of the record will help you avoid this. For example, "1992 Home Visits" would be an acceptable entry on the disposal record, however, "Home Visits: John Doe" would not. See sample on next page.

### *Obtaining authorization from the Head*

For record keeping purposes, you can obtain authorization from the Head before destroying records.

### *Disposing of records safely and securely*

Some records containing sensitive personal information should be destroyed on-site, while others may be taken off-site for destruction. Whatever method is used, it is important that proper steps be taken to ensure that personal information on all storage media (paper, electronic and video) cannot later be used or reconstructed.

Paper records containing personal information should be shredded, not simply thrown out with regular garbage or general records.

For electronic records, care must be taken because utility programs can be used to reconstruct the deleted information. Furthermore, erasing or reformatting computer disks or personal computers with hard drives that once contained personal information is not enough. Using a utility such as Norton Utilities, PC Tools, or a recent version of the operating system will remove all data from the medium so that it cannot be reconstructed.

Similarly, video tapes containing personal information should be physically destroyed — not thrown out with the regular garbage. Overwriting a video tape that contains personal information with non-personal information will remove the previous images, but this should

be done on the premises by authorized staff. For more information, please refer to *IPC Practices, Number 10 — Video Surveillance: The Privacy Implications*.

Finally, when records are destroyed by an outside agency, the privacy provisions of the *Acts* should be observed. It is a good idea to have a formally signed contract or agreement outlining these provisions and addressing the need for security, confidentiality, and the disposal method that will be used.

### *Retaining records of historic value*

While some records containing personal information have only temporary value and may be destroyed after the retention period has expired, others should be preserved or archived for future generations.

You may wish to consult other sources, such as *RIM* (Recorded Information Management). These fact sheets published by the Archives of Ontario provide tips on good records-management practices that can help you determine how to deal with maintaining records of historic value. These are available from the office of the Archives of Ontario, 6<sup>th</sup> Floor, 77 Grenville Street, Toronto, Ontario, M5S 1B3, (416) 327-1600.

### *Ensuring employee awareness and training*

Staff should understand the importance of and the best ways to safely and securely dispose of records. Establishing training and awareness sessions about the handling and use of personal information, including privacy and disposal, is a good start.

## Conclusion

It is to the advantage of every government organization to ensure that personal information is protected during the disposal process. Once an individual's privacy is lost, there is no recovering it. Inadvertent disclosures of personal information can lead to public embarrassment for the organization, as well as costly investigations and other consequences that could have been avoided. The Information and Privacy Commissioner/Ontario hopes that you will be able to use the suggestions outlined in this *IPC Practices* as a framework for enhancing or developing your own disposal policies and procedures.



## SAMPLE DISPOSAL RECORD

### WR Organization Disposal Record

Department: Administration — Facilities Unit

Date Completed: December 15, 1996

Completed By: John Doe

Records Schedule Cross-Reference	Particulars (Do not include Personal Information)	Transferred to Archives		Date	Manner of Disposal	
		Y	✓N		✓ Shredded Erased	Incinerated Re-recorded
HR - 123	HR Files - A to Z (1989-1992) Resumes, interviews, references, evaluations, notes.	Y	✓N	Nov 15 '96	✓ Shredded Erased	Incinerated Re-recorded
SEC - 684	Video Tapes of Main Entrance and Loading Dock (Feb 1995-Sept 1996)	Y	✓N	Dec 1 '96	Shredded Erased	Incinerated ✓ Re-recorded
INS - A - 876	Health Inspection Reports - Facilities (1993-1994) Written reports and computer printouts.	Y	✓N	Dec 5 '96	✓ Shredded Erased	Incinerated Re-recorded
TREAS - AP/AR	Correspondence re: Payables, Receivables and letters of notice. Paper Files (1993-1994)	Y	✓N	Dec 5 '96	✓ Shredded Erased	Incinerated Re-recorded
TREAS - AP/AR	Correspondence re: Payables and Receivables and letters of notice. Computer Disks and Backups (1993-1994)	Y	✓N	Dec 15 '96	Shredded ✓ Erased	Incinerated Re-recorded

## IPC Practices

is published regularly by the **Office of the  
Information and Privacy Commissioner.**

If you have any comments regarding this publi-  
cation, wish to advise of a change of address or  
be added to the mailing list, contact:

**Communications Department**  
Information and Privacy Commissioner/Ontario  
80 Bloor Street West, Suite 1700  
Toronto, Ontario M5S 2V1  
Telephone: (416) 326-3333 • 1-800-387-0073  
Facsimile: (416) 325-9195  
TTY (Teletypewriter): (416) 325-7539  
Web site: <http://www.ipc.on.ca>



50% recycled  
paper,  
including 20%  
post-consumer  
fibre

ISSN 1188-7206



**APPENDIX “C”**

**DESIGNATED OFFICIALS**

**“C-1”**

**MHO DESIGNATED OFFICIAL**

Director, Housing Programs Branch  
Ministry of Housing  
777 Bay St, 14th Floor  
Toronto ON M5G 2E5  
Telephone: 416-585-7021  
Fax: 416-585-6588

**“C-2”**

**SERVICE MANAGER DESIGNATED OFFICIAL**

Dave Purdy, Manager, Housing Services  
Housing, Social Services & Dearness  
City of London  
355 Wellington St. Suite 248 2nd Floor  
London ON N6A 3N7  
Telephone: 519-661-2489 ext. 5596  
Fax: 519-661-4466  
[dpurdy@london.ca](mailto:dpurdy@london.ca)

**“C-3”**

**MOF DESIGNATED OFFICIAL**

Director  
Account Management and Collections Branch  
33 King St. W., 6<sup>th</sup> Floor  
Oshawa, ON L1H 8H5

## **APPENDIX “D”**

### **OFFICIALS WHO ARE AUTHORIZED TO ACCESS PERSONAL INFORMATION.**

#### **“D-1” MHO OFFICIALS**

1. Persons working in the Housing Programs Branch, the Housing Funding and Risk Management Branch, the relevant Municipal Services Office and in the Assistant Deputy Minister’s Office.

#### **“D-2”**

#### **SERVICE MANAGER OFFICIALS**

1. Persons working within the Housing Division at the Corporation of the City of London

#### **“D-3” MOF OFFICIALS**

1. Persons working in the Account Management and Collections Branch of the Tax Compliance and Benefits Division.

## APPENDIX “E”

### STATUTORY AUTHORITIES

1. Order in Council 1206/2016 and subsection 4(2) of the *Ministry of Municipal Affairs and Housing Act* authorizes the Minister of Housing to take such measures as he or she considers appropriate to implement any housing policy or program, including entering into any agreements for such purpose with any person.
2. Section 13(1) of the *Housing Services Act, 2011* (“HSA”) provides that a service manager may establish, administer and fund housing and homelessness programs and services.
3. Section 31 of MFIPPA allows the Service Manager to disclose PI to MHO with the consent of the applicant about whom the information relates, or for the purpose for which it was obtained or compiled or for a consistent purpose.
4. Section 42(1) of FIPPA allows MHO to provide PI to MOF and the Service Manager, with the consent of the applicant about whom the information relates, or for the purpose for which it was obtained or compiled or for a consistent purpose.
5. Section 39(1) of FIPPA and section 29(1) of MFIPPA respectively allow MOF to collect the PI indirectly from MHO, and allow the Service Manager to collect the PI indirectly from MHO, in each case, with the consent of the applicant about whom the information relates.
6. MOF on behalf of MHO will obtain from all Applicants signed consents:
  - (i) permitting MOF on behalf of MHO to disclose PI contained in and accompanying the Application Form to MHO, ServiceOntario, the Canada Revenue Agency (CRA) and the Applicant’s Service Manager for the purpose of administering the Program and permitting the collection, use, and sharing of this PI by these parties; and
  - (ii) permitting the Applicant’s Service Manager to disclose PI under its custody and control including information that it compiles (including income information) to MOF, MHO, and/or ServiceOntario for use in connection with administering the Program and permitting the collection, use and sharing of this PI (other than tax information) by these parties.
7. Order in Council (O.C. 1568/2011) of December 7, 2011 assigns the functions, responsibilities and programs that had been previously carried out by the Ministry of Revenue to the Ministry of Finance;
8. Subsection 11(1) of the *Ministry of Revenue Act* (the “MOR Act”) authorizes the minister to enter into agreements and provide services to another Ontario Ministry or any public body for the administration of a government assistance program;

9. MHO and MOF are parties to a Memorandum of Understanding effective April 1, 2018 under which MOF will provide services to MHO to assist MHO in the administration of the Program.
10. Subsection 11(4) of the MOR Act authorizes an employee of the other Ministry or public body to disclose to an employee of MOF such information as MOF may require, and authorizes an employee of MOF to disclose to an employee of the other Ministry or public body any information to which the employee of MOF has access that relates to an individual seeking or receiving assistance under the program;
11. Subsection 11(6) of the MOR Act requires that the information received be collected, used and disclosed:
  - (a) in the case of MOF, only for the purposes related to the provision of the services; and
  - (b) in the case of the other Ministry or public body, only for purposes related to the provision of a government assistance program.
12. The HSA permits a Service Manager to enter into an agreement with an Ontario ministry for the collection, use and disclosure of information and may disclose personal information collected for the purpose of administering the HSA (e.g. special priority category status) to that ministry if the disclosure is made in accordance with the agreement and the ministry agrees to use the information only for the administration of a social benefit program. The Service Manager may also collect personal information from the ministry if the collection is made in accordance with the agreement.