Unclassified



Employment and Social Development Canada

Standard Operating Procedure for the Regional Emergency Operations Centre (REOC)

Revised: 1 August 2019

**Contents**

[1. Purpose and Scope 3](#_Toc17286367)

[2. Authorities 3](#_Toc17286368)

[3. Incident Management Governance at ESDC 4](#_Toc17286369)

[3.1 Departmental Crisis Management Team (DCMT) 5](#_Toc17286370)

[3.2 National Emergency Operations Centre (NEOC) 5](#_Toc17286371)

[3.3 Regional Crisis Management Team (RCMT) 5](#_Toc17286372)

[3.4 Regional Emergency Operations Centre (REOC) 5](#_Toc17286373)

[4. Incident Management Procedures 6](#_Toc17286374)

[4.1 Levels of Incident Activation 6](#_Toc17286375)

[4.2 High-Level Incident Management Flowchart 7](#_Toc17286376)

[4.3 High-Level Incident Management Checklist 8](#_Toc17286377)

[4.4 Incident Activation Triggers 8](#_Toc17286378)

[5. REOC Structure 9](#_Toc17286379)

[6. Response and Recovery Process Flow 11](#_Toc17286380)

[7. Incident Planning 11](#_Toc17286381)

[Annex A - Functional Checklists 15](#_Toc17286382)

[REOC Executive Director 15](#_Toc17286383)

[Safety Lead (HRSB) 16](#_Toc17286384)

[Public Information Lead (PASRB) 16](#_Toc17286385)

[Information Technology Lead (IITB) 17](#_Toc17286386)

[Operations Lead 17](#_Toc17286387)

[Planning Lead 18](#_Toc17286388)

[Logistics Lead 19](#_Toc17286389)

[Finance Lead (CFOB) 19](#_Toc17286390)

[Annex B – Incident Action Plan (IAP) 20](#_Toc17286391)

[Annex C – Situation Report (SitRep) 23](#_Toc17286392)

[Annex D – Incident Management Contact List 27](#_Toc17286393)

[Annex E – Document History 29](#_Toc17286394)

|  |
| --- |
|  **Note****!**If this is an immediate threat, GO DIRECTLY to [Emergency Response Procedure](#_4._Incident_Management_1). |

# 1. Purpose and Scope

This Standard Operating Procedure (SOP) provides Employment and Social Development Canada’s (ESDC’s) Regional Emergency Operations Centres (REOCs) with a clear and effective procedure and toolset.

The REOC SOP is comprised of two components:

* An Incident Management System; and
* A procedure with supporting templates designed to standardize emergency information gathering in support of fact based decision-making.

# 2. Authorities

Under the [Federal Emergency Response Plan (FERP)](http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-rspns-pln/index-eng.aspx), ESDC has responsibility for the following Emergency Service Functions (ESFs):

* Primary department for the Emergency Support Function (ESF) 7 on Human and Social Services;
* Supportive role to Public Safety Canada for ESF 11 on Logistics Operations Management; Supportive role to Public Safety Canada for ESF 12 on Communications, with ESDC telephone, in-person and Web channels of communication.

ESDC also provides services on behalf of other government departments ([SEMP Annex F](http://iservice.prv/eng/is/security/emergency_continuity/tools_and_resources/strat_emergency_mgt_plan.shtml#Annex_F)).

The [Federal Policy for Emergency Management (FPEM](https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/plc-mrgnc-mngmnt/index-en.aspx)) and the ESDC Strategic Emergency Management Plan (SEMP Figure 1, page 8) outline the four emergency management functions within the Government of Canada:

* Prevention and Mitigation
* Preparedness
* Response
* Recovery

Scope of the REOC SOP is limited to pillars 3 and 4, RESPONSE and RECOVERY.

## 3. Incident Management Governance at ESDC



## 3.1 Departmental Crisis Management Team (DCMT)

Within ESDC’s organization, the Departmental Crisis Manager (DCM), the Departmental Crisis Coordinator (DCC) and the Departmental Crisis Management Team (DCMT) are the command authorities responsible for the management of the incident at the national level. The role of the DCM is fulfilled by the Chief Operating Officer (COO), and the DCC is fulfilled by the Assistant Deputy Minister (ADM) of Integrity Services Branch (ISB).

## 3.2 National Emergency Operations Centre (NEOC)

The Departmental Emergency Management and Business Continuity (EMBC) team supports the DCMT through National Emergency Operations Centre (NEOC). The EMBC team provides a coordinating and reporting function for the DCMT during various events and situations.

The NEOC is the Department’s central command and control facility. It has 24/7 capability and is built to respond to all-hazard emergency situations in a timely and efficient matter and to ensure the continuity of our critical operations.

Crisis Management Teams from Branches and Regions are responsible for the coordination process for events/incidents affecting their respective physical environment or functional area of responsibilities.

## 3.3 Regional Crisis Management Team (RCMT)

The RCMT is led by the Regional ADM, and supported by their Regional Executive Director (ISB) and Directors General from their key business lines as well as the Regional Emergency Operations Centre (REOC). The RCMT are the command authority responsible for the management of incidents at a Regional level.

The RCMT acts as the primary decision-making body for the regional response, business continuity or resumption approaches and activities. In addition, they provide situational awareness reports to the DCC, Chief Security Officer, NEOC and others as appropriate as well as support and provide direction to the DCMT.

## 3.4 Regional Emergency Operations Centre (REOC)

The REOCs are ESDC’s regional operations centres for incident, emergency and crisis response and management. Each ESDC region has a functional REOC, most of which operate virtually. The Department’s four (4) REOCs apply various principles of the incident command system to manage local and regional emergency and crisis situations.

The REOC is also responsible for gathering operational picture, assessing the level of response, creating/ update the incident action plan (IAP), brief and obtain IAP approval from the RCMT. Additionally, REOCs are required to provide information for situational awareness to the NEOC.

As the majority of the emergency events in the NCR have an impact on multiple business lines and regions, the NEOC will support the NCR-RSO for NCR incidents, emergency response and management.

# 4. Incident Management Procedures

## 4.1 Levels of Incident Activation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Level of Incident | Incident Definition and Description | REOC Activation\* Status | RCMT Activation Status | NEOC Activation Status | DCMT Activation Status |
| EXTREME | Incident affecting CANADA – Major disasters, serious risks to the health, safety or security of Canadians or Government of Canada operations | Full Activation(If region is affected)Monitoring(if region is not directly affected)  | Full Activation(If region is affected)Monitoring(if region is not directly affected) | Full Activation | Full Activation |
| HIGH | Incident affecting the DEPARTMENT –Major incident with serious risks to ESDC or its employees | Full Activation(If region is affected)Monitoring(if region is not directly affected)  | Full Activation(If region is affected)Monitoring(if region is not directly affected) | Full Activation | Full or Partial Activation as required |
| MODERATE | Incident affecting NHQ or a REGION – Significant impact on service delivery or employees | Full or Partial Activation as required | Monitoring(If incident is confined to a single region) | Monitoring(If incident is confined to a single region)Full or Partial Activation as required(If incident requires national support or has national service delivery implications) | Monitoring |
| LOW | Incident affecting Local Offices – Minor Disruption to service delivery or building level incidents | Monitoring(If Regional support is not required)Full or Partial Activation as required | Stand-by | Stand-by | Stand-by |

\*Activation is the implementation of business continuity procedures, activities and plans in response to a serious incident, emergency, event or crisis.

## 4.2 High-Level Incident Management Flowchart



## 4.3 High-Level Incident Management Checklist

|  |  |  |
| --- | --- | --- |
| Activation | Response | Recovery |
| * Assess scope and severity of incident
 | * Conduct preliminary damage and impact assessments
 | * Implement recovery strategies to achieve full normal service levels
 |
| * Provide for safety of employees, protection of property and government operations
 | * Develop an Incident Action Plan
 | * De-escalate the DCMT, NEOC, REOC and support staff
 |
| * Advise Departmental Crisis Coordinator and/or the Departmental Crisis Manager
 | * Implement Incident Action Plan and other contingency plans, business recovery strategies or mitigations as appropriate to the incident
 | * Address post incident needs of affected employees (EAP/HR) and conduct reconciliation activities as required
 |
| * Initiate activation of REOC, RCMT, NEOC and DCMT as appropriate to the level of the incident
 | * Monitor the incident as it evolves and revise the Incident Action Plan as required
 | * Conduct Post Incident Review and provide closing briefings
 |
| * Provide initial reporting
 | * Establish minimum services levels
 | * Update plans and procedures as required
 |

## 4.4 Incident Activation Triggers

The decision to activate the REOC, RCMT, NEOC and DCMT should be based on the level of the incident and potential activation triggers for incidents that:

* Threaten the health, safety or security of Canadians
* Pose significant property damage potential
* Require specialized or coordinated emergency services
* Require urgent emergency public communications
* Threaten the delivery of services to Canadians
* Affect ESDC’s ability to deliver on its Emergency Support Function mandate
* Involve criminal activity or have the potential to result in legal actions
* Create a situation beyond ESDC’s ability to shelter or evacuate employees
* Pose the potential for long term negative affect on ESDC or its reputation
* Generate significant media attention

Incident Activation Triggers include:

* Natural disasters with implications for service delivery or health and safety of employees (earthquakes, floods, fires, hurricanes)
* Strikes, protests, civil unrest (postal strikes, Public Service Union job actions) that impact multiple ESDC locations in the Region simultaneously
* Mass acts of violence or terrorism affecting ESDC Space (shootings, attacks or substantiated threats)
* Uncontained cyber-attacks, largescale network issues, blackouts

# 5. REOC Structure

The structure of the REOC is based on the world-wide standardized Incident Management System – (also known as Incident Command System). The Incident Management System is designed to establish a flexible and scalable team structure for fast and efficient emergency and business continuity management.

Each emergency situation is unique and requires its own response expertise. Using the Incident Management System, functional teams within the REOC are easily activated or decommissioned as the incident dictates.

|  |  |
| --- | --- |
| Function | Primary Responsibility |
| REOC Executive Director | The REOC Regional Executive Director is the person in charge of managing the response to emergency situations for their respective regions. Regional ADM leads the Crisis Management Team for their respective Region and provides situational awareness reports to the CMT, NEOC, CSO and others as required. |
| Safety  | The Safety Lead assesses hazardous and unsafe situations and develops measures for safeguarding employees during an emergency. This lead may exercise authority to stop unsafe activities that is imminent danger. |
| Public Information  | The Public Information Lead coordinates all internal and external communications on the emergency situation. The Communications Lead works in close collaboration with the Regional Executive Directors and with the Regional ADM for the three main channels of service and communication – telephone, in-person and Web. This contact must work in collaboration with NHQ Public Affairs and Stakeholder Relations Branch. |
| Information Technology | The Information Technology Lead is in charge of any system issues that relates to the emergency situation. In the case of a cyber-incident or an emergency situation where the emergency concerns primarily the systems, the Information Technology Lead role will merge with the Operations Lead role and the Information Technology Lead would become the Operations Lead. |
| Operations | Responders from affected business units. Focus is:* Life safety
* Protection of property
* Damage containment
* Crisis processing
* Post incident reconciliation
* Return to normal operations
 |
| Planning | Advance planning of operational needs and activities for the next operational response period. Focus is:* Resources
* Situation forecasting
* Demobilization
* Documentation
 |
| Logistics | Obtaining, positioning and arranging needs of all teams.Focus is:Service* Telecomm
* Medical
* Food
* Support

Supplies* Facilities
* Other Misc. Support
 |
| Finance/Admin | All aspects of financial and admin needs of all teams. Focus is:* Procurement
* Time tracking
* Cost reporting
* Travel needs
* Compensation
* Claims
 |

# 6. Response and Recovery Process Flow

The internal integrity and security directorate supports the RCMT through REOC co-ordination and reporting services.

Consult

Partners and

Stakeholders

Do Staff Need to be Notified?

Assess Damage and Impact

Brief Senior

Management

(as required)

Contingency Plans,

Disaster Recovery Plans

Continue to Full Recovery

Carefully Decommission Teams and Workarounds

Notify Staff (as required)

Post Incident Review

Emergency Workaround Reconciliation Activities

After Action Report and Plan Updates

Implement BCP?

Apply/update

Recovery

Strategies

Recovery and

Resumption

to MSL?

Recovery and Resumption

To Full Service

END

**No**

**No**

**YES**

**YES**

**No**

# 7. Incident Planning

**YES**

**YES**

END

Using the Planning Cycle ensures that any incident is managed as efficiently and effectively as possible. It results in the proper use of resources, appropriate strategies and tactics, control of incident costs, and better overall effectiveness. **Planning Cycle Diagram** illustrates how each phase of the planning cycle flows. **Planning Cycle Phases** describes each phase and who leads it. **Planning Meeting** contains details and the agenda for the planning meeting.

**Planning Cycle Diagram**

***Incident Action Plan:*** The IAP is a written plan that defines the incident objectives and reflects the tactics necessary to manage an incident during an operational period

**Planning Cycle Phases**

|  |  |  |
| --- | --- | --- |
| *Phase* | Lead by | Description |
| *Assess Situation* | REOC Regional Executive Director/Manager | Gather information on the current status of the incident. Response and recovery teams provide information. These teams are formed by a representative from each functional group (operations, planning, logistics, finance/admin). |
| *Hold Planning Meeting* | REOC Regional Executive Director/Manager | Determine/review the incident objectives. Incident objectives should be clear, measurable, achievable, and flexible. The REOC Regional Executive Director then calls the **Planning Meeting**. |
| *Complete Incident Action Plan (IAP)* | Planning, REOC Regional Executive Director | Document the IAP according to the outcome of the **Planning Meeting**. Indicate when all elements of the plan and support documents are required to be submitted, so the plan can be collated, duplicated, and made ready for the approval process. REOC Regional Executive Director will review and approve the IAP. **Appendix: Incident Action Plan** |
| *Inform RCMT/NEOC* | Planning, REOC Regional Executive Director | Using the approved IAP, Planning will create a Situation Report for use in briefing the RCMT and the NEOC. The REOC Director and RCMT should review/approve the Situation Report per region. It is important to synchronize the RCMT briefings with the planning cycle to achieve the following:* Brief RCMT and NEOC on the latest situation
* Seek approval of the IAP
* Identify issues warranting direction/decisions from the RCMT
* Make a connection between the strategic guidance provided by the RCMT and the meetings of REOC

**Appendix: Situation Report** |
| *Implement Plan and Evaluate Outcome* | Operations | The IAP is evaluated at various stages in its development and implementation. Operations may make the appropriate adjustments during the operational period to ensure that the objectives are met and effectiveness is assured.  |

**Planning Meeting**

|  |  |
| --- | --- |
| **Purpose** | Formulate *incident objectives* Gather input and develop incident strategiesProvide immediate direction that cannot wait until the planning process is completedDetermine tactics  |
| **Participants** | REOC |
| **Documents required**  | * A documented list of incident objectives
* IAP
 |
| **Agenda** | **Agenda Topic** | **Lead by** |
| Roll call | Scribe |
| Opening remarks | REOC Regional Executive Director / Manager |
| Discuss incident objectives for the upcoming operational period | REOC Regional Executive Director/ Manager |
| Describe/update current situation | REOC Regional Executive Director/Operations/ Manager |
| Round table discussion, including the following:* Current status and issues
* Constraints, limitations, and shortfalls
* Input needed to finalize the incident objectives and establish *tactics*
 | All  |
| Develop tactics and assign resources  | Operations, Logistics, Planning  |
| Identify methods for tracking ongoing issues | Planning |
| Open discussion | All |
| Closing remarks | REOC Regional Executive Director/ Manager |
| **Documents produced**  | * Updated IAP
 |

***Incident Objectives:*** Define what must be accomplished to achieve the priorities based on best knowledge of the current situation and the resources available. They include sufficient detail to ensure understanding but are not to be so prescriptive as to preclude innovation.

***Tactics*:** Define how specific actions will be performed to achieve a planned outcome. Tactics specify who, what, where, and when in describing the deployment and direction of resources for implementing strategies to achieve incident objectives.

***Operational Period:***An operational period is the period of time scheduled for executing a given set of operational actions as specified in the Incident Action Plan (IAP). The length of the operational period (typically 12 to 24 hours), is established during first Establish Incident Objectives and Tactics phase and subsequently reviewed and adjusted throughout the life cycle of the incident as operations require.

# Annex A - Functional Checklists

## REOC Executive Director / Manager

The REOC Regional Executive Director is the person in charge of managing the response to emergency situations for their respective regions. The Regional ADM leads the RCMT for their respective Region and provides situational awareness reports to the RCMT, NEOC, CSO and others as required.

|  |  |  |
| --- | --- | --- |
| Activity | % Done | Time/Date |
|[ ]  Convene all the appropriate people to the REOC. |  |  |
|[ ]  Decide with the REOC if others stakeholders should join. |  |  |
|[ ]  Assess the situation and develop an Incident Action Plan with the REOC – deciding on the approach and establishing leads activities and timeframes. |  |  |
|[ ]  Assign an Operations Lead, a Planning Lead and a Logistics Lead. |  |  |
|[ ]  Mandate the team members to report back on their action plan activities. |  |  |
|[ ]  Decide when, how frequently and how the REOC will meet to report back on their activities. |  |  |
|[ ]  If necessary, reassess the situation with the REOC and adapt the action plan. |  |  |
|[ ]  Decide how often Incident Action Plan and Situation Reports should be provided to the RCMT, NEOC, CSO and what they should contain (media information, internal stats, etc.). |  |  |
|[ ]  Confirm tasks and timelines with each team member. |  |  |
|[ ]  Keep in in close communication with the NEOC throughout the process. |  |  |
|[ ]  Makes the decision to cease the REOC meetings and activities. |  |  |
|[ ]  Other incident specific activities: |  |  |

## Safety Lead

The Safety Lead assesses hazardous and unsafe situations and develops measures for safeguarding employees during an emergency. This lead may exercise authority to stop unsafe activities that is imminent danger.

|  |  |  |
| --- | --- | --- |
| Activity | % Done | Time/Date |
|[ ]  Provide guidance and work closely with other team members to prevent workplace accidents and injuries when implementing the Incident Action Plan. |  |  |
|[ ]  Work in collaboration with internal and external partners. |  |  |
|[ ]  Work in close collaboration with the REOC Regional Executive Director. |  |  |
|[ ]  Confirm activities and timeframes with the REOC. |  |  |
|[ ]  Address the health and safety portion of the action plan. |  |  |
|[ ]  Negotiate deadlines and resources when required. |  |  |
|[ ]  Other incident specific activities: |  |  |

## Public Information Lead

The Public Information Lead coordinates all internal and external communications on the emergency situation. The Communications Lead works in close collaboration with the RCC and with the Regional DG of CSB for the three main channels of service and communication – telephone, in-person and Web.

|  |  |  |
| --- | --- | --- |
| Activity | % Done | Time/Date |
|[ ]  Work on the action plan from an internal and external communications perspective. |  |  |
|[ ]  Work in close collaborations with the REOC Regional Executive Director on internal communications. |  |  |
|[ ]  Provide media and social media monitoring assistance. |  |  |
|[ ]  Work on external communications with CSB, who is responsible for the three main channels of communications: telephone, in-person and Web. |  |  |
|[ ]  Confirm activities and timeframes with the REOC Regional Executive Director. |  |  |
|[ ]  Address the communications portion of the action plan. |  |  |
|[ ]  Negotiate deadlines and resources when required. |  |  |
|[ ]  As required, establish groups to address specific activities of the action plan. |  |  |
|[ ]  Other incident specific activities: |  |  |

## Information Technology Lead (IITB)

The Information Technology Lead is in charge of any system issues that relates to the emergency situation. In the case of a cyber-incident or an emergency situation where the emergency concerns primarily the systems, the Information Technology Lead role will merge with the Operations Lead role and the Information Technology Lead would become the Operations Lead.

|  |  |  |
| --- | --- | --- |
| Activity | % Done | Time/Date |
|[ ]  Work on the action plan from a systems perspective. |  |  |
|[ ]  Work in close collaboration with TISMB for the delivery of benefit programs and/or others for the delivery of other programs. |  |  |
|[ ]  Work in close collaboration with Shared Services Canada. |  |  |
|[ ]  Confirm activities and timeframes with the REOC. |  |  |
|[ ]  Address the systems portion of the action plan. |  |  |
|[ ]  Negotiate deadlines and resources when required. |  |  |
|[ ]  As required, establish groups to address specific activities of the action plan. |  |  |
|[ ]  Other incident specific activities: |  |  |

## Operations Lead

The Operations Lead is responsible for the overall coordination of the tactical incident operations.

|  |  |  |
| --- | --- | --- |
| Activity | % Done | Time/Date |
|[ ]  Appointed by the REOC Regional Executive Director. |  |  |
|[ ]  Manage high-level operations. |  |  |
|[ ]  Work on the action plan from an operational perspective. |  |  |
|[ ]  Address the operations portion of the action plan. |  |  |
|[ ]  Keep in communication with the REOC. |  |  |
|[ ]  Ensure interaction is taking place with other branches and partners. |  |  |
|[ ]  Approve expedient changes to the operations portion of the action plan. |  |  |
|[ ]  Negotiate timelines and resources when necessary. |  |  |
|[ ]  Confirm activities and timeframes with the REOC Regional Executive Director. |  |  |
|[ ]  As required, establish groups to address specific activities of the action plan. |  |  |
|[ ]  Other incident specific activities: |  |  |

## Planning Lead

The Planning Lead provides planning and status data for the emergency situation.

|  |  |  |
| --- | --- | --- |
| Activity | % Done | Time/Date |
|[ ]  Appointed by the REOC Regional Executive Director. |  |  |
|[ ]  Work on the action plan from a planning perspective. |  |  |
|[ ]  Provide planning guidance in the development and implementation of the Incident Action Plan. |  |  |
|[ ]  Address the planning portion of the action plan. |  |  |
|[ ]  Confirm activities and timeframes with the REOC Regional Executive Director. |  |  |
|[ ]  Keep in communication with the REOC Regional Executive Director. |  |  |
|[ ]  Collect and manage all incident-relevant operational data. |  |  |
|[ ]  Establish information requirements and provides data reports to the REOC Regional Executive Director. |  |  |
|[ ]  Establish specialized data collection processes when necessary. |  |  |
|[ ]  Determine specialized resources to support the incident action plan. |  |  |
|[ ]  Negotiate timelines and resources when necessary. |  |  |
|[ ]  As required, establish groups to address specific activities of the action plan. |  |  |
|[ ]  Other incident specific Action Plan activities: |  |  |

## Logistics Lead

The Logistics Lead is responsible to provide facilities, transportation, communications equipment, supplies, equipment maintenance, food and medical services during the emergency situation.

|  |  |  |
| --- | --- | --- |
| Activity | % Done | Time/Date |
|[ ]  Appointed by the REOC Regional Executive Director. |  |  |
|[ ]  Work on the action plan from a logistics perspective. |  |  |
|[ ]  Work in close collaboration with the REOC Regional Executive Director and Finance Lead. |  |  |
|[ ]  Address the logistics portion of the action plan. |  |  |
|[ ]  Confirm activities and timeframes with the REOC Regional Executive Director. |  |  |
|[ ]  Determine specialized resources when necessary. |  |  |
|[ ]  Negotiate timelines and resources when necessary. |  |  |
|[ ]  As required, establish groups to address specific activities of the action plan. |  |  |
|[ ]  Other incident specific activities: |  |  |

## Finance Lead (CFOB)

The Finance Lead is responsible for monitoring incident-related costs, administering any necessary procurement contracts and human-resource costs and coordinating facilities request. In an emergency situation primarily affecting departmental facilities, the Chief Financial Officer Branch will become the Operations Lead.

|  |  |  |
| --- | --- | --- |
| Activity | % Done | Time/Date |
|[ ]  Work on the action plan from a finance and administrative perspective. |  |  |
|[ ]  Work in close collaboration with the REOC Regional Executive Director and the Logistics Lead. |  |  |
|[ ]  Work in close collaboration with Public Services and Procurement Canada (PSPC). |  |  |
|[ ]  Confirm activities and timeframes with the REOC. |  |  |
|[ ]  Address the finance and administration portions of the action plan. |  |  |
|[ ]  Negotiate deadlines and resources when required. |  |  |
|[ ]  As required, establish groups to address specific activities of the action plan. |  |  |
|[ ]  Other Incident specific activities: |  |  |

# Annex B – Incident Action Plan (IAP)

|  |  |
| --- | --- |
| 1. **Incident Name**
 | 1. **Operational Period**
 |
|  | **Date** | From: |  | To: |  |
| **Time** | From: |  | To: |  |
| 1. **Current Situation**
 |
|  |
| 1. **Incident Objectives**
 |
|  |
| 1. **Strategies to Achieve Objectives**
 |
|  |
| 1. **Tactics**
 |
|  |
| **7. General Security Message** |
|  |
| **8. Key Communication Message** |
|  |
| **9. Future Outlook** |
|  |

|  |
| --- |
| **10. Briefing/Planning Cycle** |
|  |
| **11. Organizational Structure** |
|  |
|  | **Functional Lead** | **Assigned Resources** |
| **REOC Executive Director/Manager** |  |  |
| **Safety** |  |  |
| **Public Information**  |  |  |
| **Information Technology** |  |  |
| **Operations** |  |  |
| **Planning** |  |  |
| **Logistics** |  |  |
| **Finance/Admin** |  |  |
| **12. Document Management** |
|  | **Name** | **Function** | **Signature** | **Date/Time** |
| Prepared By |  |  |  |  |
| Approved By |  |  |  |  |

**Purpose:**

**\*Operational periods are of no fixed length, however as a guideline they should be no longer than 24 hours.**

The Incident Action Plan (IAP) specifies the objectives, strategies, tactics, and other appropriate information for us in managing an incident.

**Preparation:**

The IAP is usually completed by the Planning functional lead and must be approved by the Incident Commander prior to distribution.

**Distribution:**

The completed IAP may be distributed to all functional leads, and shared with assisting and supporting organizations.

|  |  |  |
| --- | --- | --- |
| Item # | Item Title | Instructions |
|  | **Incident Name** | Print the name assigned to the incident. |
|  | **Operational Period** | Enter the start and end date (YYYY/MM/DD) and time (using the 24hr clock) for the timeframe to which the form applies. |
|  | **Current Situation** | Include specific information on the nature of the incident and known consequences at time of report. This may include information on scope, casualties, hazards, operational considerations, current response activities, outstanding issues, identified needs, etc. |
|  | **Incident Objectives** | **For this Operational Period**, enter clear, concise statements for what needs to be accomplished. Ideally these objectives will be listed in priority order. |
|  | **Strategies to Achieve Objectives** | Enter clear, concise statements to outline the high-level plan to manage this incident and meet the incident objectives. |
|  | **Tactics** | Enter clear, concise statements to explain the specific actions that will be taken |
|  | **General Security Message** | Enter information regarding known security hazards and precautions to be observed during this operational period.  |
|  | **Key Communication Messages** | Enter clear, concise messages to be communicated to internal/external stakeholders, as well as the media.  |
|  | **Future Outlook** | Note potential future developments based on current information. |
|  | **Briefing/Planning Cycle** | Note all incident management-related briefings (which may include media briefings) and Planning Cycle meetings scheduled within the operational period (include time and briefing title/lead). |
|  | **Organizational Structure/chart** | Enter the names of personnel who have been assigned to each function. |
|  | **Document Management** | Enter the name, function and signature of the person preparing and approving the form. |

# Annex C – Situation Report (SitRep)

Région / Region :

**Date:** 2019-06-05

|  |
| --- |
| **Description de la situation :****Situation description :** |
| **Section A : À être complété par le CROU / To be completed by REOC** |
| **Impacts:** |
|[ ]  Danger immédiat pour la vieImmediate Threat to Life |[ ]  Santé et sécurité du personnelHealth and Safety of Staff |
|[ ]  Santé et sécurité des clients publics Health and Safety of Public Clients |[ ]  Public de la prestation de servicesService Delivery Public |
|[ ]  Partenaires fédéraux de la prestation de servicesService Delivery Federal Partners |[ ]  Autres :Other: |
| **Confirmer le degré de gravité de la situation :** **Confirm Activation Level:** |
|[ ]  Extrême – Incident touchant le CANADA – catastrophe majeure, risques graves pour le gouvernement du CanadaExtreme - Incident affecting CANADA – major disaster, serious risks to Government of Canada |[ ]  Élevé – Incident touchant le MINISTÈRE – incident grave, risque grave pour EDSCHigh - Incident affecting the DEPARTMENT – major incident, serious risk to ESDC |
|[ ]  Modéré - Incident touchant la RCN/RÉGION – incidence sur la prestation ou les employésModerate - Incident affecting NHQ/REGION – impact on delivery/employees |[ ]  Faible - Incident touchant les BUREAUX LOCAUX – interruption mineure de la prestation de services ou incident dans l’immeubleLow - Incident affecting LOCAL OFFICE – minor disruption to service delivery or building incident |
| **Défis :** **Challenges:** |
|  |
| **Mesures prises à ce jour :****Actions to-date:** |
|  |
| **Prochaines étapes :****Next Steps:** |
|  |
| **Besoins :****Needs:** |
|  |
| **Temps estimé de résolution :****Estimated Time to Resolve:** |
| **Section B : À être complété par les lignes d’affaire / To be completed by Business lines** |
| **Planification de l’intervention à long terme et approbation du plan d’action en casd’incident :****Forward Response Planning and Incident Action Plan Approval:** | **Activités/Données :****Activities/Metrics:**  |
| 1. | 1 800 O-Canada |  |
| 2. | Web - Données Web spécifique aux pages concernant l’interruption des services postaux / Web Page Metrics related to the postal disruption:  |  |
| 3. | Web – Mon dossier Service Canada / My Service Canada Account |  |
| 4. | Centres Service Canada / Service Canada Centres |  |
| 5. | Communications (DGAPRI) / Communications (PASRB) |  |
| 6. | Prestations d’assurance-emploi (AE) / Employment Insurance Benefits (EI) |  |
| 7. | Pensions publiques :* Régime de pensions du Canada
* Prestations d'invalidité du Régime de pensions du Canada
* Pension de la Sécurité de la vieillesse

Public pensions:* Canada Pension Plan
* Canada Pension Plan disability
* Old Age Security
 |  |
| 8. | Centres d’appels spécialisés (AE/RPC/SV) / Specialized Call Centres (EI/CPP/OAS) |  |
| 9. | Numéro d’assurance sociale (NAS) / Social Insurance Number (SIN) |  |
| 10. | Programme de prestation de services de passeport :* Traitement/centres d’appels
* Rétroaction des clients

Passport Services Delivery Program:* Processing/Passport Call Centre
* Client Feedback
 |  |
| 11. | Programme du travail / Labour Program |  |
| 12. | Programme canadien de prêts aux étudiants / Canada Student Loans Program |  |
| 13. | Programme canadien pour l'épargne-études / Canada Education Savings Program |  |
| 14. | Allocation canadienne aux parents de jeunes victimes de crimes (PJVC) / Canadian Benefits for Parents of Young Victims of Crime (PYVC) |  |
| 15. | Subventions incitative aux apprentis (SIA) / Apprenticeship Incentive Grants (AIG)Subvention à l’achèvement de la formation d’apprenti (SAFA) / Apprenticeship Completion Grant (ACG) |  |
| 16. | Programme de protection des salariés (PPS) / Wage Earner Protection Program (WEPP) |  |
| 17. | Direction générale de l'innovation, de l'information et de la technologie / Innovation, Information and Technology Branch |  |
| 18. | Direction générale des services de ressources humaines / Human Resources Services Branch |  |
| 19. | Direction générale des politiques stratégiques et de service / Strategic and Service Policy Branch |  |
| 20. | Direction générale des compétences et de l'emploi / Skills and Employment Branch |  |
| 21. | Secrétariat ministériel / Corporate Secretary |  |
| 22. | Région de l’Atlantique / Atlantic Region |  |
| 23. | Région du Québec / Québec Region |  |
| 24. | Région de la capitale nationale (RCN) / National Capital Region (NCR) |  |
| 25. | Région de l’Ontario / Ontario Region |  |
| 26. | Région de l’Ouest et des territoires / Western Canada and Territories Region |  |
| **Date et heure du prochain rapport de situation :****Next SitRep Meeting Date/Time:** |
|  |

# Annex D – Incident Management Contact List

|  |
| --- |
| DCMT |
| Commander (DCM) |  Leslie Maclean |
| Coordinator (DCC) |  Elise Boisjoly |

|  |
| --- |
| NEOC |
| NEOC Director / Manager | Bill Danielsen , Jennifer Forsythe |
| Safety (HRSB) | Penny Lavigne, Guy Cyr |
| Public Information (PARSB) | Sean Rowan, Ree Schwartz |
| Information Technology | Marc Larocque, Nathalie Delisle |
| Operations |  Brian Wright, Jenipher Rossall |
| Planning |  Kenneth Johnson, Melanie Gagnon |
| Logistics |  Sylvie St-Arnaud, Jean-David Brouillette, Olivia Truong |
| Finance/Admin |  Diane Rodrigues, Josée Cléroux |

|  |
| --- |
| RCMT |
| ON ADM | Mary-Ann Triggs |
| Benefits Delivery Services Branch, DG | Geoff Anderton |
| Citizen Services Branch, DG | Darren Deneumoustier |
| Program Delivery, DG | Tom Azouz |
| Integrity Services Branch, DG | Kathy Garvey |
| Management Services Branch, DG | Aretha Constant |
| Strategic Services Branch, DG | Mary Crescenzi |
| QC ADM | Claire Caloren |
| Benefits Delivery Services Branch, DG | Rui Costa |
| Citizen Services Branch, DG | Benoit Lymburner |
| Program Delivery, DG | Patrick Lefort |
| Integrity Services Branch, DG | Philippe Emond |
| Strategic Services Branch, DG | Élaine Chatigny |
| ATL ADM | Sarah Filbee |
| Benefits Delivery Services Branch, DG | D. Johnson |
| Citizen Service and Program Delivery Branch, DG | Christine McDowell |
| Integrity and National Services Branch, DG | Jody Doyle |
| Strategic Services Branch, DG | I James |
| Human Resources Services Branch | N. Sutherland |
| Chief Financial Officer Branch | J. Qin |
| Innovation, Information and Technology Branch  | R. Bergeron |
| W-T ADM | Sylvie Bérubé |
| Benefits Delivery Services Branch, DG | Jacqueline Zuk |
| Citizen Services Branch, DG | Pat Chaba |
| Program Delivery, DG | Allyson Rowe |
| Integrity Services Branch, DG | Cam King |
| Strategic Services Branch, DG | Jackson McKiee |

|  |
| --- |
| REDs |
| ON  |  Kathy Garvey, Benoît Gagnon; |
| QC |  Philippe Emond, Denis Lamouche; |
| ATL | Jody Doyle, Michel Bertin; |
| W-T | Cam King, Ricky Dagan-Skedd; |

|  |  |
| --- | --- |
| Region | GD boxes |
| ATL | Atlantic General MailboxATL-INT-SECURITY-SECURITE-GDAtlantic Regional Emergency Operations Centre (REOC)ATL-DIST-REOC-CROU |
| NCR | NCR General MailboxEDSC.RCN.BRS.SECURITE-SECURITY.RSO.NCR.ESDC |
| ON | Ontario Incident MailboxNC-ONT\_INCIDENTS-INCIDENTS\_ON-GDOntario Regional Emergency Operations Centre (REOC)ON-REOC-CROU-GD |
| QC | Quebec General MailboxQc-sécurité-security-DIIS-IISD-GD Quebec Regional Emergency Operations Centre (REOC)QC-REOC-CROU-GD |
| W-T | W-T General and Incident MailboxW-T-Security-Sécurité-GD W-T Regional Emergency Operations Centre (REOC)W-T-REOC-CROU-GD |

# Annex E – Document History

| **Date:** | **Change/Update Details:** | **Approved by:** |
| --- | --- | --- |
| July 2019 | SOP creation | — |
| Sept 2019 | Revised SOP approved at InSNC |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |