INFORMATION INCIDENT RESPONSE PROTOCOL

Public facing | v1.0 September 2024

OVERVIEW OF INCIDENT RESPONSE

This following **Information Incident Protocol** provides an outline of the process the Canadian Digital Media Research Network (CDMRN, or Research Network) uses to identify and respond to information incidents. This document is applicable to all types of incidents.[1] See Figure 1 below for a visual overview of the protocol.

INFORMATION INCIDENT RESPONSE PROCESS

This protocol identifies and describes information incident response through six steps (see Figure 1 for visual overview of the process):

1. Detect & Assess	Continuously monitor social and traditional media for potential incidents and assess when identified.
2. Activate	Activate Information Incident Response Team and begin data collection.
3. Plan	Develop an incident-specific research plan and establish a timeline.
4. Notify	Develop and issue an Incident Notification.
5. Analyze & Inform	Issue ongoing Incident Updates to share research findings and new insights as they emerge.
6. Debrief	Summarize Incident Updates and overall findings, reflect on lessons learned and provide recommendations for future incidents.

[1] As this research program evolves, it is anticipated that additional incident-specific protocols will also be developed to tailor our response capabilities to the complexities of different types of incidents. The process is also anticipated to evolve over time as the Research Network develops further experience with incident response; it will be updated accordingly.

INFORMATION INCIDENT RESPONSE TIMELINE

Although each incident response will follow the steps outlined in this protocol, the timeline of the response will vary based on the five criteria:

1. **Significance** (low versus moderate versus high significance)
2. **Incident Duration** (rapid onset vs protracted)
3. **Urgency** (timeliness of response information needed)
4. **Sensitivity** of the incident (i.e. risk to researchers and/or the organization versus continued value derived from studying the incident)
5. **Complexity** of the incident (the resources and time necessary for research to generate sufficient novel and useful insight on the issue)

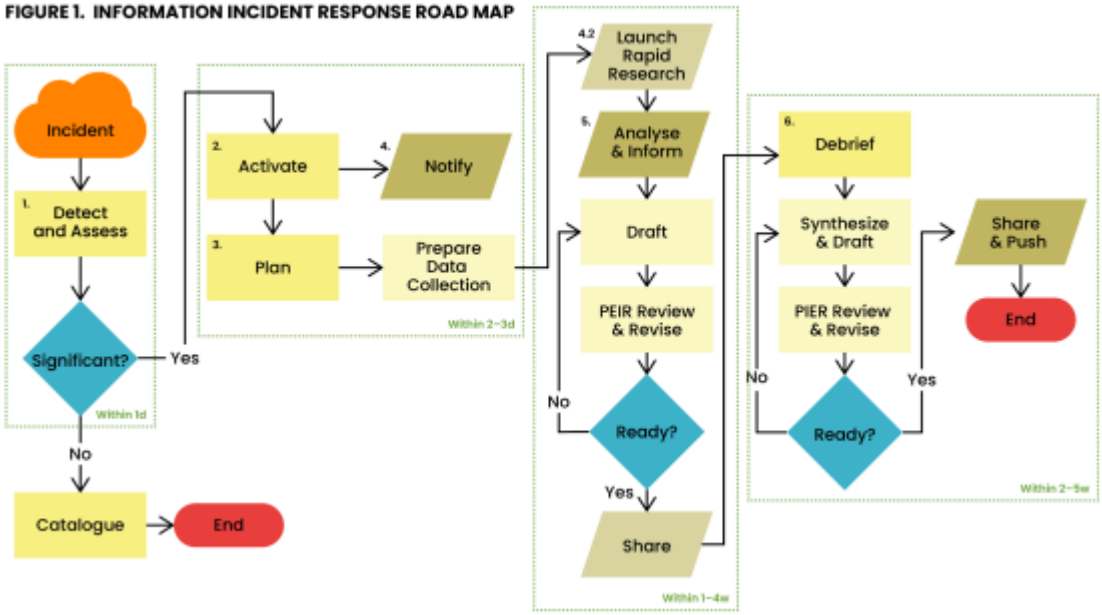
A typical timeline will look like the following:

Within 1 business day	1. Detect
Within 2-3 business days	2. Activate, 3. Plan, 4. Notify
Within 1-4 weeks	5. Inform
Within 2-5 weeks	6. Debrief

ROAD MAP OF INFORMATION INCIDENT RESPONSE

The visualization below provides a visual summary of the information incident protocol, complete with how it maps onto our timeline.

FIGURE 1. INFORMATION INCIDENT RESPONSE ROAD MAP



The following document includes a Table of Contents, a description of each step of the response, a section on incident planning (efforts required before an incident response to build response capability and capacity), and a Glossary of terms.

About

The Canadian Digital Media Research Network is a body of experts that collaborates to fortify and foster resilience within Canada's unique information ecosystem. Our mission is to understand the dynamics of information production, dissemination, and consumption across digital media with the goal of empowering Canadians to navigate the complexities of the modern digital age.

The Media Ecosystem Observatory at McGill University and the University of Toronto, coordinates and supports the Research Network.

Information incident response is part of a broader initiative led by the Project on Information Ecosystem Resilience (PIER). PIER is a research project to support civil society organizations, government, media, public and private institutions to prevent and mitigate, prepare for, respond to and recover from information incidents, and improve information ecosystem resilience.

TABLE OF CONTENTS

1. DETECT & ASSESS | Identify & Evaluate Information Incident Significance

1.1. Detect an information incident

The Research Network conducts ongoing monitoring of social media and news outlets to detect and identify online events that have the potential to become or are considered information incidents. Any member may alert the Incident Commander to the presence of a potential incident. Upon receiving such an alert or identifying a potential incident through some other means, the information incident response protocol is activated.

1.2. Assess the information incident

The Incident Commander, in consultation with relevant stakeholders, evaluates the potential incident according to a predefined set of criteria described below.[2] These criteria can be quickly assessed to identify the significance and severity of an incident. Both current and potential impacts of the incident are considered, even though the criteria are framed in terms of the incident's present state.

Criteria for initial evaluation of an information incident

Speed	Rate of which an incident is spreading throughout the ecosystem
Engagement	Level of engagement with the incident, e.g. level of social media and/or news media coverage
Scale	Size, nature and/or diversity of population affected, e.g. large vs. small population, multiple communities affected or a particular vulnerable community affected

[2] An information incident classification matrix is in development and will be implemented for faster, more generalizable classification of incidents in the future.

Criteria for initial evaluation of an information incident	
Scope	Characteristics of the ecosystem affected, e.g. political, economic, social, cyber sub-systems; information integrity, political perception, public trust, social cohesion, faith in democratic institutions, etc.
Complexity	The resources and time necessary for research to generate sufficient novel and useful insight on the issue as well as the extent of uncertainty of scope and scale.
Intervention efforts	Resources required to respond to/maintain the incident.
Learning potential	Potential to learn from, inform and prepare for more severe events in the future.

If an incident is deemed NOT to be significant::

Catalogue & document the no-go decision

The Incident Commander generates a high-level written summary of the event, key sources, rationale for the non-significance decision, high-level insights and observations, and relevant lessons learned. These documents are generated so they can be compiled into an annual report on "close-call incidents".

If an incident is deemed to be significant:

Categorize & identify features of the incident

The Incident Commander identifies the type and features of the information incident to enable activation of the most knowledgeable subject matter expertise.

2. ACTIVATE | Trigger Information Incident Response

2.1. Activate the Incident Response Team

The Incident Commander coordinates the activation of an Incident Response Team specific to the incident:

1. **Broadcast message to the Research Network** - activate the Research Network through an internal broadcast message announcing the detection of an information incident and soliciting engagement.
2. **Solicit engagement from Information Incident Expert Roster** - in addition to the broadcast message, send a targeted follow-up message to specific researchers, both in and outside the Research Network, whose expertise is particularly relevant for the type and characteristics of the information incident (as identified in step 1.2).
3. **Formalize Incident Response Team** - confirm all members of the Incident Response Team (IRT) that are available to contribute to the response. Each IRT will consist of an Incident Commander, communications, incident-specific experts, as well as researchers skilled in digital trace and survey media monitoring and analysis techniques..

2.2. Prepare Data collection

The Incident Commander initiates relevant data collection as soon as the protocol is activated including:

1. **Survey** - customization of the rapid-response survey for the incident to address questions as it relates to awareness, perception and understanding, potential impacts and expected responses; and communication with the survey provider to establish intention for survey launch.
2. **Digital trace** - identification and collection of digital trace data that may need to be saved quickly before content is taken down.

3. PLAN | Develop Incident-Specific Research Plan

3.1. Generate Research Plan

The Incident Commander coordinates an incident response team meeting to generate a rapid research plan for incident update topics and develop a timeline for release. Objectives for the first Incident Response Team meeting include:

- Establishing the **purpose** and **objectives** of the response to the specific information incident;
- Identifying preliminary **research questions**;
- **Assigning research topics** among the incident response team to address research questions; assign leads and supporting members;
- Identifying a research **timeline** for each incident update and compile a draft publishing schedule for all incident updates;
- Identifying **resource (or surge capacity) needs**, e.g. needs for additional resources or sharing resources to enable rapid research.

3.2. Supplementary data collection

Survey is finalized and launched with the survey provider, in line with IRT timelines and research needs. Highly relevant digital trace data that did not meet the criteria for 2.2 is collected to meet the research needs.

4. NOTIFY | Issue Incident Notification

4.1. Prepare Incident Notification System

The communications team prepares a new section on the Research Network website for the incident.

4.2. Develop Incident Notification

The IRT develops an incident notification that provides the following information:

- Overview of the incident
- Background information
- Incident Timeline
- Incident Relevance (why it's important)
- What are we doing about it (key questions guiding the response)
- Research Response (planned approach)
- Research Partners (member organizations engaged in the response)
- Key contacts for news/media inquiries

For previous examples of notifications, see those for Kirkland Lake Bot Campaign and Russian Funding of US and Canadian Political Influencers.

4.3. Share Incident Notification

The communications team (in close collaboration with the IRT) disseminates the incident notification broadly through social media, website, mailing lists, and broader network of contacts:

- **Social media** - the initial Incident Notification is posted on Linkedin, Instagram and X.
- **Media outreach** - broadcast that the response team is monitoring the situation. Journalists who have expressed interest (including those who have covered the story) about a specific incident are contacted.
- **Subscribers list** - an email is sent to our subscribers list to inform them of the incident, provide more context, and let them know that our team has activated its response protocol.

5. ANALYZE & INFORM | Issue Ongoing Incident Updates

The bulk of the incident response consists of developing and sharing Incident Updates (research findings for specific research questions) as they emerge. Using the initial incident notification as a foundation, the aim of each Update is to generate novel information on the incident.

5.1. Launch Research and Analyze Data

Each member of the IRT, with support from the Incident Commander, is responsible for mobilizing resources to develop their Incident Update(s). Steps may include:

- Analyzing data from the rapid response survey;
- Collecting and analyzing supplementary and core digital trace data;
- Tasking their research team with specific actions related to their Incident Update(s);
- Ensuring clear channels of communication are established.

5.2. Draft Submission

Incident Updates will provide novel information in one or more of the following areas:

- **Nature and context of the incident** (What caused the incident? Why did it happen? Who is responsible? How did the incident unfold across the information ecosystem?)
- **Situating the incident** (How significant is this incident in the bigger picture? Is the incident unique, repeated, or likely to occur again)
- **Observed and/or potential impacts** (What amplified the incident? What are the immediate and downstream direct and indirect impacts? Who is affected and how? What are the implications of these impacts?)
- **Recommendations and lessons learned** (What vulnerabilities or emerging threats were identified from this incident? What can we learn to inform future planning? What should we do about it?)

Situational awareness and deeper understanding of the incident is developed through distributed study over time, i.e. each update acts as a puzzle piece among a broader investigation. Results are drafted as they emerge, they are critiqued through

rapid peer-review (see 6.3 PIER review below) and shared on a very short-turnaround period.[3]

Each research lead and team of supporting researchers compile their findings, write and share their first draft for review.

5.3. PIER Review and Revise (In-house Rapid Peer-Review)

The PIER review team (small group of diverse subject-matter experts) reviews the incident update and provides feedback to the lead author within one working day. This team acts as a rapid peer-review panel to ensure research findings shared are as clear and accurate as possible.

5.4. Share Update via Social Media

The communications team works with the lead of each Information Update to create social media post(s) to highlight sharing the update and direct readers to the Research Network website which hosts all Incident Updates. Updates will be shared on at least one social platform, with high-impact Updates shared across multiple social media platforms.

5.5. Continuously assess further need

As Incident Updates are published, the Incident Commander, in consultation with the full Incident Response Team, continuously evaluates the value of additional updates and resources devoted to the incident. The continued relevance of the incident, future likelihood of a similar incident, resources and time necessary for research to generate further novel and useful insight on the issue, and risk to impacted individuals and/or impacted organizations, are all accounted for in such a determination.

[3] Note, while this approach is meant to provide information as fast as it is discovered, this implies periodically later results may revise previous ones. Corrections are made and changes are highlighted when this is the case.

6. DEBRIEF | Issue Incident Debrief

Once a determination has been made to conclude the response, no further Incident Updates will be produced. At this point the Incident Commander closes the incident and issues, in collaboration with the full Incident Response Team, an Incident Debrief.

6.1. Synthesize all research findings & draft report

The Incident Debrief serves as a final comprehensive summary of an information incident and the organization's response. It consolidates findings from Incident Updates, offers key insights, and provides actionable recommendations to mitigate future risks. The Incident Debrief may include some or all of the following sections:

- **Incident Overview**: A brief summary of the incident, including key dates, involved parties, and the overall nature of the event.
- **Incident Response Actions**: An overview of the steps taken by the IRT, including communication, relevant research methods, technical responses, and mitigation efforts.
- **Timeline of Events**: A chronological breakdown of major events related to the incident, including initial detection, responses, and updates.
- **Public and Media Reaction**: A summary of how the incident was perceived and discussed externally, including media coverage and public discourse.
- **Key Findings**: A synthesis of research and data collected during the investigation, with conclusions drawn from both qualitative and quantitative analyses.
- **Analysis of Causes:** A detailed assessment of the root causes and factors contributing to the incident, including any system vulnerabilities or external influences.
- **Impact Assessment:** A summary of the direct and indirect impacts (or downstream consequences) of the incident, including who was affected.
- **Vulnerabilities Exposed**: A description of any specific weaknesses uncovered by the incident and their potential for future exploitation.
- **Threat Assessment**: An evaluation of future risks posed by the same or similar actors or methods, considering the broader implications of the incident.

- **Lessons Learned**: Identification of important takeaways from the incident, highlighting gaps in current processes, response improvements, and preventative measures for the future.
- **Recommendations**: Actionable suggestions aimed at reducing the risk of similar incidents in the future, including technological, procedural, and policy changes.

6.2. PIER Review & Revise

All members of the IRT as well as the PIER review team will review and revise the draft Incident Debrief to ensure that the document is accurate, comprehensive, and aligned with the organization's standards for incident reporting.

6.3. Translate and compile

Upon review, the Debrief is translated into French and any other necessary languages to ensure accessibility. A single document is created, compiling the incident notification, all subsequent incident updates, and the full debrief in both French and English. This compilation ensures that stakeholders have access to all relevant materials in a consistent and organized format.

6.4. Share final incident debrief

The final Debrief is distributed to the public and relevant stakeholders. This involves media outreach (our media mailing list and targeted journalists who have worked on this topic), social media dissemination (on Linkedin, X and Instagram), subscribers list and direct sharing with impacted organizations and individuals. The aim is to raise awareness, provide clarity on the event, and offer guidance on preventing similar incidents in the future. Messages will typically include the following information: a recap/overview of the event (very short), an explanation of what all teams investigated, initial questions and their answers, vulnerabilities and conclusion/key takeaways!

Information Incident Planning

The information incident response process is predicated on the ongoing development of underlying capability and capacity of the Research Network to mobilize prior to and during an incident. The dependencies required to do so include:

- Pre-establishing **roles & responsibilities** for leadership, collaboration, communications and research support.
- Building a **virtual communications infrastructure** for distributed communication and collaboration prior to, during and post incident.
- Generating **forms, templates, pre-established research questions** that can be used to facilitate rapid deployment of incident notifications, incident updates, debriefs, and our incident response survey.
- Establishing a **fan-out list** of all internal and external partners of the Research Network to notify in the event of an activation.
- Building a **roster of information incident experts** that can act as advisors and/or collaborators during an incident, as well as respond to media inquiries.
- Building **impactful communications capability** by developing a communications strategy, building significant social media presence and influence, and preparing a **template** of content to be shared.
- Formalizing **collaboration agreements**, e.g. Memorandums of Understanding (MOUs) with Research Network members and affiliates.
- Clarify and ensure all **ethical and legal precautions** are clearly identified and articulated to provide guidance during an incident response.
- Ensuring **financial infrastructure** is established and agile in the event rapid disbursement of funds are needed beyond normal operational protocols.
- Ensuring **team readiness** through ongoing discussion, development, and reflection prior to, during and post information incidents.
- Building and evolving **data collection infrastructure** to ensure continuous data intake and agile/adaptable data collection infrastructure and processes.
- Developing and sustaining relationships with subject matter experts (interdisciplinary, academic and practitioner), traditional media organizations, and broader intended stakeholders and beneficiaries that depend on and/or would like to **collaborate in incident response**.

Glossary

Canadian Digital Media Research Network: A pioneering initiative committed to fortifying and fostering resilience within Canada's unique information ecosystem. Our mission is to understand the dynamics of information production, dissemination, and consumption across digital media with the goal of empowering Canadians to navigate the complexities of the modern digital age.

Information ecosystem: The sum of complex but analyzable set of relationships found in and across digital media. An online information ecosystem is thus composed of interconnected but distinct communities across social and traditional media. Distinct because of the different platforms that constitute it but interconnected by a common set of individuals and organizations (entities) who share information and relationships across multiple platforms.

Information incident: A disruption in the information ecosystem, including both sudden and prolonged interruptions, that significantly impacts the normal flow and/or integrity of information, leading to potential or actual harm to the public, government, Canadian democracy, and/or the broader information ecosystem.

Incident Commander: The role that oversees all aspects of an information incident response. Their responsibilities include the coordination of response efforts, resource allocation, and decision-making during an incident. The Incident Commander is tasked with establishing objectives, ensuring communication across all involved parties, and managing operational strategies to effectively control the situation.

Information Incident Expert Roster: List of pre-identified and pre-vetted interdisciplinary subject matter experts, academic or practitioner, from within Canada or abroad. Individuals are included in the list if they are available to provide expert opinion, collaborate on rapid research, and act as a key contact for media and the broader public during a response on a very short turnaround period.

Incident Response Team: a group of individuals and organizations assembled to respond to and manage a specific information incident. The Incident Response Team is responsible for collectively organizing and delivering an effective response to minimize impact and maximize resilience to the information incident. Members of the Incident Response Team are drawn from the Research Network as well as the broader national and international information ecosystem health community of practice.

PIER Review Team: An interdisciplinary, academic-practitioner collection of subject matter experts not involved in the development of an incident update that conducts a rapid-peer review of the research before publication.

Project on Information Ecosystem Resilience (PIER): A Research Network research project to support civil society organizations, government, media, public and private institutions to prevent and mitigate, prepare for, respond to and recover from information incidents, and improve information ecosystem resilience.

Rapid Response Survey: A survey instrument that is developed, launched and analyzed within a maximum one week cycle. A generic survey core is developed prior to an incident and customized during activation. It assesses awareness, perceptions & understanding, potential impacts, and expected outcomes/responses of a specific incident and associated issues.