Crisis Communication Plan

INSTRUCTIONS FROM ECOSYSTEM

Last Updated May 2025

ecosystem

Table of Contents

1

Overview

Purpose

In a crisis, every second counts. The last thing you should be doing is creating a plan in the middle of an emergency; there simply isn't the time. That's why this playbook was developed proactively, to provide a clear and consistent framework for identifying, responding to, and recovering from crises.

This guide focuses on situations that require immediate action or may involve media attention. While health and safety events can qualify as a crisis, if a site manager has the situation under control, they should contact Jerome Bergeron, Director of Health and Safety, directly. For Ecosystem's standard OSHA-approved Health and Safety Plan, [click here.]

Crisis vs Incident

Whether a situation qualifies as a crisis often depends on its severity. To determine the level of seriousness, consider the following factors.

	Crisis	Issue
Urgency	**High:** requires immediate decisions and actions	**Low to moderate:** allows time to evaluate and prepare an appropriate response
Impact	**Widespread:** threatening lives, the environment, operations, or the company's reputation	**Local:** affects specific teams or operations without endangering core business functions
Scope	**Severe:** often requires involvement from executive leadership and the Communications team	**Manageable:** Can generally be addressed through standard operational practices
Action	**Reactive:** focuses on immediate damage control	**Proactive:** centers on monitoring, communication, and strategic planning to prevent escalation
Timeframe	**Explicit:** immediate window of time for resolution	**Variable:** can unfold over days, months, or years
Risk	**Unquantifiable:** the potential of risk is so significant that it cannot be easily measured	**Quantifiable:** outcomes can be measured and assessed

In a crisis, speed, accuracy, and consistency are crucial. As Ecosystem values complete transparency, we are committed to keeping employees informed throughout the process, though the details may be temporarily limited. Once an action plan is activated, all employees will receive a debrief to ensure clarity and alignment.

While it may take several days to complete a full investigation and develop a comprehensive "Lessons Learned" report, we recognize that uncertainty can cause concern. Employees are encouraged to reach out to their direct managers for updates or clarification.

If you review the criteria above and believe a situation may meet some of the crisis identifiers, err on the side of caution and report it immediately to your direct manager. If the situation is clearly a crisis, contact Nathalie Lachance, Vice President of Communications and Human Relations, right away.

Crisis Management Framework

A crisis is any event or situation that threatens the organization's people, operations, reputation, or stakeholders. A crisis can vary in types and severity.

Common crisis categories include, but are not limited to:

- Operational: system failures, workplace accidents, shutdowns
- Reputational: public backlash, misinformation
- Financial: fraud, sudden losses, or significant misalignment
- Legal/Compliance: regulatory violations, lawsuits, or ethical breaches
- Personnel: leadership misconduct, sexual harassment, or other types of employee harm
- Environmental: natural disasters, severe weather, pandemics
- Security: data breaches, hacking, or cyberattacks

Roles & Responsibilities

Ecosystem has established a Crisis Management Team (CMT) to guide the company through any severe or high-impact crisis. The members of this team ensure timely decisions, transparent communication, and coordination across all departments. Contact information for CMT members can be found in the Appendix.

Crisis Lead - Nathalie Lachance & Jerome Bergeron (Health and Safety)

The two Crisis Leads are the primary decision-makers and guide all aspects of the crisis management strategy, especially in defining strategic priorities. This role coordinates with members of the CMT and any other executive leadership that may be involved to ensure the strategy is executed immediately and effectively.

Legal Counsel - Patrick Raby

Patrick serves as the main liaison between Ecosystem and its external legal counsel. He provides real-time updates, reviews communication material for legal accuracy, and advises the team on what can be disclosed publicly. Patrick will work closely with the Communications Team to ensure that all messaging complies with legal and regulatory standards.

Executive Spokespersons - Andre Rochette and Lynne McArthur

As Ecosystem's founder and CEO, both individuals serve as the company's official spokespersons. They communicate strategically and transparently with clients, stakeholders, and the media. Alongside the Crisis Leads, they play a key role in high-level decision-making and in reinforcing Ecosystem's commitment to accountability and trust.

Communications - Marie-Christine Fournette & Michele Midori

The Communications Team develops and executes all crisis communication plans, ensuring timely and accurate dissemination of information with both internal and external audiences. Together, they ensure all public and internal statements reflect Ecosystem's commitment to transparency.

Marie-Christine oversees real-time media alerts, press inquiries, and external messaging. Michele monitors all digital channels, including social media, and manages online communications.

HR and Employee Relations - Marianne Roberge (CA) and Jyoti Krishan (US)

The HR and Employee Relations Leads act as the liaisons between executive leadership and company employees. They assess potential impacts on morale, productivity, and workplace safety, coordinate employee communication and support, and manage policies and future training related to the issues at hand.

Operations - Sylvie Barbeau (CA) and Max Lamirande (US)

Both individuals will organize and deploy all necessary staff, including construction managers, site supervisors, and engineers, to implement solutions that minimize disruptions to projects. They ensure all relevant logistics are communicated and executed efficiently to all affected parties.

IT and Data Security - Eric Côté

Leads the team of IT specialists in identifying and containing any data breaches or cyberattacks. His team works to restore systems, secure data, and minimize operational impact while providing regular updates to the CMT.

2

Crisis Identification & Escalation

Identifying a potential crisis early allows Ecosystem to respond quickly, minimize risk, and maintain trust with employees, clients, and stakeholders. The following outlines how crises are detected, assessed, and escalated to the appropriate decision-makers.

Detection & Early Warning Systems

Ecosystem uses multiple monitoring channels to identify, and sometimes stop, potential risks before they escalate into full crises. Any potential issues detected need to be documented and reported immediately to the relevant department managers, who will escalate the issue as needed.

Detection Methods:

- Client and Partner Feedback Surveys: responses are collected from clients and partners on a quarterly basis. Any concerns, complaints, or unexpected inquiries that may lead to reputational or operational issues are acted on immediately.
- Regulatory and Legal Notifications: alerts from government agencies in Canada and the US, inspectors, or external auditors signaling compliance risks.
- Media and Social Monitoring: continuous monitoring of social media platforms, digital channels, and the media for mentions of Ecosystem and any of its projects.
- Internal Reports: Employee observations, near misses, and operational disruptions reported through managers.
- Technology Alerts: Automated system notifications sent directly to the IT department, identifying data breaches, cyber attacks, or technological infrastructure failures.

Assessment Criteria & Crisis Decision Matrix

To determine whether an issue qualifies as a crisis, assess it using the factors outlined in the chart on the following page. Consult the Crisis Decision Matrix to determine the appropriate response level and escalation path.

Assessment Criteria

Criteria	Questions to Consider
Severity	Does this event threaten people, the environment, project operations, or company reputation?
Impact Scope	Is the issue limited to one project or site? Does it affect multiple locations or stakeholders? Could it cause physical harm? Will it interrupt operations?
Time Sensitivity	How urgently should an action be taken to minimize damage or harm?
Visibility	Is this event isolated, or is it likely to go public?
Operational Disruptions	Does this event affect key business functions? Will any projects or sites need a temporary or permanent shutdown?
Legal Risk	Could this event have any legal repercussions? Are any compliances being violated?
Likelihood of Escalation	Should I bring this issue up to my manager? Could it worsen or attract negative media attention?

Crisis Decision Matrix

Level	Crisis	Issue
Level 1 - Incident	Localized, limited impact, minimal disruption.	Managed at the departmental level using standard operating protocols.
Level 2 - Elevated Issue	Moderate impact with potential to affect operations or reputation.	Department lead alerts Crisis Leads for guidance; begin internal communication preparations.
Level 3 - Crisis	High-impact event affecting people reputation, or operations. Media or public attention likely.	Full CMT activated. Implement crisis communication and management plan immediately.

When in doubt, escalate. It is always better to over-report an issue than to delay response to a genuine crisis. If any answers to the previous questions are unclear, contact the project lead or your direct manager to report it. Early notification allows Ecosystem to manage and avoid risk, control the narrative, and protect our employees and reputation effectively.

Escalation Path

Once an issue meets the threshold for escalation, the following four-step process ensures that the crisis is addressed at the correct level and with the right urgency.

Step 1: Initial Detection

Who: Any employee, manager, or automated monitoring system

Objective: *Identify and document potential risks early*

- Recognize an unusual or concerning event (e.g., safety incident, data breach, reputational issue, and system outages).
- Verify the situation through available facts, avoiding any assumptions or speculations
- Document key details
  - Who is involved?
  - What occurred?
  - When and where did it happen?
  - Why or how did it happen?
  - What is the potential or actual impact?
- Notify your direct manager or relevant department lead immediately

Step 2: Department Review

Who: Direct managers or relevant department lead

Objective: *Evaluate and classify the issue*

- Review the documented situation against the crisis assessment criteria (impact on safety, operations, finances, reputation, or stakeholders).
- Determine whether the event can be resolved internally or must be escalated to the Crisis Leads
- If escalation is required:
  - Notify Nathalie Lachance and/or Jerome Bergeron
  - Provide all supporting information gathered to date
  - Maintain internal confidentiality to prevent misinformation

Step 3: Activation of the CMT

Who: Crisis Leads (Nathalie Lachance and/or Jerome Bergeron)

Objective: *Mobilize an organized and coordinated response*

- Review the situation and determine if the event qualifies as a crisis
- If confirmed, activate the CMT and send a notification via the emergency communication protocol (Teams alert in the CMT channel and/or SMS)
- Assign an internal case ID for documentation purposes
- The Crisis Leads will:
  - Establish immediate priorities (safety, containment, and communication)
  - Convene the CMT within the first 15-30 minutes
  - Determine whether executive leadership or legal counsel should be briefed immediately

Step 4: Ongoing Assessment

Who: Full Crisis Management Team

Objective: *Continuously evaluate, adapt, and stabilize the response*

- Monitor new information as it becomes available
- Reassess the crisis level regularly (using the Decision Matrix)
- Adjust response strategies as the situation evolves
- Document all actions, communications, and decisions for accountability and future learning

3

Crisis Activation

Communication Strategy

The core principles of crisis management strategy are accuracy, speed, empathy, and consistency behind the messaging. All external statements must be authorized with the CMT's verified information. A First Hour Checklist can be found in the Appendix.

Internal Communications

- Issue a short Intranet and Teams post acknowledging the crisis and confirming it is being handled
- Specify who is authorized to discuss the issue (typically Andre, Lynne, or Nathalie)
- Emphasize confidentiality and discourage speculation or gossip
- Send a Teams notification and company-wide email directing staff to the official post for updates

External Communications

Media Protocol

- Only Marie-Christine and Nathalie may engage with journalists
- When appropriate, proactively reach out to trusted media to establish the narrative
- Maintain message consistency; avoid speculation or unverified claims
- Use empathy-forward language focused on resolution and safety
- Train reception and admin teams to redirect all media calls to Nathalie.
- Employee statement if approached by media: "I am not authorized to speak to the media. Please direct all questions and inquiries to our Media Relations Lead, Nathalie Lachance."

Stakeholder Updates

- Determine which clients, partners, or stakeholders should be informed based on the crisis type and location.
- Only Business Development Managers or Directors may contact their assigned clients.
- Choose the most appropriate channel (phone, in-person, email)
- Outline that an action plan is underway, and indicate whether external advisors (PR, legal, technical) are involved
- Refer to the Communication Templates in the Appendix for approved language

Vendor & Subcontractor Updates

- Determine which vendors and/or subcontractors should be informed based on the crisis type and location
- Project Directors and Construction Team Leads may contact their assigned vendors and/or subcontractors
- Choose the most appropriate channel (phone, in-person, email)
- Outline that an action plan is underway, and indicate whether external advisories (PR, legal, technical) are involved
- Refer to the Communication Templates in the Appendix for approved language

Social Media

- Only Michele Midori may publish to official Ecosystem accounts based on approved CMT statements
- All employees are prohibited from posting about the crisis or responding to direct messages related to it
- See the company's Social Media Policy for full guidance

Digital and Media Monitoring

- Michele Midori, with Laura Henderson as support, will monitor social and digital conversations for sentiment and misinformation.
- Any media mentions or inquiries online must be escalated to Marie-Christine and Nathalie
- Monitoring will occur through Hootsuite streams, updated regularly with key reporters and outlets
- Only official Ecosystem accounts may publish responses or clarifications once the holding statement is approved

Communication Templates

Pre-approved templates of various crisis types can be found in the Appendix.

4

Recovery & Post-Crisis Evaluation

A crisis does not end when the immediate threat is resolved. Recovery ensures operations return to normal safely and efficiently, while evaluation ensures the organization learns from the event and strengthens future resilience. This phase focuses on restoring business continuity, reviewing the effectiveness of the crisis response, and implementing improvements.

1. Return-to-Normal Plan

Objective: *Safely resume standard operations while maintaining control, consistency, and awareness of any lingering risks.*

1.1 Stabilization

- Confirm that immediate risks have been neutralized (safety, technical, operational, and reputational)
- Ensure emergency or temporary procedures can be phased out
- Validate that impacted systems, sites, or teams are secure before resuming work

1.2 Operational Restorations

- Restore all halted or impaired business functions
- Conduct equipment, system, or network checks (IT, facilities, operations)
- Communicate “all clear” notices to relevant teams, with instructions for any modified operating conditions
- Ensure employee well-being and ability to return to work safely

1.3 Stakeholder Notification

- Update clients, partners, and vendors as needed:
  - Status of operations
  - Expected timelines
  - Any remaining impacts
- Provide follow-up messaging (internal + external) prepared by the Communications team and approved by Legal

1.4 Documentation of Restoration Steps

- Record timelines for reopening, system restoration, staff return, and public communication
- Note any remaining risks or monitoring measures still in place

After-Action Review (AAR)

Objective: *Conduct a structured evaluation of the organization's crisis response to identify strengths, gaps, and necessary improvements.*

2.1 Timing

The AAR should occur within 3-7 business days of crisis stabilization, while information is fresh, but emotions have settled

2.2 Required Participants

- Crisis Leads
- Communications
- Legal
- HR
- Operations
- IT/Data Security
- Executive spokespersons
- Any additional subject matter experts involved in the incident

2.3 Core Questions

The AAR focuses on five areas:

- What happened?
  - Timeline of events
  - Point of detection
  - Triggers and escalation
- What was done well?
  - Rapid response actions
  - Effective communication
  - Stakeholder engagement
  - Team collaboration
- What challenges emerged?
  - Delays in detection
  - Gaps in communication or approvals
  - Resource limitations
  - Conflicts between departments
- What could have gone better?
  - Missing protocols
  - Incomplete checklists
  - Miscommunication
  - Unclear roles
- What should be improved now?
  - New procedures
  - Staff training
  - Revised communication templates
  - Updated escalation paths

2.4 Evidence Collection

- Email and communication logs
- Media coverage
- Social media monitoring reports
- IT or operational logs
- Internal reports or witness statements
- Timeline documentation from the CMT

3. Lessons Learned Report

Objective: *Produce an official, shareable report summarizing insights and recommended changes.*

3.1 Report Components

- Executive Summary
  - Description of the crisis
  - High-level outcomes
- Incident Overview
  - What happened
  - Who was impacted
  - Crisis category and severity
- Response Summary
  - Actions taken
  - Performance of the Crisis Management Team
- Strengths Identified
  - What worked well
  - Positive stakeholder feedback
- Areas for Improvements
  - Gaps in procedures, communication, or training
- Recommendations
  - New policies
  - Revised protocols
  - Technology improvements
  - Staffing or resource considerations
- Timeline Appendix
  - Verified fact-based chronology

3.2 Distribution

- Executive leadership
- Crisis Management Team members
- Department leaders
- HR (for training updates)
- Operations/IT (for procedural updates)

3.3 Employee Sharing

A summarized, non-sensitized version will be issued on the Intranet by Jerome to employees to reinforce transparency and organizational trust.

4. Policy & Training Updates

Objective: *Convert insights into actionable improvements that reinforce preparedness and prevent recurrence.*

4.1 Policy Updates

- Revise crisis escalation criteria
- Update communication templates
- Modify social media, media relations, or internal notification policies
- Adjust safety or cybersecurity procedures

4.2 Training and Education

- Update learning modules for crisis roles
- Conduct refresher training for:
  - Managers
  - Employee relations staff
  - Spokesperson
  - Digital monitoring team
- Incorporate crisis learnings into:
  - New hire onboarding
  - Annual compliance training
  - Tabletop exercises and simulations

4.3 Simulation Exercises

- Schedule tabletop or live simulations based on the crisis type
- Test updated procedures, communication flows, and escalation paths
- Capture new insights and refine materials as needed

4.4 Implementation Timeline

- Assign owners and deadlines for each update
- Provide quarterly progress reports to Crisis Leads
- Verify that all corrective actions are completed

5. Crisis Closeout

Objective: *Formally conclude the crisis, ensuring recovery steps and improvements are documented and communicated.*

- Crisis Leads certify that operations have fully normalized
- All documentation is archived in the crisis management repository
- A final communication will be sent to employees summarizing recovery and reinforcing key messaging
- Crisis is officially closed

New York

462 7th Ave Floor 22
New York, NY 10018
(646) 692 7800

Boston

(617) 838 6100

Los Angeles

(213) 534 7985
License #1089288

Toronto

8 King Street East, Suite 910
Toronto, ON M5C 1B5
(416) 649 1298

Montreal

407 McGill Street, Suite 600
Montreal, Quebec H2Y 2G3
(514) 940 5156

Quebec

2875 Laurier Blvd.
Delta 3 Building, Suite 950
Quebec, Quebec G1V 2M2
(418) 651 1257

ecosystem-energy.com