IT Disaster Recovery Crisis Communications - Template

Crisis Communications Framework

VERSION 1.2

MAY 15, 2023

Prepared by

Cybersecurity Division

Technology and Innovation

Table of Contents

Approved by:	**Owner:** Director Governance Risk and Compliance	
Approval date: 18-April-2023	**Reviewed date:** 18-April-2023	**Next review date:** 31-March-2024
Contact: Cyberalberta@gov.ab.ca	**Policy Instrument type:** Framework	

IT DISASTER RECOVERY – CRISIS COMMUNICATIONS FRAMEWORK

About this Plan

This template is designed to assist in the development of a Crisis Communications Plan and will be a supplement to the IT Disaster Recovery Plan. Ensure that the plan developed aligns with the organization's Business Continuity Plan and Communications Plan. It is advisable that the Communications Officer and Business Continuity Officer review this document. Keep it brief! Instead of paragraphs of verbiage, consider using tables, matrices, diagrams, charts. Create a short 'quick reference' guide to accompany this plan.

EMERGENCY NOTIFICATIONS

If an event or impending event has the potential to cause harm to staff, an emergency notification will take place at the site level by the building's Facility Emergency Response Team (FERT). This team is guided by a Facility Emergency Response Plan (FERP), specific to the work site. If required, staff will be directed to follow life-safety Emergency Response actions such as evacuation or 'shelter in place' procedures. <Provide link to FERPs and other Emergency Response Plans in the Reference section>

The top priority for all staff should be to make sure that they are out of harm's way and that they remain safe!

CRISIS NOTIFICATIONS

The Process

Life and safety takes priority. Stress that emergency procedures are followed before initiating the notification process.

IMPORTANT: If there is an imminent threat to life and/or property, activate fire alarm/panic button, or call 911 first

Example Communications Matrix:

COMMUNICATIONS MATRIX				
Severity of Event	**Impact of Event**	**Key Messages Delivered By**	**Audience**	**Communication Channels**
Minor	– No loss of life, no injuries – Little to no damage to assets or facilities – Critical services not disrupted – Little to no media interest	– Director – Manager	– Affected site level staff – Other staff, depending on situation – Media, if public might be impacted	– Email – Telephone (call tree) – MS Teams – SMS ('Text) Messaging
Moderate	– No loss of life, some injuries – Damage to facilities requiring relocation of less than 2 weeks – Critical services may be disrupted – Potential physical security threat to staff or infrastructure – Local media interest	– Division's ADM – Communications Director if more than one Ministry or Public is impacted – Division's Executive Director – Directors in affected Divisions, Branches, Offices, Business Units	– Staff in affected Divisions, Branches, Offices, Business Units – Media, if public might be impacted	– Email – Telephone (call tree) – MS Teams – SMS ('Text') Messaging <add more as required>
Major	– Loss of life, extensive injuries – Extensive damages or facilities are destroyed, requiring relocation of more than 2 weeks – Critical services cannot be delivered – Imminent physical security threat to staff or infrastructure – Regional, National media interest	– CEO –	– All staff – Media and Public	– Email – Telephone (call tree, mass automated, 1-800 line) – MS Teams – SMS ('Text') Messaging – Social media: Twitter, Facebook (provide links) – Media notification (e.g. news releases online bulletin, etc.) <add more as required>

KEEPING EMPLOYEES INFORMED

Staff will be provided with updates and instructions as soon as possible. Who delivers the information, as well as the mode and frequency, will depend on the nature of the event and its impacts. Refer to the **Communications Matrix** for more information.

<Consult with the Business Continuity Officer and/or Communications Officer…a process may already exist>

STATEMENT OF CONFIDENTIALITY/FOIP

Briefly:

1. Address FOIP
2. Address Confidentiality
3. Address distribution restrictions

<Example – Please revise as is appropriate>

THIS DOCUMENT CONTAINS [ORGANIZATION NAME HERE] AND OTHER THIRD PARTY (TPI) CONFIDENTIAL (CONF) INFORMATION PROTECTED UNDER THE ALBERTA FREEDOM OF INFORMATION PROTECTION OF PRIVACY (FOIP) ACT.

PRIVATE AND PERSONAL (PERS) INFORMATION CONTAINED WITHIN THIS PLAN WAS COLLECTED FOR THE SOLE PURPOSE OF INFORMATION TECHNOLOGY DISASTER RECOVERY IN THE EVENT OF A DISRUPTION AND MAY NOT BE RELEASED OR USED FOR ANY OTHER PURPOSE. PERSONAL INFORMATION IS PROTECTED UNDER THE ALBERTA FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT.

UNLESS INDICATED OTHERWISE, ALL PAGES OF THIS DOCUMENT CONTAIN CONFIDENTIAL INFORMATION AND ARE TO BE TREATED ACCORDINGLY.

DISTRIBUTION, USE OR RELEASE OF THIS DOCUMENT OR THE INFORMATION CONTAINED HEREIN MUST BE APPROVED BY [ORANIZATION NAME HERE].

VERSION CONTROL TABLE

At a minimum, include the following information in the Version Control table:

1. Document version identifier
2. Reasons for the change (i.e. update contact information)
3. Who made the change
4. When the change was made

<Example> Any and all changes to this document can only be made by one of the following:

1. An authorized member of the [ORGANIZATION NAME] Communications Branch
2. IT Disaster Recovery Manager (or designate)
3. [ORGANIZATION NAME] Business Continuity Manager

Version Number	Reasons for change	Changed by	Date
1.1	Yearly updates to Document. Removed BlackBerry Reference, Updated Video Conferencing information.	IT DR Team	2021-04-12
1.2	Yearly update to document	ITDR Team	2023-05-15

COMMUNICATION POLICIES

Reference any Communications Policies here and where they can be found. It can be contained within the Appendices or referenced through a URL. The policy should come from the designated Communications Officer.

CRISIS COMMUNICATIONS

Crisis Communications Team

Typically includes Executive and Senior Management. This team will determine when and to whom information should be divulged.

Activity 1 – Crisis Communications Team

1. Create a template in which to identify crisis communications team members, their roles and contact information. Collaborate with the Communications Officer as they may have a good idea as to who should be on this team and what their roles should be (and should not be).
2. Include as much contact information as you think team members are willing to provide i.e. home address, alternate email, alternate cell numbers, etc. *Make clear that the alternate contact information being asked for is voluntary and will not be used for any other purpose except for Business Continuity or IT Disaster Recovery purposes.
3. A brief description of responsibilities should be included e.g. a quick reference RACI type matrix. Be clear about who will have the authority to do specific tasks such as activating the Crisis Communications team, speaking to media, speaking to staff, etc. Make sure that teams are aware of their responsibilities.

Example Crisis Communications Team

<Example>	Spokesperson	Deputy Minister / ADM	Executive Director(s)	Comms Director / Officer	BCO	IT DR Manager	Directors, Managers	Communications
Crisis Activate IT DR Communications Plan		✔	✔			✔		
Inform stakeholders	✔							✔
Inform Management Teams		✔	✔		✔			
Inform staff		✔	✔	✔				
Craft Key Messages				✔				✔
Assess Risk to Reputation		✔	✔	✔				
Test Crisis Comms Plan					✔	✔	✔	
Inform Public	✔	✔						✔

4. The Crisis Communications Team will also monitor media releases during the event to gauge whether messages are accurately portrayed and to get an idea of public response to the situation.

Note: Tips for speaking to the media and writing media releases are usually going to be out of scope for the IT Disaster Recovery Crisis Communications Plan. The Communications Branch are responsible for media relations but they may ask for assistance in crafting key messages or when a subject matter expertise is required to respond to technical questions.

Activity 2 – Identify the Spokesperson(s)

Consult with the Communications Director. This will likely have been predetermined. Include the Spokesperson's contact information and specific responsibilities in the Crisis Communications Plan.

<Example> When employees are approached by the media, they should redirect them to one of the identified spokespersons, who have been identified as <Jane Doe>, <John Doe>. Note: For major events, the Minister may act as the media spokesperson. However, there are situations where executives, senior managers, etc, may be designated to speak on behalf of the organization or as a Subject Matter Expert.

Activation Process

Activity 3 – Activation Process

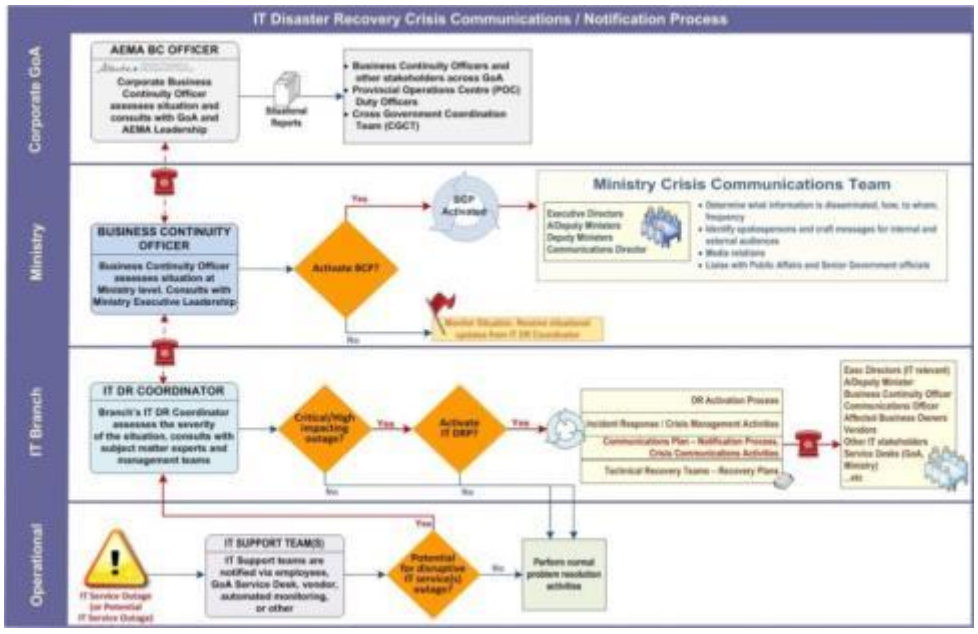
Create a process that describes under what conditions a Crisis Communications Plan is to be activated. It should contain what the process is and who is authorized to activate the plan.

Notification Process

Activity 4 – Notification Process

1. Document how Executive and Management teams, recovery teams, staff, vendors, stakeholders, etc, will be notified.
2. Affected employees will need to receive updates and instructions – describe how they will be reached and frequency. Include contact details and methods for communicating (cell, text, website, etc.). This process should identify those to be notified and their contact information. This process should be reviewed by the Business Continuity Officer and the Communications Officer. Ensure a contingency plan is in place in case certain means of communication are not available during the crisis e.g. email.
3. Develop a list of external parties that may require information and updates during a crisis. As well, this may include entities that will may be called upon for assistance. The list should include contact information for representatives of partnering agencies, critical infrastructure providers (Epcor, Telus, etc), or vendors that may need to be contacted during a crisis.
4. Obtain notification processes developed by the Business Continuity Officer and/or Crisis Communications Team. This team should have developed a process specific for key audiences such as the public, employees, etc.
5. Include a process diagram, where possible.

<Sample Crisis Communications process flow>



Visio diagram:

Crisis Comms Notification_ITDR.vsd

<Example> When **IT support teams** are notified of an issue, they quickly determine if it will or could result in a disruptive outage. If there is reasonable cause to believe this could be a disruptive event, the **IT Disaster Recovery (DR) Manager** is contacted.

The **IT DR Manager** will consult with subject matter experts and the management team from the affected areas to determine impact. The IT DR Manager will also consult with the **Business Continuity Officer (BCO)** to assess what impact the outage may have on the affected business(es) and the services it delivers. If the impact is high, a decision will be made by the Deputy Minister whether to activate the IT Disaster Recovery Plan (IT DRP).

If the IT DRP is activated, the Notification Process is initiated as per the Crisis Communications Plan. The Executive Team, ADM(s), Communications Officer/Director, affected Business Owners, vendors, and other stakeholders/clients will be notified.

The BCO will consult with Executives and consult with Business Owners to determine whether or not the Business Continuity Plan(s) associated with the affected services should be activated. If so, the Crisis Communications Team is convened.

This **Crisis Communications Team** consists of the Deputy Minister and other high level Ministry Executives including the Communications Director. This team will liaise with the Executive Teams and other high level Government officials and stakeholders. This team will identify a Spokesperson, craft/approve outgoing messages, and engage in media relations.

The Business Continuity Officer will liaise with other Ministry Business Continuity Officers and with **Alberta Emergency Management Agency (AEMA)**. AEMA will consult with the BCOs and assess the situation. If this is an event that has broad and severe implications, they may convene the Cross Government Coordination Team (CGCT) so that resources can be leveraged for a cross-government response. If the situation is severe, AEMA may activate the Provincial Emergency Centre (PEC). AEMA will provide Situational Reports (Sitreps) to stakeholders, as required.

Relocation Plan

Activity 5 – Alternate Location(s)

1. Identify two alternate locations from which the Crisis Communications team can operate. The Business Continuity Officer should be able to assist with this.
2. Identify alternate site contacts
3. Identify requirements such as the resources required to function
4. Document instructions for accessing the site
5. Considerations: Does the location allow the group to have easy access to the executive management team? What members of the group can work from home? What will they require in order to work from home? The Communications Officer could assist with this.

Situational Reports

Activity 6 - Situational Assessment

1. Make a list of the potential communications risks and identify communications issues that may arise. e.g. Email is unavailable, cell towers are impacted by a natural disaster, etc.
2. Develop contingency plans for each scenario.
3. Create assessment procedures. Determine how ‘on the scene’ information will be provided to the Crisis Communications team and by whom.

Note: Consult with the Business Continuity Officer.

Messaging

Activity 7 – Key Messages

During a crisis, it may be helpful to have pre-canned key messages already developed. Messages should be created for different types and scopes of outages and disasters. This will save time when delivering notifications to Executives, stakeholders, employees, vendors, etc.

1. The Business Continuity Officer and/or Communications Officer will have created templates for fact sheets, question-and-answer sheets, talking points and other supplementary materials for potential scenarios. Obtain a copy for the IT Disaster Recovery Crisis Communications Plan's appendices.
2. Identify recipients of key messages that would come from Information Technology recovery teams.
3. A variety of methods may be used to create these messages, including 'message maps'.

<Example 1> Message Maps apply the 'Rule of 3' Principle – 3 key messages

Situation	A large fire has erupted at the primary data centre site. The data centre has experienced extensive damage.
Stakeholder	Ministers, Deputy Ministers
Spokesperson	Minister of Technology & Innovation
Question or Concern	How does this impact the Public?
Key Message 1:	**Some services delivered by Registry Offices throughout Alberta are unavailable due to a fire at one of Government of Alberta's Data Centres**
Supporting Data	– Impacted services include drivers licenses – new and renewals – Vital statistics – birth certificates, death certificates – Land titles – real estate transactions, property surveys – Etc…
Key Message 2:	**Not all services delivered by the Government of Alberta are unavailable**
Supporting Data	– Availability will vary from Ministry to Ministry. The public can call the GoA Contact Centre at: 780-XXX-XXXX to find out what services have been temporarily suspended and which are still available – Many websites at www.gov.ab.ca are affected; however the main page is still available and will display regular updates about the service outages.
Key Message 3:	**When will affected services be restored?**
Supporting Data	– AEMA has been notified and Business Continuity Plans are being activated. – Work arounds are being implemented for services considered 'critical' or 'vital'. Critical services may be available in as little as 1-4 hours. – The recovery team is still assessing the damage and will have more information in 2 hours.

<Example 2> Primacy/Recency Principle – Key message first and last.

Situation	A large fire has erupted at the primary data centre site. The data centre has experienced extensive damage.
Stakeholder	Ministers, Deputy Ministers
Spokesperson	Minister of Technology & Innovation
Question or Concern	How does this impact the Public?
Key Message, first	**A fire at one of Government of Alberta's Data Centres has resulted in a disruption of some Government services.**
Message	Not all Government of Alberta's services were affected. The public is being asked to visit www.gov.ab.ca to find out what services have been impacted.
Key Message, last	**Business Continuity Plans are being activated. Work arounds are being implemented for services considered 'critical' or 'vital'. Critical services may be available in as little as 1-4 hours.**

4. Create a Communications Tracking Log and include in the Appendices.

   <Example> When issuing communications to large audiences, document who was communicated to, when, by whom, and what was communicated in the log found in the appendices.

5. FYI - The US National Homeland Security Council has compiled the top 77 questions asked by the media during a crisis. They are found in Appendix 5.

Evaluation

Activity 8 – Training and Awareness

1. Ensure Crisis Communications Team members understand their role and responsibilities.
2. Ensure employees know how to provide information to the IT Disaster Recovery teams and how to get information including updates and instructions.

Activity 9 – Test and Exercise

It is extremely important to test the processes and procedures of the Crisis Communications Plan. The plan should be tested on its own, frequently. Testing the Crisis Communications Plan should always be included as part of any larger exercises.

Activity 10 – Continuous Improvement

Perform post incident or post exercise debriefs and implement lessons learned. Contact all affected audiences to get feedback on how the situation was handled. Did your Crisis Communications build or damage trust and credibility?

CONTACTS

<Example>

Business Continuity Team

NAME	POSITION	TELEPHONE	CELL	EMAIL
Name	BC Coordinator - Primary	Office	Cell	…@gov.ab.ca
Name	BC Coordinator - Secondary	Office	Cell	…@gov.ab.ca
Name	BC Coordinator - Tertiary	Office	Cell	…@gov.ab.ca
Name	AEMA	Office	Cell	…@gov.ab.ca

Executive Team

NAME	POSITION	TELEPHONE	CELL	EMAIL
Name	Deputy Minister	Office	Cell	…@gov.ab.ca
Name	ADM	Office	Cell	…@gov.ab.ca
Name	Executive Director	Office	Cell	…@gov.ab.ca
Name	Director	Office	Cell	…@gov.ab.ca

Communications Team

NAME	POSITION	TELEPHONE	CELL	EMAIL
Name	Communications Officer	Office	Cell	…@gov.ab.ca
Name	Communications Director			…@gov.ab.ca
Name	Public Affairs Officer			…@gov.ab.ca
Name	Executive Director			…@gov.ab.ca
Name	A/Deputy Minister			…@gov.ab.ca
Name	Deputy Minister			…@gov.ab.ca

IT Disaster Recovery Operations Team

NAME	POSITION	TELEPHONE	CELL	EMAIL
Name	IT DR Manager	Office	Cell	…@gov.ab.ca
Name	Director, Technical Services	Office	Cell	…@gov.ab.ca
Name	Incident Commander / Lead	Office	Cell	…@gov.ab.ca
Name	Business Continuity Officer	Office	Cell	…@gov.ab.ca
Name	Communications Advisor	Office	Cell	…@gov.ab.ca

Other

NAME	POSITION	TELEPHONE	CELL	EMAIL
Name		Office	Cell	…@gov.ab.ca
Name		Office	Cell	…@gov.ab.ca
Name		Office	Cell	…@gov.ab.ca

APPENDIX 1 – COMMUNICATIONS CONTINGENCIES

Document risks and contingencies

<Example 1>

MOBILE DEVICES - VOICE		
Description	Use of a mobile device (cell phone, smartphone) for verbal communications.	
Preferred Mode For:	– High priority conversations or relaying of messages – Multiple participation - conference call – Communicating instructions internally via mass call out – When discretion is required for conveying sensitive information – Mobile telephony	
DISRUPTIONS AND CONTINGENCIES		**NOTES**
Cellular Network Overload or Failure	Use landline telephone	
	In person briefings	
	Voice over IP (VOIP)	
	Email and flag 'High Priority'	
	Post messages on www.Alberta.ca	
	Social Media or collaboration site e.g. https://twitter.com/Alberta<Ministry Name> http://www.youtube.com/user/ Alberta<Ministry Name> https://www.facebook.com/ Alberta<Ministry Name> Other relevant social media site	*Security Alert – Conversations are not private – Do not convey sensitive information
	MS Teams Conferencing	
	Push to Talk radios - Walkie-talkie/Mike Radios and paging capabilities	*Security Alert – Conversations are not private and can be overheard by other radio operators – Do not convey sensitive information
	Amateur Ham Radio	If the PECC (Provincial Emergency Contact Centre) is operational, they may involve Amateur Radio operators to help in communications efforts. *Security Alert - Conversations are not private and can be overheard by other radio operators – Do not convey sensitive information
	Satellite telephones	
	AFRRCS (Alberta First Responders Radio Communications System)	

<Example 2>

MOBILE DEVICES - EMAIL		
Description	Use of a mobile device (cell phone, smartphone) for email communications.	
Preferred Mode For:	– Mobile email communications and transfer of electronic information – Wi-Fi capabilities in case of failures in the cellular network – Record keeping, message trails – Multiple recipients – Communicating instructions via mass mail out – Statements to media outlets	
DISRUPTIONS AND CONTINGENCIES		**NOTES**
Failure of data network	Fax	
	In person briefings	
	Courier documents/letters	
	Use landline telephone to convey message verbally	cellular network may or may not be available
	Air Card (access from internet) and Social Media or collaboration site	*Security Alert - conversations are not private
	Push to Talk radios - Walkie-talkie/Mike Radios and paging capabilities	Refer to instructions for use provided with the handsets *Security Alert - Conversations are not private and can be overheard by other radio operators – Do not convey sensitive information
	Amateur Ham Radio	If the PECC (Provincial Emergency Contact Centre) is operational, they may involve Amateur Radio operators to help in communications efforts. *Security Alert - Conversations are not private and can be overheard by other radio operators – Do not convey sensitive information
	Satellite telephones	
	AFRRCS (Alberta First Responders Radio Communications System)	

APPENDIX 2 – COMMUNICATION LOG

<Example> This log should reflect the requirements of the Communications Director.

COMMUNICATIONS LOG	
MESSAGE	
DELIVERED BY	
DELIVERED TO	
DELIVERED AT TIME/DATE (HH:MM/DDMMYYY)	

APPENDIX 3 – TOP 77 QUESTIONS ASKED BY MEDIA DURING A CRISIS

The US National Homeland Security Council has compiled the top 77 questions asked by the media during a crisis. They are:

What is your name and title?
What are your job responsibilities?
What are your qualifications?
Can you tell us what happened?
When did it happen?
Where did it happen?
Who was harmed?
How many people were harmed?
Are those that were harmed getting help?
How certain are you about this information?
How are those who were harmed getting help?
Is the situation under control?
How certain are you that the situation is under control?
Is there any immediate danger?
What is being done in response to what happened?
Who is in charge?
What can we expect next?
What are you advising people to do? What can people do to protect themselves and their families – now and in the future – from harm?
How long will it be before the situation returns to normal?
What help has been requested or offered from others?
What responses have you received?
Can you be specific about the types of harm that occurred?
What are the names of those that were harmed?
Can we talk to them?
How much damage occurred?
What other damage may have occurred?
How certain are you about damages?
How much damage do you expect?
What are you doing now?
Who else is involved in the response?
Why did this happen?
What was the cause?
Did you have any forewarning that this might happen?
Why wasn't this prevented from happening?
Could this have been avoided?
How could this have been avoided?
What else can go wrong?

If you are not sure of the cause, what is your best guess?
Who caused this to happen?
Who is to blame?
Do you think those involved handled the situation well enough? What more could/should those who handled the situation have done?
When did your response to this begin?
When were you notified that something had happened?
Did you and other organizations disclose information promptly? Have you and other organizations been transparent?
Who is conducting the investigation? Will the outcome be reported to the public?
What are you going to do after the investigation?
What have you found out so far?
Why was more not done to prevent this from happening?
What is your personal opinion?
What are you telling your own family?
Are all those involved in agreement?
Are people over-reacting?
Which laws are applicable?
Has anyone broken the law?
How certain are you about whether laws have been broken?
Has anyone made mistakes?
How certain are you that mistakes have not been made?
Have you told us everything you know?
What are you not telling us?
What effects will this have on the people involved?
What precautionary measures were taken?
Do you accept responsibility for what happened?
Has this ever happened before?
Can this happen elsewhere?
What is the worst-case scenario?
What lessons were learned?
Were those lessons implemented? Are they being implemented now?
What can be done now to prevent this from happening again? What steps need to be taken to avoid a similar event?
What would you like to say to those who have been harmed and to their families?
Is there any continuing danger?
Are people out of danger? Are people safe? Will there be inconvenience to employees or to the public?
How much will all this cost?
Are you able and willing to pay the costs?
Who else will pay the costs?
When will we find out more?
Have these steps already been taken? If not, why not?
Why should we trust you?
What does this all mean?