Washington, DC

Emergency 800 Number — 888 298 7600

Water Street Suite 700
Rockville, MD 20852
301 123 4568

2018

OFFICE DISASTER RECOVERY PLAN

Washington

I. Introduction 4
- Purpose
- Crisis Management Team
- Scope
- Risk Assessment
- Risk Reduction
- Review/Procedures

II. Emergency Communications 6
- Between Regional and Field Offices
- Between Field and Regional Office
- Between Regional Office and Clients/Joint Venture Partners, Etc.
- Between Regional Office and Employees
- Crisis Management Team

III. Washington Office Evacuation 12
- Procedure for Evacuation
- Assembly Area

IV. Security 13
- Regional Office — Washington
- Field Office

V. Employee Action Plan 13
- Regional Office — Washington
- Field Offices

VI. Medical Emergencies 14
- Regional Office — Washington
- Field Offices

VII. ICT Recovery Procedures 15
- Local Server Data
- Remote Access to Corporation Network (Applications and Data) Email
- Telephone System and Voicemail
- Voice Service
- Special Desktop Applications
- Print, Scan, Fax
- End User Support
- Special Needs
- Contacts

VIII. Crisis Management Team 17
- Corporation Corporate Crisis Management Team
- Corporation Washington Crisis Management Team

IX. Media Interviews/Public Relations 18
Policy
Procedure

X. Appendix 19
Active Shooter Scenario
Corporation Contingency Quick Reference Guide

2018

OFFICE DISASTER RECOVERY PLAN

Washington

Introduction

Purpose

The purpose of the disaster recovery plan is to assure that Corporation is able to resume operations quickly, efficiently and in a controlled and orderly manner in the event of a disaster or serious disruption of operations. This is a 'living document', which will be revised/updated continuously.

Crisis Management Team

Corporation has established a 'Corporate Crisis Management Team' consisting of

Also, Corporation Washington has organized a Washington team consisting of Other individuals will be included as the need for their expertise arises. Should a potential disruption to the business occur, Steve Conley would contact each member of the team. The team will gather as a group within four hours of the first call at the Washington office.

Should the Washington office be inaccessible for the meeting, the meeting will take place at the:

- PRIMARY LOCATION
- SECONDARY LOCATION

This meeting location will change as project conditions dictate.

Scope

A disaster recovery plan established for the Washington office encompasses procedures to follow for a wide range of disruptions. Until a more detailed analysis of risks and consequences of disruption are accomplished the only defensible course is to plan for the worst-case and draw upon those portions of the plan as needed for lesser situations. The plan will encompass procedures, which cover corporate headquarters, regional offices and field offices.

The range of disruptions can vary from vandalism and theft to a loss of power or communications to a medical emergency or to a catastrophic disaster that could close an office indefinitely.

Potential disruptions to the business, which might result in a meeting of this group include, but are not limited to:

- Natural disaster,
- Threat of action, or action, against the company, any of our people, property or projects,
- Medical Emergency,
- Major accident or incident at a project site or the Washington office,
- Vandalism,
- Theft,
- Loss of Power.

Kidnap/Detention — Kidnap or detention for ransom is a possible occurrence in certain regions of the world, which could threaten Corporation may include an employee or employee family member, or a threat is made.

In this situation, ensure the safety of the victim, limit notification of the event/threat to the CMT, and act within the law and in a responsible manner. Please refer to the Corporation Contingency Quick Reference Guide in the Appendix for detailed information.

Damage to Facilities — In the event of damage to facilities (fire, flood, explosion, structural failure, natural disaster, accident, civil disturbance), ensure the safety of Corporation employees, visitors, contractors and the public, act within the law and in a responsible manner, follow official direction from local authorities and emergency services, and resume normal operations as quickly as possible in a safe manner. Please refer to the Active Shooter guide provided by the NYPD Shield Program and the Corporation Contingency Quick Reference Guide in the Appendix for detailed information.

Injury/Illness/Fatality — In the event of an injury, illness or fatality, promptly obtain medical attention/ emergency services, ensure the safety of Corporation employees, visitors, contractors and the public, act within the law and in a responsible manner, report any incidents involving injury, illness or fatalities via the EH&S manager, follow official direction from emergency services, medical professionals and local authorities, and communicate closely with and provide support to the victim's family. Please refer to the Corporation Contingency Quick Reference Guide in the Appendix for detailed information.

Active Shooter — In the event of an active shooter situation, comply with official direction from police, security and emergency services, account for employees (visitors and contractors), promptly obtain medical attention/emergency services and comply with the law. Please refer to the Corporation Contingency Quick Reference Guide in the Appendix for detailed information.

Terrorist Attack — Terrorist groups seldom warn of an impending attack. A particular terror attack may be the first in a wave of coordinated attacks. In the event of a possible terrorist attack, promptly account for all employees (visitors and contractors), closely liaise and cooperate with affected business units/sites. Please refer to the Corporation Contingency Quick Reference Guide in the Appendix for detailed information.

Extortion/Blackmail — In the event of extortion/blackmail, limit information of the event to those people who need to know, act within the law and in a responsible manner, (generally) do not pay extortion money or demands against threats alone, protect the person or asset threatened (as reasonably possible), review response to extortion and restrict knowledge of a threat with the purpose of avoiding general employee and media knowledge. Please refer to the Corporation Contingency Quick Reference Guide in the Appendix for detailed information.

Risk Assessment
Legal Officer and Officer will develop a Risk Matrix to analyze possible legal and financial issues associated with a particular disaster.

Risk Reduction
Risk reduction is accomplished with the development and implementation of routine preventive measures and a comprehensive disaster recovery plan. It is essential that all new employees receive the procedures during initial orientation and all employees receive updated procedures and training twice a year, and all project staff will be trained in project-specific risks at the start of each project and throughout the duration of the project as necessary.

These procedures should be tested twice a year by:

- Conducting drills to mock disasters
- Having employees report to assigned backup sites
- Test backup systems
- Evaluate and adjust the plan as needed

In addition, a Job Startup/Emergency Kit should be assembled which would include:

- Office supplies
- All business forms in use
- Procedures Manuals
- Etc.

Review/Procedure
The designated personnel will conduct bi-annual reviews of the personnel and procedures associated with the responsibilities of the disaster recovery plan to assure that all individuals are aware of any changes and or updates.

Emergency Communications

Between Headquarters and Regional Offices
Contingency Action Plan — Washington, DC Office

- Activate forwarding procedures with local telephone company immediately; forward incoming calls to the Office East project or, if necessary, the High Street project.
- Fax machines to be available at the Office East project contingency location to expedite secondary communications (or the High Street project, if necessary).
- The following personnel are responsible for establishing the initial communications with the regional office in the event of a disaster. The senior vice president of Corporate Affairs will coordinate the content, location and timeliness of these communications.
- The human resource manager will update the corporate client/telephone directory monthly and issue to the contingency locations and the personnel responsible for initial communications.
- The contingency locations available from which the ‘initial’ communication to regional offices are to be accomplished are:
    - Any safe and appropriate location where cellular telephones (if operational) can be used. Proceed to the front of the HighRise Hotel and remain outside where cellular phones may be used if operational.

Office East
c/o
Corporation
8210 Rishmond Avenue
Columbia, MD 20910

- The contingency locations available from which further communications to regional offices are to be accomplished are:
  - Office East
    c/o
    Corporation
    8210 Rishmond Avenue
    Columbia, MD 20910

Between Field and Regional Offices
Contingency Action Plan — Washington Office

- Activate call-forwarding procedures with local telephone company immediately; forward incoming calls to the Office East project.
- The following project personnel are responsible for establishing the 'initial' communications with the respective senior vice president of the regional office in the event of a disaster.
  - Project Executive
  - Project Manager
  - Assistant Project Manager
  - Project Support Staff
- The project support staff will update the project directory and emergency telephone list monthly and issue to the human resource manager.
- The contingency locations available from which the 'initial' communications to regional offices are to be accomplished are:
  - Any safe and appropriate location where cellular telephones (if operational) can be used.
  - Office East
    c/o
    Corporation
    8210 Rishmond Avenue
    Columbia, MD 20910

Between Regional Offices and Clients/Joint Venture Partners, etc.
Contingency Action Plan — Washington Office

The following project personnel are responsible for establishing the 'initial' communications with the respective client and/or joint venture partner in the event of a disaster.

- The project support staff will update the project directory and emergency telephone list monthly and issue to the People & Culture manager.
- The contingency locations available from which the 'initial' communications to clients and joint venture partners are to be accomplished are:
  - Any safe and appropriate location where cellular telephones (if operational) can be used.

- PRIMARY LOCATION
  Office East
  c/o Corporation
  8210 Rishmond Avenue
  Columbia, MD 20910
- SECONDARY LOCATION
  2100 High Street
  Construction Trailer
  Baltimore, MD 21202
- Or a local designated project office.

The contingency locations available from which further communications to clients and joint venture partners are to be accomplished are:

- PRIMARY LOCATION
  Office East
  c/o Corporation
  8210 Rishmond Avenue
  Columbia, MD 20910
- SECONDARY LOCATION
  2100 High Street
  Construction Trailer
  Baltimore, MD 21202
- Or a local designated project office.

Between Regional Offices and Employees
Contingency Action Plan — Washington Office

- In the event of severe weather conditions, president or executive-in-charge will advise direction to the office coordinator who will administer communications throughout the office (if during working hours) and/or on the '800' voice mail system.
- Employees are to call 1 888 298 7600* for information and direction.
- In the event of a disaster that renders the Washington office uninhabitable, the Office East project has been designated the contingency location where the '800' voice mail notification procedures can be implemented.
- The human resource manager will assemble and update the client directory and emergency telephone directory monthly and issue to the contingency location.
- Each regional office to designate an administrator who can:
  - Contact the senior vice president of corporate affairs with the '800' number update information or,
  - If human resource manager is unavailable, learn and carry-out '800' number administrator duties,
  - Immediately activate a call forwarding procedure with local telephone company.
- Set up preprogrammed fax at the designated contingency location.
- Designate portable telephones to the crisis management team for immediate communication capabilities.

Crisis Assessment Team Notification					
Stakeholder	Contact Name	Notified by	Date/Time	Updated at	Comments
Internal					
Team Members					
Communications					
Legal					
Board					
Group					
Regional CEO					
Business Units					
ICT					
EH&S					

External					
Government					
Insurance					
Property Manager					

Crisis Management Team Contacts

All crisis management teams (CMT) are to have a wallet card, which contains the following:

- Contact numbers of CMT members
- Other key contact numbers applicable to the CMT
- International SOS contact details
- Crisis definition and escalation diagram
- Crisis severity matrix relevant to the CMT
- Crisis immediate mandatory tasks list

The following tables should be populated with the contact numbers applicable to the particular CMT.

Crisis Management Team Members		
Name and Title	**Team Role**	**Alternates**
	The Chair	
	Crisis Coordinator	
	Team Member — Crisis Communication	
	Team Member — Legal	
	CMT Administrative Support	
	Team Member	
	Team Member	
	Team Member	

Group/Regional Crisis Coordinators	

Teleconference Details	
Dial in location	**Dial in details**
Office	Local International
Other relevant offices/locations	
Other relevant offices/locations	
Conference code	
Leader pin	

Additional Contacts
Populate the following table with additional key contacts that may be called upon to join the CMT or act as subject experts providing advice to the CMT in their area of specialty. Specialist examples are given below.

Name and Title	Location	Contact Numbers

Washington Office Evacuation

Procedure for Evacuation

In the event of an emergency or major disaster, follow the directions of the Corporation Washington office crisis management team in evacuating the building; proceed to the designated assembly area.

SITE MAP

Assembly Area

Proceed to the parking area behind the building (north end), as shown in the diagram below. A roll call will be taken at that time using our check in sheet from the front desk and maintained by our receptionist who will be responsible for taking that log with her during a drill.

SITE MAP

Security

Regional Offices

Contingency Action Plan — Washington Office

- Suite access is controlled by access card and monitored by Night.
- Building lockup (nightly at 5:00 p.m.) procedures are in place and are managed by the receptionist; the office manager provides backup for these procedures.
- A sign-in/sign-out procedure will be strictly enforced as a means to identify those employees in attendance on any given day. Guests will also be required to sign-in with access to our office controlled by the front desk receptionist.
- , office manager will identify the classification of documents, which are irreplaceable. Existing procedures will be reviewed to determine the most effective means of safeguarding (offsite storage/fire retardant cabinets).
- Office building manager and director of safety will implement monthly inspection program for fire extinguishers to assure proper function.
- Project executives will facilitate their respective project teams in the preparation of formwork inventories that will be at the contingency site.

Field Offices

Contingency Action Plan — Field Offices

Project Executive/Project Manager to:

- Establish sign-in procedures to control guest access.
- Establish lock up responsibilities and procedures.
- Determine classification of documents, which are irreplaceable. Mandate: obtain offsite storage and/or file retardant file cabinets for proper safeguarding.
- Inform building manager of sign-in and lock up procedures to assure consistency with other business operations located in building.
- Obtain security company to secure field offices located in trailer on site.
- Assure proper formwork inventories are located at regional office in case field office is deemed out of service as a result of emergency.

Employee Action Plan

Regional Offices

Contingency Action Plan — Washington Office

- The human resource manager will notify employees of the contingency meeting locations for employees to meet in the case of an emergency (Roll Call).
- The principal-in-charge in conjunction with the People & Culture department will identify and group by home address key personnel such as principals-in-charge, senior vice presidents and department heads. Local emergency temporary office locations, which will be used ONLY if Water Street is not accessible, will be identified in different geographic locations.
    - Local designated project office.
    - Office East
      c/o
      Corporation
      8210 Rishmond Avenue
      Columbia, MD 20910

- Emergency management team will develop ‘worst case’ responsibilities in the event of a disaster.
- will activate contingency plan with local office equipment and supply company to provide supplies in an emergency.
- The office manager will identify appropriate office space (including a working telephone system) so that office operations can continue online.
- Designate personnel to report to the contingency location to immediately implement emergency procedures.
- Employees to call ‘800’ for help for instructions.

Field Offices
Contingency Action Plan — Field Offices
Project Executive/Project Manager:

- Arrange a meeting location for employees to meet in the case of an emergency (Roll Call).
- Implement plan for employees to receive direction in case field office is closed. Information will be provided through main office. Call 1 888.

Medical Emergencies

Regional Offices
Contingency Action Plan — Washington Office

- , director of safety will notify employees that have volunteered to assist with medical emergency.
- will provide periodic health awareness information, first aid and CPR training.
- will implement monthly inspection program for fire extinguishers to assure proper function.
- Human resource manager will post emergency phone numbers throughout office.
- Corporate safety and human resource managers will provide inventory of first aid supplies, flashHigh s, etc.
- Medical Emergency Volunteers

Field Offices
Contingency Action Plan — Field Offices
Project Executive/Project Manager to:

- Be trained in first aid and CPR training,

- Post emergency telephone numbers for rescue squad, police and fire departments,
- Assure first aid supplies, flashHigh s are available in the office and onsite.
- Project sites are to follow the safety guidelines and practices as outlined by the H&S director using company policy and processes.

ICT Recovery Plan

Local Server Data

If a disaster renders the local office server hardware unusable, Corporation is able to successfully restore office data at a different location and re-point its users to this new location at PC login. To access this data, the users would need to attach to the Corporation network through VPN, a land line network connection or Citrix. It is also be important to note that data restoration could occur at any location on our network and the data restored would come from the most recent backup.

Remote Access to Corporation Network (Applications and Data)

Any Corporation employee with a Windows OS-based PC and an Internet link can access the Corporation network and all associated application using …

Email

Corporation email is now stored in the Microsoft Cloud and can be accessed where ever internet connectivity is available. An incident rendering any Corporation office inaccessible would not affect the availability of email. Email can be retrieved from any Corporation personal computer connected to the internet. Email can also be accessed from any internet connect device via portal.Corporation.com or via your Corporation email enabled smart-phone.

Voice Mail

Most offices would lose access to their local phone system including voice mail if a disaster rendered the equipment unusable. The… store all voice mail in Atlanta and would be able to access this voice mail even if their local phone system were destroyed. In cases where access to the building is restricted, but the phone system is still operational, users have remote access to voice mail systems.

Voice Service

In the event of a disaster that renders the local phone system unusable Corporation can redirect incoming calls to a reception area at another location. For offices that do not have a Cisco phone system, the calls would need to be redirected to a physical person who would direct callers to the individuals new contact number whether it be a cell number, home number or a number at another location.

Special Desktop Applications

In the event a PC is destroyed or simply not accessible any local data or local applications on that PC will also become inaccessible. If this data or these applications are critical to business functions, a plan should exist for alternate options in the event of a disaster. (See ‘Special Needs’ section for examples)

Print, Scan, Fax

In such an event that would render the office network inaccessible our employees would lose the ability to

print, scan and fax with the office equipment. In these instances, the users will need to find alternate devices to attach to where needed. When connected through Citrix or VPN our users would have access to any printer on the Corporation network and could work with employees at the chosen location to handle print, scan and faxing needs.

End User Support
The process to request support would not change in the event of a disaster. Users should continue to contact the Service Desk at 866 1200 for any and all ICT-related assistance.

Special Needs
Some special needs that were uncovered are below:

- Check Printing —check printing for accounts payable and payroll can be replicated in our New York City office. The New York office has a printer that has been configured for this purpose. A quick assessment showed that the New York office would require additional check stock to handle the load, but that enough stock could be delivered quickly.
- Local applications used to wire funds to financial institutions — under review.

Contacts
Chief Information Officer, Operations

Infrastructure Management

Crisis Management Team
Corporation Corporate Crisis Management

Media Interviews/Press Relations

In the event of an emergency or major disaster, any and all interaction with the news media must be coordinated and approved by the Corporation general manager or senior vice president of corporate affairs.

Policy

This release of information to the media is the responsibility of the corporate affairs department. Notify the corporate affairs department 24 hours per day, seven days per week of any incident deemed by you, a subcontractor, police officer, bystander, etc. as one, which may potentially attract media attention to an occurrence at one of our sites.

Refer all inquiries from the news media to the corporate affairs department before making any statements. Keep in mind that all statements made to the media are on the record; there is no such thing as a statement made ‘off the record’. This statement extends to photographers, camera people, writers, producers and anyone who may not directly represent the media but may be involved with the production of educational programs, advertisements, promotional material, etc. Ask any individual who shows up at a site without prior knowledge of the corporate affairs department to wait in our site office until notification of the corporate affairs department.

During business hours, contact the corporate affairs department at 123 456 7890. After hours process emergencies through the safety department.

Procedure

Release of Information Requests 9:00 AM — 5:00 PM

Refer all requests by newspaper, radio, television or magazine editors or reporters for interviews or commentary about Corporation, a particular Corporation jobsite, or an incident, which occurred at a jobsite to the corporate affairs department at 123 456 7890 immediately. Please write the reason for the call, the name of the media outlet, the name of the reporter and a phone number where we may get back to them. Provide no additional commentary.

Release of Information Requests 5:00 PM — 9:00 AM Weekends/Holidays

Refer requests for information by the media to the corporate affairs department. If unavailable, contact the safety manager. Report all press inquiries immediately.

Incidents

Report all incidents of the following nature in writing on a jobsite incident report followed by a call to corporate affairs department REGARDLESS of whether there was any prior media involvement or discussions:

- Accidents to building tenants or bystanders associated with the construction site or field staff described, for example, as injury by construction equipment or at a jobsite, falling debris or construction material, explosion, etc., causing injuries to the head, internal injuries, unconsciousness, poisoning, shooting, stabbing, burns or any accident requiring ambulance involvement, hospitalization or resulting death.
- Theft of personal property from tenant apartment, office building, common area, etc.
- Alleged sexual assault or sexual misconduct involving a Corporation employee, subcontractor or any agent of Corporation; also, contact your local People & Culture representative.

Where possible, a representative from the corporate affairs department will be available to come to a jobsite and provide assistance in dealing with any unpleasant incident or media attraction.

Appendix

Active Shooter Scenario

An active shooter is an armed person who has used deadly physical force on other persons and continues to do so while having unrestricted access to additional victims. Active shooter situations are unpredictable and evolve quickly. Active shooters often look for soft targets like malls, churches or schools due to their low security posture and high access to potential victims.

Call 911
Call 911 and give them the following information as calmly as possible:

- Your name
- Location of the incident (provide as many specific details as possible)
- Your exact location
- Number of shooters, the location at which they were last seen and the direction in which they traveled
- Physical description of the shooter (sex, race, clothing, type of weapon)
- Articulate the number and location of victims, and provide a brief description of injuries
- If you have heard explosion in addition to gunshots
- If you observed any suspicious devices (improvised explosive devices), provide a description and the location at which it was seen.

Avoid, Barricade, Confront
Avoid

- Evacuate the building immediately if it can be done in a safe manner.
- Do not carry any personal belongings with you, and avoid elevators and escalators if possible.
- If you are located in a high-rise building and the shooter is below, ascend as many floors as possible. Once a safe area is reached, secure the location and move away from the entranceway to a more secure location. If the shooter is above you, move down and out of the building.
- When evacuating in the stairwell, stay pressed to the wall to allow responding officers room to ascend quickly and safely.

Barricade

- If it is possible to do safely, move to a central and secure area of the building.
- Locate an area with ballistic cover, not just visual concealment. Cover stops/slows bullets, concealment does not. Think big – soda machines, copy machines, etc.
- Block the door with large, heavy objects to make entry as difficult as possible (desks, tables, file cabinets, furniture, books, etc.)
- If the only means available to barricade the door is with body, attempt to say lower than average waist level to avoid any shot fired through the door by the shooter.

Confront
There is no single procedure that can be recommended in this situation. If possible:

- If hiding or fHigh is impossible, remain quiet or ‘play dead’ to avoid detection.
- Last resort options if you come face-to-face with the assailant are twofold
    - Attempt to quickly overpower the individual with the force in the most violent manner possible.
    - If you with other people you should work as a collective group to overcome the shooter.

Remember, the attacker will continue to shoot victims unless he is stopped.
First responder response

- The officers’ primary attention will be focused on your hands. If you meet an officer, keep your hands out, open, above your head, and most important, empty.
- Do not carry any packages or items that could be confused as a weapon or device.
- Do not attempt to run towards or grab onto officers.
- Resist the urge to turn suddenly or make any sudden movements.

- **Understand that the officers' primary mission is to neutralize the shooter. Therefore, even if you are injured, officers may initially pass you by in order to contain the threat. They will return.**
- Once evacuated, be prepared to be detained for further questioning.
- Recognize that depending upon the scene, threat and size of the facility, it may take several hours for the officers to clear the area and find you. Until contact is made, remain calm, quiet and alert.

(Active Shooter scenario provided by the NYPD Shield program.)

KIDNAP/DETENTION

1.1. General

1.1.1. The following are supplementary guidelines for the Crisis Management Team (CMT) to be read in conjunction with the Crisis Management Plan.

1.1.2. Kidnap or detention for ransom is a common occurrence in certain regions of the world. It is a crime that is, in the majority of cases, a commercial transaction rather than a crime of violence or a politically motivated act. Kidnap for ransom events that threaten Corporation may include:

a) Company employee(s) is kidnapped

b) Employee's relative(s) is kidnapped, and/or

c) A threat is made to kidnap

1.2. Corporation expectations

1.2.1. Corporation has the following expectations of the CMT and other employees involved in dealing with a kidnap situation:

a) Ensure the safety of the victim(s), Corporation employees and contractors, and the public

b) Limit notification of the event or threat to the CMT Coordinator and legal, and limit information on a need to know basis

c) Act within the law and in a responsible manner

1.3. Initial actions

1.3.1. Business units should notify the CMT Coordinator immediately upon receiving information about a potential kidnap incident. Refer to standard protocols for contacting the CMT Coordinator's delegate in the event the CMT Coordinator cannot be contacted.

1.3.2. The CMT Coordinator will determine whether to convene the CMT. Given the potential impact of a kidnap event, convening the CMT should be the default response; the CMT can be stood-down if it is not required.

a) Inform:

(i) Group risk and insurance (who will notify insurers) and seek their advice in terms of specialist support

(ii) Specialist advisors, if not already appointed/engaged by insurers

(iii) Subject to specialist advice, police and law enforcement agencies

(iv) Government officials and embassy if kidnap occurs outside the country of nationality of the victim

(v) If the event of threat is in public domain, alert the communications department representative

b) Verify the situation, distinguishing facts from assumptions.

c) Strictly contain information, advise others on a need to know basis only. Consider informing Environment Health and Safety senior executives

d) Seek to achieve a media blackout

e) Do not attempt to resolve this issue 'in-house'; seek specialist advice and follow it carefully

f) Channel any communications with kidnapper through a dedicated "communicator", nominated by Corporation on the advice of the specialist advisor. The communicator should not be a member of the CMT or party to their deliberations; they will be required to communicate messages to the kidnapper without engaging in negotiations.

1.4. Key issues to consider

a) Wellbeing of victim

b) Wellbeing of family and friends of the victim(s)

c) Senior management and employee perceptions

d) Actual or potential media response

e) Public opinion when/if the story eventually breaks

1.5. Subsequent actions

a) Assess potential impact on health and well-being of victim

b) Nominate single point of contact for victim's family

c) Provide support as required to family

d) Ensure family informs nominated point of contact immediately if kidnappers or media contact them

e) Advise family not to engage with media or attempt to negotiate with kidnappers

f) Engage communications department representative to develop internal and external communications strategy

g) Draft a press release for use should story break

h) Activate relevant contingency plans (business continuity, communications plan)

i) Ensure appropriate counselling and post-incident trauma care for victim and family, other affected employees

1.6. Possible risks

a) Life of the kidnap victim(s)

b) Disruption of business operations

c) Family member goes public and criticises the company

d) Employee morale

e) Future target/copycat (particularly if there is media attention and suspicions of ransom being paid)

f) Uncontrolled media coverage causing kidnapper to act rashly

1.7. Critical success factors

a) If appropriate, external agencies such as law enforcement, emergency services, embassies, high commissions, etc., were informed and involved

b) Prompt engagement of specialist advisor

c) Safe and timely release of victim

d) No media coverage

e) Close liaison with family through single point of contact

f) Support provided to victim and family

g) Switchboard operators trained to deal with threats

h) Subsequent implementation of lessons learned

DAMAGE TO FACILITIES

2.1. General

2.1.1. The following are supplementary guidelines for the Crisis Management Team (CMT) to be read in conjunction with the Crisis Management Plan.

2.1.2. Damage to facilities could be caused by:

a) Fire

b) Flood

c) Explosion, e.g. gas main, LPG tank, petrol tank

d) Structural failure, e.g. building collapse or imminent collapse

e) Natural disaster, e.g. earthquake, storm

f) Accident, e.g. vehicle or industrial accident

g) Protest or civil disturbance

2.1.3. In the event of damage to facilities, refer to the following supplementary guidelines, if relevant:

a) Natural disaster

b) Injury/illness/fatality

2.2. Corporation expectations

2.2.1. Corporation has the following expectations of the CMT and other employees involved in dealing with a situation in which facilities have been significantly damaged:

a) Ensure the safety of Corporation employees, visitors, contractors and the public

b) Act within the law and in a responsible manner

c) Follow official direction from local authorities and emergency services

d) Resume normal operations as quickly as possible in a safe manner

2.2.2. Damage to facilities may require the establishment of alternative operating facilities. At the very least, an event will require a survey of the site(s) affected and consideration of the risk posed to employees, business operations and business continuity. If the damage restricts access for a protracted period, employees may be required to work remotely while alternative premises are found.

2.3. Initial actions

2.3.1. Affected business units will be expected to inform police and emergency services if there is immediate need, then notify CMT Coordinator of the event.

2.3.2. Following notification, the CMT Coordinator will determine whether to convene the CMT.

a) Direct relevant business units to confirm they have notified:

(i) Police and appropriate authorities

(ii) Emergency services

(iii) Site security

b) Verify the situation, distinguishing facts from assumptions.

2.4. Key issues to consider

a) Health and safety of employees, visitors and contractors on site

b) Safety of permanent and temporary structures

c) Internal communications

d) Employee/union perceptions of Corporation response and original incident

e) Wellbeing of family and friends of any affected employees

f) Media response

2.5. Subsequent actions

a) Assess potential impact on facilities, considering potential period of disruption against maximum allowable outage

b) Activate relevant contingency plans (business continuity, disaster recovery, communications plan)

c) Develop communications strategy including holding statements for various contingencies

d) Prepare an appropriate press release/s

e) Advise staff and suppliers plus other affected stakeholders

f) Notify Corporation insurance function so insurers can be notified

g) Use bulk notification tool (MIR3) to:

(i) Direct employees to notify business unit of their location and well-being

(ii) Inform employees of any alternate working arrangements

2.6. Possible risks

a) Safety of employees, contractors and the public

b) Employee/union perceptions

c) Public opinion

d) Unfavourable media response

e) Disruption to operations

f) Damage to business reputation

2.7. Critical success factors

a) Employees, visitors, contractors and public are safe

b) Adherence to contingency plans, including business continuity and communications plans

c) External agencies informed and involved, and official directions followed

d) Measures to contain damage were implemented

e) Full operations were recovered as soon as possible

f) Subsequent implementation of lessons learned

NATURAL DISASTER

3.1. General

3.1.1. The following are supplementary guidelines for the Crisis Management Team (CMT) to be read in conjunction with the Crisis Management Plan.

3.1.2. In the event of a natural disaster, refer to the following supplementary guidelines, if relevant:

a) Damage to facilities

b) Injury/illness/fatality

3.2. Corporation expectations

3.2.1. Corporation has the following expectations of the CMT and other employees involved in dealing with a natural disaster that has significantly affected Corporation operations or has the potential to do so:

a) Ensure the safety of Corporation employees, visitors, contractors and the public

b) Act within the law and in a responsible manner

c) Follow official direction from local authorities

d) Closely monitor media to understand emerging situation

3.2.2. Loss or restriction of access to facilities may require the establishment of alternative operating facilities. In the first instance, these will be established virtually using remote access and conference calls. If the disaster persists for a protracted period, employees may be required to work remotely while alternative premises are found.

3.3. Initial actions

3.3.1. Affected business units will be expected to inform police and emergency services if there is immediate need, then notify CMT Coordinator of the event.

3.3.2. Following notification, the CMT Coordinator will determine whether to convene the CMT.

a) The CMT should direct the affected business units to confirm they have contacted:

(i) Police and appropriate authorities

(ii) Emergency services

(iii) Site security

b) Use Travel Tracker to identify employees travelling to or from the affected area and notify them

c) Use bulk notification tool (MIR3) to:

(i) Instruct employees in affected area to notify relevant business unit of their location and wellbeing

(ii) Instruct employees off-site to go to closest safe haven and follow official direction from local authorities and emergency services

d) Direct business units to:

(i) Account for all personnel including employees, visitors and contractors

(ii) If required, follow evacuation procedures for the building/site

(iii) Establish if there have been any injuries or fatalities

3.4. Key issues to consider

a) Safety of all employees, visitors, contractors and the public, both on site and elsewhere

b) Accounting for all staff

c) Business continuity

3.5. Subsequent actions

a) Assess impact of the natural disaster on Corporation operations and potential period of disruption against maximum allowable outage, considering:

(i) Damage to infrastructure, plant, equipment

(ii) Accessibility of affected site

b) Disconnect utilities as required in consultation with affected building and facilities management

c) Activate relevant contingency plans (business continuity, disaster recovery, communications plan)

d) Appoint a liaison officer as a single point of contact between emergency services/local authorities and Corporation business unit

e) Develop communications strategy for key stakeholders

3.6. Critical success factors

a) Employees, visitors, contractors and public are safe

b) Adherence to contingency plans, including business continuity and communications plans

c) External agencies informed and involved; official directions followed

d) Measures to contain damage were implemented

e) Full operations were recovered as soon as possible

f) Subsequent implementation of lessons learned

INJURY/ILLNESS/FATALITY

4.1. General

4.1.1. The following are supplementary guidelines for the Crisis Management Team (CMT) to be read in conjunction with the Crisis Management Plan.

4.1.2. Whenever an employee, visitor or contractor falls seriously ill, or is injured or killed at work, the incident must be immediately reported to the relevant health, safety and environment manager, investigated and corrective actions taken.

4.2. Corporation expectations

4.2.1. Corporation has the following expectations of the CMT and other employees involved in dealing with injury/serious illness/fatality:

a) Prompt action to obtain necessary medical attention and/or emergency services response

b) Ensure the safety of all Corporation employees, visitors, contractors and the public

c) Act within the law and in a responsible manner

d) Report any incidents involving injury, illness or fatalities (or near-misses) via the health, safety and environment manager to the relevant regulators

e) Follow official direction from emergency services, medical professionals and local authorities

f) Communicate closely with victim's family and provide support

4.3. Initial actions

4.3.1. Affected business unit(s) will be expected to inform emergency and medical services if there is immediate need, then notify CMT Coordinator of the event.

4.3.2. Following notification, the CMT Coordinator will determine whether to convene the CMT.

a) Direct the affected business units to confirm they have contacted:

(i) Police and appropriate authorities

(ii) Emergency and medical services

(iii) Site security

(iv) Local regulators to fulfil legal notification requirements

b) Direct business unit to preserve the site on which any accident or near-miss has taken place (for investigative purposes)

c) Instruct People & Culture or other appropriate business unit representative to contact family/next of kin.

4.4. Key issues to consider

a) Safety of all employees, visitors, contractors and the public

b) Corporation's reputational integrity

c) Potential litigation

4.5. Subsequent actions

a) Assess impact of injury/illness/fatality on relevant business operations, considering:

   (i) Necessity of closing site for investigation by police or regulator

   (ii) Duty of care to prevent further harm from same or similar cause on affected site or on other sites where same incident could potentially occur

b) Activate relevant contingency plans (pandemic/medical, business continuity, disaster recovery, communications plan)

c) In case of deceased expatriate worker, inform relevant embassy

d) Direct business unit to provide ongoing support to affected worker and family or next of kin

e) Direct business unit, People & Culture and management to formulate return to work plan for affected employee, if appropriate

f) Direct business unit to arrange counselling for employees who have witnessed or are otherwise psychologically affected by a serious incident

4.6. Possible risks

a) Injury or death

b) Long-term incapacitation

c) Employee morale (of those immediately affected and colleagues)

d) Litigation

e) Damage to Corporation's reputation

4.7. Critical success factors

a) Medical/emergency services' assistance obtained without delay (if required)

b) Measures to contain injury/illness were implemented

c) Other employees safe from further harm

d) Families of affected personnel/deceased informed and supported

e) Employee/contractor's rehabilitation supported; employee/contractor resumes work in accordance with a return to work plan

f) Relevant work, health and safety regulator notified and other required measures followed within required timeframes

ACTIVE SHOOTER

5.1. General

5.1.1. The following are supplementary guidelines for the Crisis Management Team (CMT) to be read in conjunction with the Crisis Management Plan.

5.1.2. The following is adapted from Australian government guidance for active shooter incidents in places of mass gathering.

5.2. Corporation expectations

5.2.1. Corporation has the following expectations of the CMT and other employees involved in dealing with an active shooter event:

a) Comply with official direction from police, security and emergency services

b) Account for employees, visitors and contractors

c) Promptly obtain necessary medical attention and/or emergency services response

d) Comply with the law

5.3. Initial actions

5.3.1. Affected business unit(s) will be expected to inform police and emergency services, then notify CMT Coordinator of the event.

5.3.2. Following notification, the CMT Coordinator will immediately convene the CMT.

5.3.3. CMT should direct management of affected business unit or site to:

a) Save and protect life:

(i) Appoint an incident manager to coordinate activities until police arrive

(ii) Use the built environment to restrict or deny access

(iii) Commence CCTV surveillance and track the offender(s)

(iv) Communicate appropriate cover and concealment options to those present

(v) Identify and establish a safe medical triage/first aid location

(vi) Restrict further vehicle access to the site (bollards, gates, road closures, etc.)

(vii) Restrict physical access to the site or general vicinity

b) Facilitate the evacuation of those at risk:

(i) Use bulk messaging tool (MIR3) to notify key staff of the incident using prearranged messages

(ii) Appoint an evacuation manager and ensure they have situational awareness

(iii) Assess the suitability and potential safety of normal evacuation routes

(iv) Provide guidance on safe routes for those that are self-evacuating

(v) Evaluate the safety of standing evacuation muster points and change if necessary

(vi) Identify potential safe places or strongholds for those unable to evacuate

c) Contain the incident or threat:

(i) Consider using electronic or mechanical isolation systems to constrain the movement of the offender or restrict access to potential victims.

(ii) Identify and establish a perimeter

(iii) Use the built environment to best advantage for safety and containment action

d) Support emergency response and investigation activities:

(i) Identify and communicate safe access routes/form up points for emergency services

(ii) Use CCTV and other remote methods where possible

(iii) Commence incident and decision-making logs

(iv) Ensure access to site plans and CCTV footage (where possible)

(v) Clearly identify when incident management has transitioned to the police

(vi) Provide ongoing support to the emergency response action as requested

5.3.4. Via the site emergency response plan, appoint a suitable emergency services liaison officer (separate to the chief warden) to meet/brief the police.

5.3.5. CMT should ensure that relevant business unit has informed police of:

a) Location of the active shooter

b) Number of shooters, if more than one

c) Physical description of shooter(s)

d) Number and type of weapons held by the shooter(s)

e) Number of potential victims at the location

5.3.6. CMT will use the bulk messaging service (MIR3) to warn local employees to avoid affected location

5.4. Key issues to consider

a) Safety and protection of life of Corporation staff, visitors, contractors and the public

b) Evacuation of those at risk

c) Containing the incident or threat

d) Support of emergency response and investigation

5.5. Subsequent actions

a) Use bulk messaging tool to direct employees to account for their location and wellbeing to relevant business unit

b) Direct affected business units to account for all individuals at a designated assembly point to determine who is missing and potentially injured

c) Direct affected business units to provide regular updates at specified times, in particular on the status of missing persons

d) Appoint People & Culture representative to notify families of individuals affected by the active shooter, including notification of any casualties

e) Direct relevant business unit to assess the psychological state of individuals at the scene, and refer them to healthcare specialists accordingly

5.6. Possible risks

a) Loss of life due to poor evacuation procedures

b) Failure to quickly account for wounded staff

c) Reputational damage due to mismanagement of situation

d) Failure to inform staff of ongoing situation resulting in avoidable exposure

5.7. Critical success factors

a) Immediate reporting to and close cooperation with police

b) Accounting for employees

c) Support provided to affected employees and families

d) Safe and orderly evacuation

SINGLE LARGE OR MULTIPLE TERRORIST ATTACKS IN ONE REGION/GEOGRAPHY

6.1. General

6.1.1. The following are supplementary guidelines for the Crisis Management Team (CMT) to be read in conjunction with the Crisis Management Plan.

6.1.2. The guidelines apply to coordinated terrorist attacks across a particular region, country or city in which one or more Corporation business units or sites are located.

6.1.3. CMT should also refer to the following quick reference guides if relevant:

a) Damage to facilities

b) Injury/illness/fatality

c) Active shooter

6.1.4. Terrorist groups will very seldom warn of an attack. A particular terror attack may be the first in a wave of coordinated attacks. The first news of attacks usually breaks via social media.

6.2. Corporation expectations

6.2.1. Corporation has the following expectations of the CMT and other employees involved in dealing with a terrorist attack:

a) Promptly account for staff, contractors and visitors

b) Closely liaise and cooperate with affected business units/sites

c) Follow advice from local police and security services, particularly with regard to evacuation of buildings/areas or advice to remain indoors

d) Closely monitor media and social media to track emerging situation

6.3. Initial actions

6.3.1. Affected business unit(s) will be expected to inform police and emergency services, and then notify CMT Coordinator of the event. This should occur only once it is safe to do so for the individual making contact.

6.3.2. Following notification, the CMT Coordinator will immediately convene the CMT if any Corporation operations or staff are harmed or directly affected (or likely to be directly affected) by the attacks.

a) Confirm the following have been informed of the event(s):

(i) Police and appropriate authorities

(ii) Emergency services

(iii) Site security

b) Use bulk messaging tool (MIR3 and PA) to inform all employees in affected areas to:

   (i) Stand fast in a safe location and minimise movement unless specifically directed otherwise by security authorities

   (ii) Avoid the affected areas

   (iii) Account for their whereabouts and wellbeing

c) Liaise with affected business units/sites to account for all personnel including employees, visitors and contractors

d) Direct affected business units to provide regular updates at specified times, in particular on the status of missing persons

e) Determine whether staff in affected areas should be sent home or remain at work, following official directions of police/security forces

f) If a Corporation office is in close proximity to an attack, direct staff (via appropriate communications including MIR3, PA) to stay away from windows

g) Use Travel Tracker to identify employees travelling to or from affected areas and notify them

6.4. Key issues to consider

a) Employee, contractor, visitor, public health and safety in the affected location(s)

b) Support to families of any affected employees

c) Internal communications to inform staff in other locations of what Corporation is doing to help affected staff

d) Consistent messaging to media and relevant external stakeholders, if required

e) Assess the risk to other sites and increase protective measures to meet additional risk if appropriate.

6.5. Subsequent actions

a) Assess risk to employees due to travel to affected countries, suspend travel if appropriate

b) Assess potential impact on facilities, considering potential period of disruption against maximum allowable outage

c) Activate relevant contingency plans (business continuity, disaster recovery, communications plan)

d) Develop and send internal communications to inform staff in other locations on what Corporation is doing to protect and assist affected staff

e) Prepare media holding statement

f) Provide appropriate counselling and post-incident trauma care for affected employees, contractors and families

6.6. Possible risks

a) Safety of employees, visitors and contractors

b) Failure of business continuity processes leading to avoidable delay in resumption of operations

c) Damage to Corporation's reputation due to failure to respond appropriately

d) Damage to employee morale as result of failure to respond appropriately or failure to communicate steps taken to help affected employees, contractors and families

6.7. Critical success factors

a) Accounted for employees, visitors and contractors

b) Close and regular communication between CMT and affected business units/sites

c) Official directions followed

d) Measures to remove personnel from harm were implemented

e) Measures to contain serious injury/death were implemented

EXTORTION/BLACKMAIL

7.1. General

7.1.1. The following are supplementary guidelines for the Crisis Management Team (CMT) to be read in conjunction with the Crisis Management Plan.

7.1.2. Extortion is a demand by an individual or group of people against a threat to carry out a criminal act that could harm an individual(s), equipment or operations, or otherwise damage Corporation's reputation. Most commonly, the threat will involve inflicting commercial harm on Corporation and/or its clients.

7.1.3. In all cases, physical safety is paramount and the CMT should instruct all employees involved with dealing with the incident accordingly.

7.2. Corporation expectations

7.2.1. Corporation has the following expectations of the CMT and other employees involved in dealing with an extortion or blackmail attempt:

a) Limit information of the event or threat to only those people who need to know

b) Act within the law and in a responsible manner

c) Generally, do not pay extortion money or demands against threats alone

d) Protect the person or asset threatened as much as reasonably possible

e) Review response to extortion very carefully following a detailed threat assessment

f) Restrict knowledge of a threat with the purpose of avoiding general employee and media knowledge. Respond robustly to media enquiries on such occasions ("Corporation is aware of the situation and working with authorities")

7.3. Initial actions

7.3.1. Affected business unit(s) will be expected to promptly inform the CMT Coordinator of the threat.

7.3.2. Following notification, the CMT Coordinator should in the case of a credible or potentially credible threat, immediately convene the CMT.

a) Secure the evidence:

(i) If the threat is contained in a letter, minimise handling and place it in a manila folder. Take a photo or have a transcript made to preserve the evidence. Do not photocopy it.

(ii) If the threat was made by telephone, direct the individual who received the call to write down their recollection without delay. Do not question the individual in detail before they have done this, as this may influence their recollection.

(iii) If the threat was in an email, save it as a file without delay – do not rely on a forwarded version for evidence purposes.

b) Contact:

(i) Police and law enforcement agency

(ii) Australian Government officials and Australian embassy, if extortion occurs overseas

(iii) Group Risk & Insurance team for notification to insurers

c) Verify the situation, distinguishing facts from assumptions

d) Strictly contain information; advise others on a need to know basis only

e) Seek to achieve a media blackout

f) Identify specialist support to supplement the police investigation. This may include a forensic psychiatrist to assess the credibility of the threat

7.4. Key issues to consider

a) Health and safety of employees, visitors and contractors

b) Senior management and employee perceptions

c) Public opinion when/if the story breaks

d) Wellbeing of the victim(s)'s family and friends

e) Actual or potential media response

f) Reputation

g) Any government/political levers, if event occurs off-shore

7.5. Subsequent actions

a) Assess the credibility of the threat and the potential impact on Corporation, its employees, operations and reputation if it were carried out

b) Develop internal and external communications strategy

c) Draft a press release in case the story breaks

d) Activate relevant contingency plans (business continuity, disaster recovery, communications plan)

e) Formulate a plan for communications with extortionist/blackmailer, with advice from specialist and police

f) Ensure appropriate counselling for any employees or contractors and their families who have been the subject of threats or have been exposed to distressing events

7.6. Possible risks

a) Threat is carried out, leading to harm to person/damage to site

b) Disruption of business operations

c) Details are released to the public, making resolution more difficult

d) Damage to reputation

e) Damage to employee morale

7.7. Critical success factors

a) Safety and wellbeing of affected person(s)

b) External agencies were informed and involved

c) Prompt engagement of specialist advisor

d) No media coverage or media coverage limited and controlled should story break

e) Appropriate support provided to victim(s) family

f) Full operations were recovered as soon as possible