Emergency Response & Disaster Recovery

An Executive Runbook Template



EMERGENCY RESPONSE & DISASTER RECOVERY

Executive Runbook

Organization: _____

Document Owner: _____

Version: _____
Effective Date: _____
Last Reviewed: _____
Next Review: _____

Classification: RESTRICTED/CONFIDENTIAL

This document contains personal contact information, insurance information, emergency procedures, and other sensitive organizational information. Copies should be limited to personnel who require access for emergency response purposes.

Assigned To: _____

PURPOSE

This Executive Runbook provides senior leadership with the information necessary to coordinate the organization's response to a significant operational disruption, cybersecurity incident, natural disaster, facility loss, critical technology failure, or other emergency.

This Runbook is intended to remain usable when normal corporate systems, communications, or documentation are unavailable or cannot be trusted.

This document is not intended to replace detailed technical disaster recovery, incident response, business continuity, or system recovery procedures. It identifies the people, authorities, external resources, communications channels, and high-level actions required to initiate and coordinate those processes.

Quick Start

Identify your Incident Commander

What to do in the first 60 minutes

EMERGENCY QUICK START

If a Significant Incident Is Occurring:

1. Protect life and safety.

If there is an immediate threat to life, health, or physical safety: **Call 911.**

Do not delay emergency services while attempting to contact company leadership.

2. Contact the Incident Commander

Primary Incident Commander

Name: _____

Role: _____

Personal Mobile: _____

Personal Email: _____

Alternate Contact Method: _____

Alternate Incident Commander

Name: _____

Role: _____

Personal Mobile: _____

Personal Email: _____

3. Establish a Trusted Communications Channel

If corporate email, messaging, identity systems, or devices may be compromised, **do not use them to coordinate the incident until you determine they are trustworthy.**

Approved emergency communication method:

Emergency conference number/bridge:

Emergency meeting location:

Alternate meeting location:

---

4. Determine the Nature of the Incident

Check all that apply:

☐ Cybersecurity incident
☐ Ransomware
☐ Suspected data breach
☐ Cloud or technology outage
☐ Critical vendor outage
☐ Telecommunications outage
☐ Fire
☐ Flood/water damage
☐ Severe weather/natural disaster
☐ Facility unavailable
☐ Utility outage
☐ Physical security incident
☐ Workplace safety incident
☐ Critical personnel unavailable
☐ Other: _____

5. Begin an Incident Log

Recorded by the Incident Commander:

- Time incident was discovered
- Who discovered/reported it
- Known systems or facilities affected
- Actions taken
- Individuals contacted
- Significant decisions
- External organizations contacted
- Evidence preserved
- Communications issued

FIRST 60 MINUTES

The Incident Commander should coordinate the following as appropriate.

First 15 Minutes

☐ Address immediate life-safety issues.

☐ Contact the Incident Commander or designated alternate.

☐ Establish a trusted communication method.

☐ Identify the apparent scope and type of incident.

☐ Begin the incident log.

☐ Preserve relevant evidence.

☐ Notify executive leadership.

First 30 Minutes

☐ Assemble the appropriate incident leadership team.

☐ Identify the technical/operational lead.

☐ Contact legal counsel if the event may involve security, privacy, contractual, regulatory, employment, or liability issues.

☐ Contact the cyber insurance carrier if the event is cyber-related and potentially significant.

☐ Determine whether outside incident response or forensic assistance is required.

☐ Determine whether facilities, property insurance, or emergency contractors need to be contacted.

☐ Establish the next executive briefing time.

First 60 Minutes

☐ Establish an initial understanding of business impact.

☐ Identify affected critical systems and business functions.

☐ Determine whether Disaster Recovery or Business Continuity procedures should be activated.

☐ Determine whether customers, employees, partners, regulators, insurers, law enforcement, or other external parties may require notification.

☐ Establish responsibility for internal communications.

☐ Establish responsibility for external communications.

☐ Engage PR/crisis communications resources if appropriate.

☐ Establish an executive decision and approval process.

☐ Establish the schedule for subsequent situation reports.

CRITICAL CAUTIONS

Unless necessary to protect life or prevent immediate additional damage:

DO NOT:

- Destroy, wipe, reimage, or materially alter potentially affected systems before considering evidence requirements.
- Delete suspicious emails, files, logs, or accounts.
- Do not communicate with a suspected attacker without authorization.
- Agree to a ransom demand.
- Make a ransom or extortion payment.
- Make public statements regarding the incident.
- Admit liability to customers, vendors, regulators, media, or other parties.
- Speculate about the cause, scope, or responsible party.
- Notify potentially affected individuals before Legal determines notification requirements.
- Retain major cyber-response vendors without considering cyber insurance requirements.
- Assume corporate email, messaging, VPN, password management, or identity systems are trustworthy during a suspected compromise.

When practical, coordinate significant cyber-response expenditures with the cyber insurance carrier and Legal before retaining outside providers.

Contact Information

Your Lists of Who to Contact

INCIDENT COMMAND & EXECUTIVE SUCCESSION

Incident Command Succession

If the designated Incident Commander cannot be reached, authority passes in the following order.

Order	Name	Role	Personal Mobile	Personal Email
1				
2				
3				
4				
5				

EMERGENCY CONTACT LIST

Supplement corporate contact information with **personal contact information** because corporate systems may be unavailable.

Role	Name	Personal Mobile	Personal Email	Alternate
CEO				
COO				
CFO				
CIO/CTO				
CISO/Security Lead				
General Counsel				
HR Lead				
Comms/PR				
Operations Lead				
Engineering Lead				
Infrastructure/ Cloud Lead				
Facilities				
Other				

DECISION AUTHORITY MATRIX

Document who is authorized to make critical emergency decisions.

Decision	Primary Authority	Alternate	Required Consultation
Declare a disaster			
Activate Incident Response			
Activate Disaster Recovery			
Activate Business Continuity Plan			
Shut down production systems			
Isolate systems/networks			
Engage outside counsel			
Engage forensic/IR firm			
Notify cyber insurer			
Notify property insurer			
Contact law enforcement			
Contact regulators			
Notify affected individuals			
Notify customers/partners			
Issue employee communication			
Issue public/media statement			
Approve emergency expenditure			
Approve system restoration			
Enter ransomware negotiation			
Authorize ransom payment			
Close/reopen facilities			

Emergency Spending Authority

Up to $_____: _____

Up to $_____: _____

Above $_____: _____

CYBERINSURANCE

Insurance Carrier: _____

Policy Number: _____

Policy Period: _____

24×7 Incident/Breach Hotline: _____

Claims Email: _____

Broker: _____

Broker Contact: _____

Broker Mobile: _____

Claims Representative: _____

Claims Representative Mobile: _____

Panel Breach Counsel: _____

Approved Incident Response Firm: _____

Approved Ransomware/Negotiation Firm: _____

Other Approved Providers: _____

Important Policy Requirements

Paste or summarize insurer-specific notification, consent, ransomware, forensic, or other requirements here:

Location of Full Policy:

PROPERTY, BUILDING & BUSINESS INTERRUPTION INSURANCE

Carrier: _____

Policy Number: _____

Claims Hotline: _____

Broker: _____

Broker Mobile: _____

Property Coverage Notes:

Business Interruption Coverage Notes:

LEGAL COUNSEL

Primary Outside Counsel

Firm: _____

Attorney: _____

Office: _____

Mobile: _____

Email: _____

Area of Responsibility: _____

Privacy / Breach Counsel

Firm: _____

Attorney: _____

24×7 Contact: _____

Mobile: _____

Email: _____

Other Specialized Counsel

_____

_____

_____

LAW ENFORCEMENT & GOVERNMENT CONTACTS

Emergency: 911

Local Police - Non-Emergency

Agency: _____

Phone: _____

FBI

Field Office: _____

Cyber Contact: _____

Phone: _____

Email: _____

CISA / Federal Cyber Assistance

Contact Information:_____

State/Local Emergency Management

Agency: _____

Contact: _____

Phone: _____

Other Authorities

_____

_____

_____

PUBLIC RELATIONS & CRISIS COMMUNICATIONS

External PR / Crisis Communications Firm

Company: _____

Primary Contact: _____

24×7/Mobile: _____

Email: _____

Alternate: _____

Authorized Company Spokesperson

Primary: _____

Alternate: _____

Unless otherwise authorized, employees should not communicate with the media independently regarding an active incident.

Communications Approval

Public statements require approval from:

☐ CEO
☐ Legal
☐ Incident Commander
☐ Communications
☐ Other: _____

INCIDENT RESPONSE / FORENSICS

Primary Incident Response Firm: _____

24×7 Hotline: _____

Account/Contract Number: _____

Primary Contact: _____

Mobile: _____

Email: _____

Services available:

☐ Digital forensics
☐ Incident response
☐ Malware analysis
☐ Ransomware response
☐ Threat hunting
☐ Evidence preservation
☐ Recovery assistance
☐ Other: _____

MSP / MSSP / CONTINGENT TECHNOLOGY SUPPORT

Managed Service Provider

Company: _____

24×7 Support: _____

Account Number: _____

Escalation Contact: _____

Mobile: _____

Managed Security Provider

Company: _____

24×7 SOC: _____

Escalation Contact: _____

Mobile: _____

Emergency IT / Cloud Resources

_____

_____

Contingent Staffing

Staffing Firm: _____

Contact: _____

Mobile: _____

Capabilities:

_____

_____

CRITICAL TECHNOLOGY PROVIDERS

Complete this section for systems whose failure could materially affect operations.

Service/System	Provider	Business Owner	Emergency Support	Account ID
Cloud Hosting				
Corporate Identity				
Email/Productivity				
DNS/Domain Registrar				
Source Code				
Primary Database				
Data Warehouse				
CRM				
Finance/ERP				
Payroll				
Banking				
Customer Support				
Endpoint Management				
Security Detection and Response (EDR)				
Backup Provider				
Telecommunications				
Other				

FACILITIES & PHYSICAL EMERGENCY CONTACTS

Primary Facility

Address: _____

Property Manager: _____

24×7 Contact: _____

Landlord: _____

Building Security: _____

Alarm Company: _____

Fire/Sprinkler Provider: _____

Electric Utility: _____

Gas Utility: _____

Water Utility: _____

Internet Provider: _____

Emergency Restoration Company: _____

Water/Fire Remediation: _____

Electrician: _____

HVAC: _____

Locksmith: _____

Alternate Work Location

Business Continuity Quick Guides

How to get operational

BUSINESS CONTINUITY PRIORITIES

Identify the organization's most critical business functions in recovery order.

Priority	Business Function	Owner	Maximum Tolerable Outage	Dependencies
1				
2				
3				
4				
5				
6				

Detailed Business Continuity Plan Location:

_____

_____

CRITICAL SYSTEM RECOVERY PRIORITIES

Insert the approved system recovery sequence below.

Recovery Order	System/Service	Business Owner	RTO	RPO	Technical Runbook
1					
2					
3					
4					
5					
6					
7					
8					

IF CORPORATE IT IS UNAVAILABLE OR COMPROMISED

This procedure applies when normal corporate technology is inaccessible or untrustworthy.

Examples include:

- Corporate email unavailable or compromised
- Identity provider unavailable
- Employee accounts compromised
- Password manager unavailable
- Corporate messaging unavailable
- VPN unavailable
- Endpoint management unavailable
- Administrators locked out
- Corporate laptops potentially compromised

Emergency Communications

Primary out-of-band method:

Secondary method:

Emergency conference/meeting method:

Clean Device Procedure

Insert organization-specific procedures here:

Emergency Identity / Administrative Access

DO NOT place passwords, private keys, MFA recovery codes, or other authentication secrets in this runbook.

Location/procedure for obtaining emergency administrative access:

Offline Documentation Location

CYBER / RANSOMWARE QUICK GUIDE

If ransomware, destructive malware, account takeover, or widespread compromise is suspected:

☐ Contact Incident Commander.

☐ Contact Security/Technology Lead.

☐ Establish out-of-band communications.

☐ Preserve evidence.

☐ Isolate affected systems where appropriate.

☐ Protect known-good backups from further compromise.

☐ Contact Legal.

☐ Contact cyber insurance carrier.

☐ Engage approved forensic/IR provider.

☐ Determine whether law enforcement should be contacted.

☐ Determine whether regulated or sensitive information may have been accessed or exfiltrated.

☐ Begin documenting affected systems and business functions.

☐ Establish recovery priorities.

☐ Engage crisis communications if public/customer impact is likely.

Organization-specific procedures:

DATA BREACH / PRIVACY INCIDENT QUICK GUIDE

☐ Preserve evidence.

☐ Contact Security.

☐ Contact Legal/Privacy Counsel.

☐ Determine what information may have been accessed.

☐ Identify potentially affected individuals.

☐ Identify relevant jurisdictions.

☐ Preserve logs and records necessary for investigation.

☐ Determine contractual notification obligations.

☐ Determine regulatory notification obligations.

☐ Coordinate notifications through Legal.

☐ Coordinate external communications through Communications/PR.

Applicable Notification Requirements:

FACILITY LOSS / NATURAL DISASTER QUICK GUIDE

☐ Protect life and safety.

☐ Contact emergency services if necessary.

☐ Account for affected personnel.

☐ Contact property/building management.

☐ Contact property/business interruption insurer.

☐ Determine facility accessibility.

☐ Determine whether remote operations can continue.

☐ Activate alternate workspace arrangements if required.

☐ Protect or recover critical physical assets when safe.

☐ Engage restoration/remediation providers.

☐ Communicate work instructions to employees.

Alternate Operations Procedure

INTERNAL COMMUNICATIONS

Employee Emergency Communication

Primary method: _____

Secondary method: _____

Emergency notification system: _____

Responsible executive: _____

Executive Situation Reports

During a significant incident, executive updates should normally address:

- What happened?
- What do we know?
- What remains unknown?
- What systems/business functions are affected?
- Are customers or employees affected?
- Is sensitive data potentially involved?
- What actions have been taken?
- What outside organizations have been engaged?
- What decisions are currently required?
- What are the next major milestones?
- When is the next update?

Update Frequency During Active Incident:

EXTERNAL COMMUNICATIONS

Consult the designated Communication Lead or PR firm. Communications may be required with:

☐ Customers
☐ Employees
☐ Board of Directors
☐ Investors
☐ Business partners
☐ Vendors

☐ Insurance carriers
☐ Law enforcement
☐ Regulators
☐ Banks/lenders
☐ Media
☐ General public
☐ Other: _____

Preapproved Templates / Location

_____

_____

Status Page

URL/Location: _____

Administrator: _____

Emergency Access Procedure:

_____

_____

BOARD NOTIFICATION

Primary Board Contact: _____

Personal Mobile: _____

Personal Email: _____

Alternate Board Contact: _____

Notification criteria:

_____

_____

_____

BANKING & FINANCIAL EMERGENCY CONTACTS

Primary Bank

Institution: _____

Relationship Manager: _____

Fraud/Emergency Hotline: _____

Account Identifier: _____

Payroll

Provider: _____

Emergency Contact: _____

Payment Processing

Provider: _____

Emergency Contact: _____

Emergency Financial Procedures:

_____

_____

_____

RECOVERY AUTHORIZATION

Technical teams should not assume that restoring a system automatically means it should be returned to production immediately.

Before restoring significantly affected services, consider:

☐ Cause of incident understood sufficiently for recovery.

☐ Threat contained.

☐ Compromised credentials addressed.

☐ Restored systems validated.

☐ Data integrity validated.

☐ Security controls operational.

☐ Required evidence preserved.

☐ Business owner approves service restoration.

☐ Security/Technology approves service restoration.

☐ Legal requirements considered.

☐ Communications/customer support prepared.

Authority to return critical systems to production:

_____

_____

INCIDENT CLOSURE

Before closing a significant incident:

☐ Confirm critical services restored.

☐ Confirm business operations stabilized.

☐ Confirm outstanding security risks documented.

☐ Confirm required notifications completed.

☐ Confirm insurance documentation retained.

☐ Confirm incident records preserved.

☐ Confirm financial losses and expenses documented.

☐ Schedule post-incident review.

☐ Identify corrective actions.

☐ Assign corrective-action owners and deadlines.

☐ Update this Runbook where necessary.

POST-INCIDENT REVIEW

Incident Name: _____

Incident Date: _____

Review Date: _____

Incident Commander: _____

What Happened?

Business Impact

What Worked Well?

What Did Not Work?