

CRISIS COMMUNICATIONS | MAJOR INCIDENT COMMAND | BUSINESS RESILIENCE

Enterprise Communication Resilience & Redundant Operations Plan

What happens when the platform you use to run the incident becomes part of the incident?

I designed this plan for the failure mode most incident processes overlook: the communications platform itself goes down during the event. The plan keeps command, message control, acknowledgment, evidence, and recovery coordination intact by moving the response onto alternate channels in a set order, with every step rehearsed in advance.

ENVIRONMENT

Multi-state retail enterprise with ~280 stores, distribution centers, and design studios supporting 3,000+ corporate users.

MY ROLE

Authored the plan, set the activation rules and channel hierarchy, integrated it into major incident command, and owned the drill and audit cadence, a scope executive leadership added to strengthen accountability.

4

fallback channel tiers in a fixed order

8

activation steps from assessment to evidence

P1

channel outages auto-activate the plan

4

readiness cadences, from monthly to post-event

FIXED ORDER

Every tier has a defined place, purpose, and exit signal, so the next move is never a debate.

ONE VOICE

Severity language and command authority match the primary incident process exactly.

PROOF ON RECORD

Every message, approval, and acknowledgment leaves evidence for reconciliation.

ROUTE THROUGH THIS SAMPLE



STOP 02

Activation and Decision Rights

Channel failure triggers the plan. Severity sets how it activates, and channel condition sets how far down the hierarchy it travels.

P1
AUTOMATIC

Any critical outage that impairs normal channels activates the plan with major incident command.

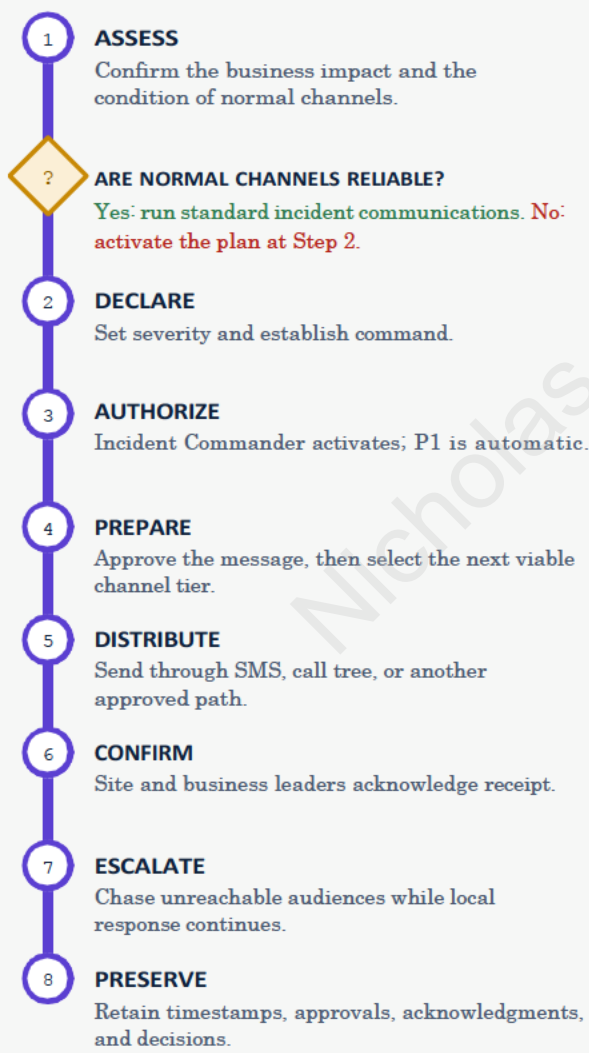
P2
CONDITIONAL

The Incident Commander activates the plan for a multi-site disruption when normal channels are unreliable.

P3 to P5
AS NEEDED

Alternate channels support localized events based on escalation and operational need.

ACTIVATION WORKFLOW



DECISION RIGHTS

Incident Commander

Authorizes activation and owns every decision to change channels.

Communications Lead

Drafts, secures approval for, and sends each fallback message, then tracks acknowledgment.

Contact Steward

Maintains validated escalation and distribution lists on a monthly cycle.

Site and Business Leaders

Confirm receipt, act on instructions, and relay messages to local teams.

Legal and Executive Reviewers

Approve regulatory or externally sensitive messages before release.

If the Incident Commander cannot be reached, a pre-designated deputy assumes full authority, so no decision waits on one person.

STOP 03

Channel Hierarchy and Message Control

When primary platforms fail, the response follows a fixed sequence of alternate channels. Each tier has a defined purpose and a clear signal to move to the next one.

EMAIL, CHAT, ALERTS



PRIMARY DOWN

1

SMS

2

CALL TREE

3

ALT BRIDGE

4

SITE RELAY

TIER 1

SMS Alerts

Broad, concise notice when internet-based channels are impaired.

MOVE ON WHEN

Delivery fails, or acknowledgments stall past 15 minutes.

TIER 2

Voice Call Tree

Direct escalation, command confirmation, and critical instructions.

MOVE ON WHEN

A tree stalls at one level or leaders need a shared working session.

TIER 3

Alternate Bridge

Coordinated recovery on an approved external conferencing service.

MOVE ON WHEN

No conferencing path stays reliable for the affected audience.

TIER 4

Manual Site Relay

Last-mile communication through designated local site leaders.

CLOSES THE LOOP BY

Leaders report back on any working path, and the relay is logged.

MESSAGE STANDARD

- State the known condition and the current business impact.
- State what users or locations must do now.
- State the next update time or the escalation path.
- Keep speculation, unverified root cause, and technical detail out of constrained channels.
- Use the same severity language as the primary incident process.

ACKNOWLEDGMENT AND EVIDENCE

- Every message carries a logged author, approver, channel, audience, and timestamp.
- Receipt confirmations are recorded by site and by leader within 15 minutes.
- Each unreachable audience is escalated to a named owner.
- The fallback log reconciles to the incident record after primary systems return.

STORE NATURAL-EVENT PROCEDURES

The same channel hierarchy includes store procedures for hurricanes, winter storms, and flooding, the events most likely to take normal channels down with them.

BEFORE THE EVENT

Validate store leader contacts and call-tree order, confirm fallback access on mobile devices, secure store technology by checklist, and report closure decisions to command.

REOPENING AFTER THE EVENT

Confirm power, connectivity, and payment systems before opening, report store status through the fallback channel, and assign damaged equipment to a named owner.

STOP 04

Live Message Exhibit

Scenario: Company-wide email and chat outage during peak store hours. Tier 1 and Tier 2 carry the response, and one district escalates to a Tier 4 site relay.

Representative scenario. Times, counts, and wording are illustrative.

TIER 1 MESSAGES TO STORE LEADERS

IT INCIDENT ALERTS

P1 IT ALERT 09:40: Email and chat are down company-wide. Payments and store systems are working. Urgent issues: call the IT hotline. Next update 10:10. Reply 1.

160 characters | approved by Incident Commander

1

Store leader confirmation

P1 UPDATE 10:10: Email is restored. Chat remains down. Store actions are unchanged. Next update 10:40. Reply 1.

111 characters | next update stated

TIER 2 CALL-TREE SCRIPT

OPEN

“This is [name] calling for the IT Incident Commander with a Priority 1 update.”

CONDITION

“Email and chat are down company-wide. Payments and store systems are working.”

ACTION

“Route urgent IT issues to the hotline and keep store operations running as normal.”

NEXT

“The next update arrives at 10:10 by text.”

READ-BACK

“Please repeat the action back to me.”

CASCADE

“Call your next contacts within ten minutes and report anyone you cannot reach.”

MESSAGE ANATOMY

P1 IT ALERT
09:40

Severity and time

Email and chat
are down

Known condition

Payments are
working

Business impact

Call the IT
hotline

Required action

Next update
10:10

Update
commitment

Reply 1

Acknowledgment

ACKNOWLEDGMENT BOARD AT T+20

District 1

Confirmed

District 2

Confirmed

District 3

Confirmed

District 4

Tier 2 call

District 5

Confirmed

District 6

Confirmed

District 7

Confirmed

District 8

Escalated

District 9

Confirmed

District 10

Confirmed

District 11

Confirmed

District 12

Confirmed

Ten districts confirmed within the 15-minute response window. District 4 stalled and received a Tier 2 call; District 8 could not be reached by phone and moved to a named owner for a Tier 4 site relay. Every action carries a timestamp for reconciliation.

STOP 05

Readiness and Validation

A fallback plan earns trust only through rehearsal. Four cadences keep contact data current, people practiced, and gaps owned.

Monthly

Contact validation

Confirm current escalation and distribution information.

Quarterly

Analog fallback drill

Exercise a full transition away from normal digital channels.

Annual

Recovery exercise

Validate communications continuity inside a broader recovery scenario.

After events

Communication audit

Find delivery, acknowledgment, governance, or message-quality gaps.

DRILL SCORECARD

MEASURE	WHAT IT PROVES
First fallback message within 10 minutes of activation	Command continued without interruption.
Correct tier selected for each audience	The hierarchy works as designed under pressure.
Critical audiences confirmed within 15 minutes (T+15)	Messages reached the people who must act.
Local action matched the instruction	Leaders understood what to do.
100% of messages approved and timestamped	Message control held on constrained channels.
Event rebuilt from retained evidence	The record stays defensible after recovery.
Every gap owned and dated within 5 business days	The next drill starts from a stronger position.

OPERATIONAL VALUE

Communications continuity becomes part of recovery engineering. The plan removes ambiguity during channel failure, preserves command discipline, gives every location a clear escalation path, and keeps the incident record defensible after primary systems return. The same design serves a single office with a phone list and a national footprint with hundreds of sites, because it depends on order, ownership, and rehearsal.