SUMMIT
TECH SOLUTIONS

Incident Response Plan

Dual Inclement Weather Disaster

Presented by the ***Business Continuity Team:***

Jasmine Restrepo-Gaitan
Rafael Mejia Galvan
Vannellia Velez
Walter Bozzetti

Dual Disaster Scenario for Summit Tech Solutions

EVENTS

Denver Data Center

Historic winter storm bringing blizzards and extreme cold

Seatle Data Center

Bomb cyclone storm with hurricane-force winds and possibly coastal flooding

THREATS

- Workforce safety issue
- Data center failure for both sites
- Forecasted widespread power outages
- Potential network outages
- Cloud service interruption
- SOC cyber monitoring service disruption
- Potential damage to facilities

Responsible for Recognizing the Incident

Name	Role	Responsibility
Hayden Brooks	Business Continuity Manager / Risk and Compliance Council	Continuously scans for operational risk triggers and environmental events from sources like National Weather Service(NWS), Federal Emergency Management Agency (FEMA).
Michael Tran	Director of Infrastructure Services	Assesses potential impact to Infrastructure Services. Receives automated alerts from monitoring systems on power, bandwidth, and server issues.
Jake Kim	NOC Manager	Monitors infrastructure, weather, and threats 24/7. Typically first to raise alerts. Assesses event impact on network operations and critical services.
Steven Jonhson	Cloud Computing & Storage Manager	Confirms potential multi-location service degradation affecting customer-facing cloud systems.
Nelson Mandel	SOC Manager / Cybersecurity Engineer	Determines the impact of the events on the organization's systems, data, and overall security posture.
Rolando Cruz	Facility Manager	Assesses potential facility damage, accessibility issues, or utility failures.

Communication Steps to Activate The BCP

1) Internal Alert Triggered	2) Initial Assessment Meeting	3) Declare BCP Activation	4) Document with Timestamp	5) Issue Internal Notification	6) Notify Clients & Partners
Hayden Brooks, BCM receives notification from NWS or FEMA. Calls for an initial assessment meeting within 30-60 min.	Convene a meeting with stakeholders and executives to recognize the incident, scope, and assess its impact.	James Holt, CIO (Incident Commander) authorizes formal BCP activation.	All decisions, communications, and actions are recorded in an incident log for audit and post-incident review	Utilize BCP Communication Plan to notify company employees of impeding dual disaster events and threats.	Customer Service & Communications leads initiate alerts to clients and vendor partners to manage SLA expectations.
				Email, Team, Slack, SMS Alert	Email, Website, Customer Portal

Incident Response Team (IRT)

Function	Name	Role	Responsibility
IT	James Holt	Incident Commander/ CIO	Leads the response, makes strategic decisions, allocates resources, coordinates inter-department
Legal	Hayden Brooks	Business Continuity Manager / Risk and Compliance Council	Ensures execution of the continuity plan, tracks impacts, maintains documentation
IT	Michael Tran	Director of Infrastructure Services	Assesses data center and network damage, initiates failover or cloud migration procedures
IT	Nelson Mandel	SOC Manager / Cybersecurity Engineer	Monitors for secondary threats (e.g., cyberattacks during downtime), coordinates cyber incident containment
IT	Steven Jonhson	Cloud Computing & Storage Manager	Leads rerouting to redundant services or regions, activates DRaaS platforms
IT	Jake Kim	Monitoring & NOC Manager	Ensure the continued operation and recovery of the organization's network and critical systems including the NOC team in proactive monitoring, incident response, and restoration efforts.

Incident Response Team (IRT)

Function	Name	Role	Responsibility
Operations	Rolando Cruz	Facility Manager	Coordinates preparation of our hardened facilities, safety of on-site personnel, readiness of disaster-safe workspace: Sleeping accommodations, Food, Water, etc. Communicates with utility/emergency services.
Legal	Stacy Walt	PR & Communication Manager	Issues controlled internal and external updates to executives, staff, clients, partners and media (if needed)
HR	Rose Gillis	HR / Employee Safety Officer	Tracks staff safety and availability, coordinates emergency contact, remote policies
IT	Rita Ortiz	Director of Service Delivery	Coordinates SLA impact communications, escalates critical client support cases

Incident Response Plan

Pre-defined Tasks (24-72 hours before)

72 Hours Before (Early Warning Phase)

Area	Task
Infrastructure	Initiate readiness checks for Seatle and Denver data centers. Pre-stage hardware backups for critical connectivity systems. Verify UPS and generator fuel system redundancy
Maintenance / Physical Security	Inspect weather seals, rooftop access, flood barriers, and raise sensitive equipment off the floor. Verify diesel generators are fueled and tested.
Cloud / Service Continuity	Begin data replication of all active workloads to a warm cloud DR platform
Personnel	Issue weather threat advisory to all staff and confirm emergency contacts.
Documentation	Ensure offline copies of BCP, IRP, and DRP for site teams.

48 Hours Before (Alert Phase)

Area	Task
Personnel / Remote Operations	Prepare mobile work kits (laptops, satellite internet, portable batteries). Distribute instructions and test VPN/MFA access for essential remote staff
Infrastructure	Begin asset protection protocols (raise server racks, seal cable runs). Deliver emergency kits (tools, batteries, snacks, contact lists) to both sites.
Communication	Prep executive comms templates for possible client outages or failovers.
Infrastructure / Communication	Prepare disaster safe work location and war room for activation. Test virtual/physical conference room and verify roles (note-taker, escalation lead, comms host)

24 Hours Before (Pre-Impact Phase)

Area	Task
Personnel	Issue work-from-home policy for non-essential, on-site staff. Verify shelter-in-place or evacuation plans and notify teams.
Infrastructure / Communication	Issue disaster-safe work location directive. War room directive for essential on-site staff. Note-taker establishes live incident log and documents evolving impact in real-time
SOC Continuity	Assign backup SOC operators. Ensure SIEM, firewall, and EDR visibility is maintained.
Personnel / Remote Operations	Confirm all remote users can securely access essential apps with mobile work kits.
Communication	Provide status update to clients and stakeholders

During Event - Personnel & Assets Well-Being

First 24 hours (Impact Phase)

Area	Task
Personnel Safety	Confirm employee safety, activate shelter/evacuation plans, launch HR support hotline.
SOC / Cybersecurity	Maintain SOC monitoring, scan for cyber threats, review SIEM/firewall alerts. Rotate SOC analysts every 8 hours to avoid fatigue
Backup / Data Integrity	Monitor replication jobs, lock down immutable backups, test restore points.
Infrastructure	Run real-time diagnostics on Seattle and Denver data centers. Track generator, UPS, and environmental sensors at both data centers.
Communication	Send internal updates hourly via Teams or secure comms, client alerts every 6–12 hours via status page and client email, log all decisions

48 Hours (Impact Ongoing Phase)

Area	Task
Personnel Support	Support displaced staff, verify secure remote access to collaboration tools and data, continue status checks.
Operational Continuity	Shift non-critical workloads to cloud, prioritize client-facing systems. Monitor queue of client tickets, SLAs, and escalations
Cloud & SaaS Management	Validate CRM/ERP availability, monitor vendor status, escalate as needed. Engage SaaS vendor support if needed for failover assistance
SOC / Cybersecurity	Recheck integrity of security controls EDR/SIEM, verify endpoint security for remote users. Escalate anomalies.
Communications	Provide proactive SLA updates to clients, report any impacts, maintain transparency.

72+ Hours (Impact Subsides Phase)

Area	Task
Personnel & Wellness	Assess staff availability for recovery and re-entry. Prepare HR incident reports for affected employees.
Facilities	Plan safe inspections to assess equipment and power restoration when local authorities clear access.
System & Data Integrity	Run full backup validation jobs, test restores, compare actual vs. target RTO/RPO in BCP. Review error reports.
Incident Review Prep	Begin drafting of preliminary incident report, document actions, prep post-mortem.
Communication	Inform stakeholders of current service status and estimated recovery timelines. Begin planning of formal communication to regulators or auditors if data or SLA commitments were breached

Immediately After the Event (24- 72 hours)

24 Hours After (Initial Recovery Phase)

Area	Task
Personnel	HR conducts emergency wellness checks. Identify unavailable and unreachable staff. Escalate critical absences to leadership for workforce planning.
Maintenance / Physical Security	Physical inspections of data center buildings, assess for damages (roof, flooding, indoor environmental safety)
Infrastructure & Cloud / Service Continuity	Assess what systems are down, who's available, and where workloads are running. • *Example:* VPN/MFA services offline in Seattle/Denver, running on cloud failover
Cloud / Service Continuity	Confirm integrity of systems replicated pre-disaster. Begin restoring critical functions (e.g., CRM, ERP) in DR site.

48 Hours After (Stabilization Phase)

Area	Task
Personnel	Identify teams with reduced headcount. Augment workforce using contractors or reassignments. Update on-call and escalation contacts.
Infrastructure	If safe, re-enter data centers to assess impacted equipment (tech & environmental). Begin incident log and submit first status report to leadership.
Communication	Provide client updates with recovery milestones. Brief internal teams on available services and limitations.
SOC Continuity	Review logs for missed alerts or anomalies during outage period. Ensure no threats occurred during monitoring gaps.

72 Hours After (Post-Incident Transition Phase)

Area	Task
Personnel	Share return-to-office timelines and mobile kit check-in/out instructions. Support impacted staff.
Infrastructure	Conduct environmental testing (cooling, air, electrical). Finalize log of outages, degraded systems, and recovery actions.
SOC Continuity	Verify security tools, logs, and alerting. Ensure monitoring coverage is fully restored.
System Recovery	Restore offline systems. Use hardware backups or cloud failovers as needed.
Communication	Meet with IRT/CMT to review outcomes. Start After-Action Review and document lessons learned.

Adverse Events & Impact Analysis

Seattle Adverse Event and Impact Analysis

Adverse Event	Description	Potential Impact	Severity	Likelihood
Hurricane-force Winds	Wind speeds exceeding 74 mph	Structural damage, personnel unable to access data center	Medium	High
Coastal Flooding	Water inundation due to storm surge and heavy rain	Flooding of lower levels, equipment damage	Medium	Medium
Power Infrastructure Damage	Power lines downed by winds or flooding	Data center power loss, prolonged service interruption	High	High
Communication Disruption	Damage to telecom infrastructure	Delay in response coordination, loss of client communications	Medium	Medium
Water Damage to Equipment	Leakage or flooding affecting servers and critical hardware	Loss of hardware functionality, data corruption	High	Low
Network Outages	Physical disruption to fiber optics or network hubs	Loss of cloud services, reduced operational capabilities	Medium	High

Denver Adverse Event and Impact Analysis

Adverse Event	Description	Potential Impact	Severity	Likelihood
Extreme Cold Temperature	Temperatures significantly below freezing for extended periods	Generator and battery failures, HVAC inefficiencies	High	High
Severe Snowfall	Severe snowstorm causing reduced visibility and mobility	Personnel unable to access data center, delays in repairs	Medium	High
Ice Accumulation on Infrastructure	Ice buildup causing damage to external structures and cabling	Network outages, structural integrity compromise	High	Medium
Frozen Utility Lines	Frozen water and gas pipelines	Disruption to cooling systems, increased fire risk	Medium	Medium
Power Grid Failure	Regional power failures due to storm intensity	Extended reliance on backup systems, potential outages	High	High
Roof Collapse Due to Snow Load	Structural damage from excessive snow accumulation	Severe facility damage, potential harm to equipment	High	Low

IRP Adaptations to Current Conditions

Trigger/Event	Change Made	Justification	Owner / Team
Storm severity escalates	**Activated full BCP** earlier than scheduled – moved from advisory to full response mode; all IR teams on standby	Proactive stance to minimize impact: early activation ensured resources and staff were in place ahead of peak crisis (reducing response time).	BCM Lead & Incident Commander
Staff at risk	**Switched to mostly remote management (95%)** of incident; engaged third-party remote hands for urgent data center tasks	Safety of personnel is paramount. Remote management ensured incident response continues. Leverages BCP's remote work provisions.	IRT Leads & HR
Primary comms outage	**Utilized backup comm channels**: activated emergency notification system, satellite phones, and personal devices for critical comms	Maintained command & control. Redundant channels prevented communication breakdown, which is vital for coordination during crisis.	Communications Lead
Datacenters power failure	**Initiated cloud failover** for critical applications; re-routed traffic to cloud DR environment (already pre-configured)	Sites become unavailable – failover preserved service continuity. Change prevented extended downtime for customer-facing systems.	Infrastructure/DR Team
Generator strain	**Load shedding & resource reallocation**: non-essential systems temporarily shut down; shared workload with Seattle's cloud instance to reduce generator load	Ensured generator could support critical systems longer; prioritized power for essential services. Adaptation prevented total failure at Denver despite fuel limitations.	Data Center Ops Team

Disaster Recovery Plan:
Remote Access

Disaster Recovery Plan

Service Name: Remote Access / VPN Service

System Components Covered

- ❑ **VPN Servers** (Primary and Cloud-Hosted Backup)
- ❑ **Firewall & Network Security Systems** (Cisco Firepower)
- ❑ **MFA Systems** (e.g., Duo, Google Authenticator)
- ❑ **RBAC & Directory Services** (Active Directory/Azure AD)
- ❑ **Endpoint Access Clients** (AnyConnect, custom VPN clients)

Recovery Objectives

RTO (Recovery Time Objective): 2 hours – Resume remote access via backup infrastructure
RPO (Recovery Point Objective): 1 hour – All access policies, roles, and MFA settings restored
MTD (Maximum Tolerable Downtime): 4 hours

Disaster Recovery Plan

1 Assess and Confirm Outage

- ❑ Use monitoring tools (SIEM, NOC dashboards, firewall logs) to validate that **no users** can access via VPN.
- ❑ Confirm whether the issue is a **system failure**, **network configuration issue**, or **external attack (e.g., DDoS)**.
- ❑ Escalate to Michael Tran (**Director of Infrastructure**) to trigger the BCP/DRP.

2 Activate Backup VPN Infrastructure

- ❑ **Switch to cloud-based VPN solution** (AWS, Azure, etc.) already configured with mirrored access rules.
- ❑ Update **DNS settings** or send out backup VPN client instructions.
- ❑ Notify users via alternate channels (email, Slack, SMS) with:
  - New connection instructions
  - Temporary access limitations (if applicable)
  - Security advisories

3 Restore Authentication & Access Controls

- ❑ Reconnect **MFA system** (backup token or SMS-based verification).
- ❑ Sync RBAC permissions from **last good configuration backup** (within RPO limit of 1 hour).
- ❑ Enable access for **critical personnel first**, then full team once authentication systems are confirmed stable.

4 Monitor and Stabilize

- ❑ Actively monitor:
  - VPN load on backup system
  - Login activity (success/failure rates)
  - System logs for service errors or anomalies

Disaster Recovery Plan

5 Document Incident and Begin Root Cause Analysis

- ❑ Start compiling a full **incident log**: timestamps, teams involved, systems impacted.
- ❑ Begin forensic investigation:
  - Why did the primary VPN fail?
  - Were backup systems activated quickly enough?
- ❑ Assign Nelson Mandel (**Cybersecurity Engineer**) to review traffic patterns and provide incident report.

6 Plan Reversion or Reinforcement

- ❑ Once primary VPN is restored:
  - Test for stability and security.
  - Gradually shift users back or keep cloud-based VPN as new primary (depending on findings).
- ❑ Update firewall and endpoint configurations accordingly.

7 Conduct Post-Incident Review

- ❑ Hold internal debriefing within 24–48 hours.
- ❑ Update DRP and BCP documents with lessons learned.
- ❑ Prepare an executive summary for leadership including:
  - Timeline of events
  - Actions taken
  - Downtime duration vs. RTO/RPO goals
  - Recommendations

Restoration and Return to Normal Operations

Restoration Triggers:

Power and network services restored in Seattle and Denver

Critical systems pass health checks (VPN, RMM, backups, CRM)

Stable endpoint connectivity across departments

Steps to Resume Operations

1 **Step 1 – Gradual Transition**

- Migrate users back to the primary VPN infrastructure.
- Confirm stable authentication and access across systems.

2 **Step 2 – Validation of Systems and Data**

- Ensure no data loss occurred; confirm RPO/RTO objectives were met.
- Double-check VPN, MFA, and RBAC configurations.

Restoration and Return to Normal Operations

3 Revoke Temporary Controls

- Remove emergency firewall rules, temporary access credentials, and DNS redirects.
- Reinstate normal security posture.

4 Operational Reinstatement

- Resume day-to-day operations in all departments.
- Ensure internal teams confirm full system functionality.

5 Communication to Stakeholders

- Internal: Notify staff and execs that operations are back online.
- External: Send recovery confirmation to clients, vendors, and partners.

6 Review and Update Plans

- Conduct post-incident review with BCP team and leadership.
- Update BCP and DRP with improvements and new action items.

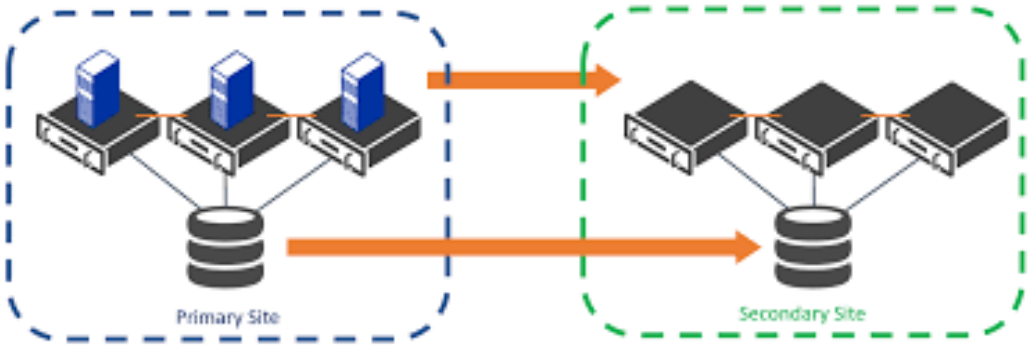
Restoration and Return to Normal Operations

Area	Normalcy Indicator	Readiness Threshold
Power & Infrastructure	• Power fully restored at Seattle and Denver data centers • Environmental controls (cooling, humidity) within safe range	90% Seattle 90% Denver
Networking	• Equipment that supports network infrastructure (Firewall, Routers, Switches, Access Points) has restored successfully	100% (At least one data center)
Backup System Validation	• All RPO targets met • Backup restore tests successful across major systems	100%
Security Monitoring Restored	• SOC back at full coverage (SIEM, EDR, firewall alerts all green) • No anomalies or missed detections in logs during downtime	100%
Remote Access Services	• VPN/MFA stable with normal login success rate • No more failover usage; DNS reverted to primary systems	100%
Critical Systems Operational	• CRM, ERP, email, and collaboration systems tested successfully	90%
Workforce & HR	• Staff accounted for and back online (remote or phased return) • HR wellness checks complete, critical roles reassigned if needed	80%
Client Communications	• Clients notified of service restoration • SLAs back on track with no outstanding critical issues	100%
Return to Office/Site Readiness	• Data centers inspected and cleared for re-entry • Mobile kits returned or checked in	70% (Depending on conditions of building)

INJECT: Key Denver Staff Accessibility to Address Apps Errors

Current issue: Several Key Staff for Denver location are unable to return after the storm. Their homes were impacted and route to the center is dangerous. The NOC is reporting errors on applications supported by these key staff.

Mitigation 1: Fail over to Seattle replicated application servers while errors can be addressed



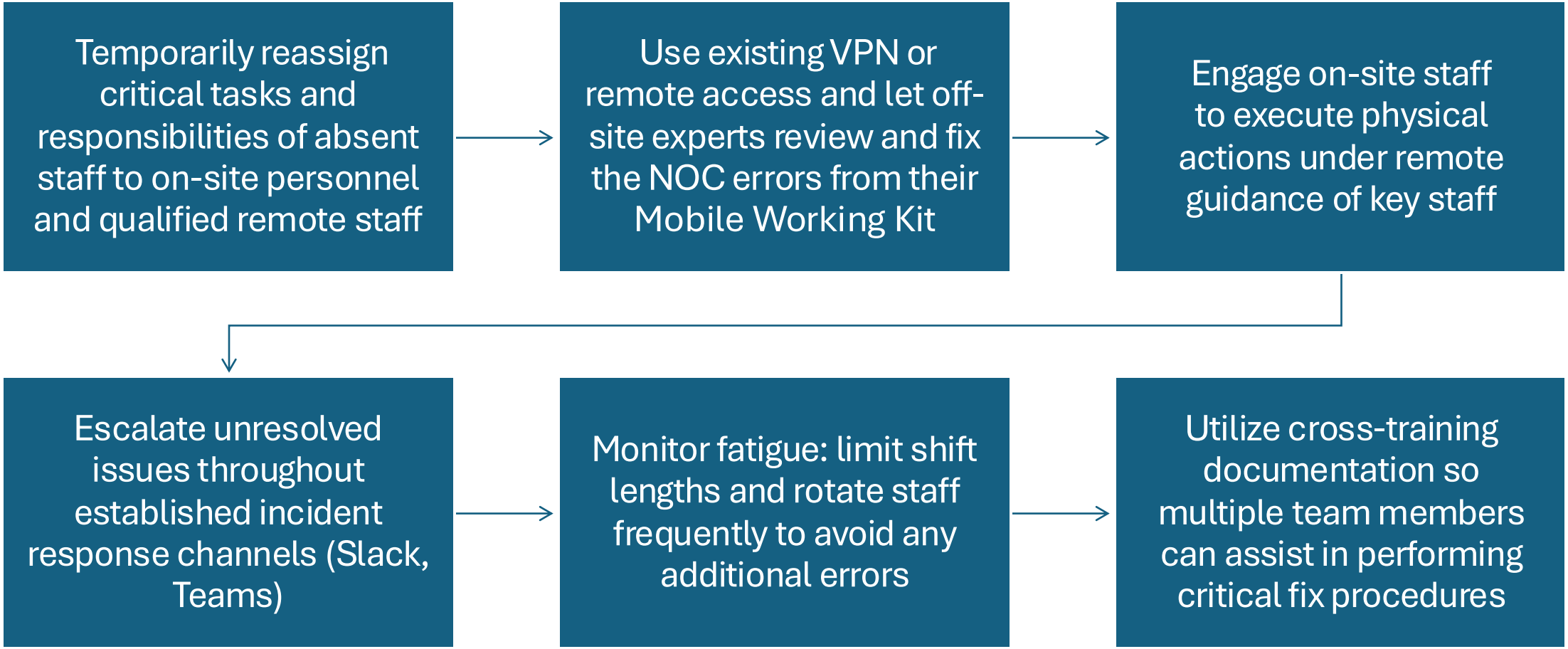
Denver, CO Data Center

Seattle, WA Data Center

Mitigation 2: Key Staff connect from home utilizing Mobile Working Kit

1. ATT Satellite Internet
2. Ecoflow Portable Batteries
3. Laptops

INJECT: Key Denver Staff Accessibility to Address Apps Errors



Lessons Learned – What Went Well

Action / Capability	Outcome	Contributing Factors
Robust Remote Work Infrastructure	Operational continuity maintained, employees safely remained productive remotely, minimal disruption to client services.	• Strong VPN and cloud infrastructure investments • Regular remote-work preparedness drills • Organizational culture supportive of remote working during emergencies
Early BCP Activation & Forecast Monitoring	Staff safety maintained, minimal operational confusion, reduced downtime and damage.	• Real-time weather tracking and early warnings • Proactive leadership decisions • Defined criteria for timely BCP activation
Redundant Power & Network Systems	No data loss, fast recovery of critical systems, minimal downtime for online services.	• Regular testing of backup generators/UPS • Multiple connectivity providers (e.g., secondary ISPs) • Spare hardware strategically located for quick deployment
Cloud DR and Off-Site Backups	Seamless failover to cloud, successfully achieved RTO/RPO goals, minimal service disruption.	• Comprehensive and regularly tested DR plan • Reliable off-site data backups and replication • Pre-configured, scalable cloud infrastructure
Effective Communication Plan	Stakeholders remained informed, preserving client and employee trust, effective crisis management.	• Pre-prepared communication templates and updated contact lists • Multi-channel alerting system (email, SMS, Slack) • Dedicated 24/7 crisis communication team

Lessons Learned – Major Issues and Their Mitigations

Issue	Mitigation/Response	Description and Rationale
Communication gaps	Alternate alerts via multiple channels, direct manager follow-ups using phone trees.	Initial communication missed certain groups; alternate channels quickly re-established comprehensive alerts ensuring critical messages reached all affected parties.
Backup power limits	Prioritized essential systems, coordinated emergency fuel deliveries, collaborated with utilities for prioritized service restoration.	Recognized insufficient generator runtime; promptly managed resources to extend power availability and coordinated external support.
Dual-site workload strain	Prioritized incidents, rotated and cross-trained staff from other departments to maintain operational effectiveness.	Managed overwhelming workloads effectively by strategic reprioritization, rotating personnel, and leveraging internal staffing flexibility to prevent burnout.
Unanticipated DR scenario	Quickly engaged third-party cloud services; transparently communicated longer recovery times.	Unforeseen dual-site disaster required improvisation; used alternate solutions effectively but acknowledged delayed recovery to manage client expectations honestly.
Not enough cross training	Utilizing the documentation on hand some of staff was able to handle the roles of critical staff that was not able to be present	The unforeseen lack of critical staff being able to be on site during an emergency forced us to leverage our documentation.

Lessons Learned – Opportunities for Future Improvements

Issue	Recommendation	Actionable Steps
Communication Resilience	Expand multi-channel and out-of-band communication systems.	• Implement battery-backed SMS broadcast systems • Regularly update and verify contact information • Conduct frequent communication drills
Backup Power Capacity Enhancement	Improve power resilience for longer outages.	• Increase generator fuel storage capacity or duration • Establish priority refueling contracts • Incorporate battery backup systems or renewable energy sources
Incident Team Scalability	Strengthen incident response for concurrent multi-site events.	• Update IR plan to include surge staffing protocols • Arrange cross-regional mutual aid agreements • Regularly conduct tabletop exercises simulating multiple simultaneous disasters
Comprehensive DR Scenario Planning	Plan thoroughly for multiple simultaneous data-center failures.	• Revise DR plan for worst-case, multi-site failures • Implement tertiary cloud failover systems • Expand data replication strategies to cover concurrent regional outages
Extensive Cros-Training	Critical staff should be trained to handle multiple roles in case individuals are unable to show up during an emergency.	• Conduct weekly and monthly trainings • Specific documentation for critical roles • Documented guides for resolving errors that have ever encountered

Application of AI in This Project

AI tools such as ChatGPT (OpenAI) were instrumental in drafting and refining our Incident Response Plan (IRP) for SummitTech Solutions. These tools enabled us to simulate realistic crisis scenarios, assign roles accurately, and outline structured steps across various phases of the incident.

OpenAI – ChatGPT (Prompt Engineering & Document Generation)
🔗 https://platform.openai.com/docs/guides/prompt-engineering
➞ Used for generating structured plans, DRP content, and response scenarios.

🤖 Prompts Used

Use Case	Prompt Example
Role Assignment	“What are the typical responsibilities in an Incident Response Team (IRT)?”
Timeline Structuring	“Create a timeline for incident response before, during, and after a disaster”
Cybersecurity Actions	“What cybersecurity controls should be checked after a major outage?”
Communication Planning	“Draft a communication sequence during a disaster affecting two data centers”
Restoration Strategy	"How do you transition from disaster recovery to normal operations?"

AI References & Sources

🏛️ Frameworks & Standards

- **NIST SP 800-34 Rev. 1** – *Contingency Planning Guide for Federal Information Systems*
  https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final
- **ISO 22301:2019** – *Business Continuity Management Systems*
  https://www.iso.org/standard/75106.html
- **FEMA Continuity Guidance Circular**
  https://www.fema.gov/continuity-guidance-circular
- **CIS Controls v8** – *Cybersecurity Controls for Availability & Resilience*
  https://www.cisecurity.org/controls

🧰 Toolkits & Guides

- **Ready.gov Business Continuity Toolkit**
  https://www.ready.gov/business-continuity-plan
- **SBA Emergency Preparedness Guide**
  https://www.sba.gov/prepare-emergencies
- **Harvard University IT BCP Planning Guide**
  https://huit.harvard.edu/files/huit/files/bcp_planning_guide.pdf

Thank you!