

# Business Continuity Plan

**Document ID:** COM-INT-010 **Effective Date:** January 1, 2024 **Last Updated:** March 2024 **Owner:** Operations & Risk Management **Classification:** Confidential

---

## Purpose

This Business Continuity Plan (BCP) ensures NovaTech can maintain essential business operations during and after a disaster or significant disruption.

---

## Scope

This plan covers: - Critical business functions - Technology systems - Personnel - Facilities - Third-party dependencies

---

## Business Impact Analysis

### Critical Functions

Function	RTO	RPO	Priority
Customer-facing applications	1 hour	15 min	P1
Customer support	4 hours	1 hour	P1
Payment processing	1 hour	0	P1
Internal communication	2 hours	4 hours	P2
Email	4 hours	1 hour	P2
Development environments	24 hours	4 hours	P3
Corporate systems (HR, Finance)	24 hours	24 hours	P3

**RTO:** Recovery Time Objective - Maximum acceptable downtime **RPO:** Recovery Point Objective - Maximum acceptable data loss

## Revenue Impact

Downtime	Estimated Impact
1 hour	\$50,000
4 hours	\$200,000
1 day	\$1,200,000
1 week	\$8,400,000

---

## Disaster Scenarios

### Scenario 1: Data Center Outage

**Description:** Primary cloud region unavailable **Likelihood:** Low **Impact:** High

**Response:** 1. Automatic failover to secondary region 2. DNS update (if manual intervention needed) 3. Communication to customers 4. Monitor secondary region

**Recovery:** 1. Assess primary region status 2. Plan failback 3. Execute during maintenance window 4. Verify data integrity

### Scenario 2: Cyber Attack

**Description:** Ransomware or significant breach **Likelihood:** Medium **Impact:** Critical

**Response:** 1. Activate Incident Response Plan 2. Isolate affected systems 3. Engage security team and legal 4. Assess damage

**Recovery:** 1. Restore from clean backups 2. Rebuild compromised systems 3. Implement additional controls 4. Conduct post-incident review

### Scenario 3: Natural Disaster

**Description:** Earthquake, fire, or flood affecting offices **Likelihood:** Low **Impact:** Medium (remote-first company)

**Response:** 1. Account for all personnel 2. Assess facility damage 3. Communicate alternate work arrangements 4. Redirect mail/deliveries

**Recovery:** 1. Evaluate facility usability 2. Arrange alternate workspace if needed 3. Replace damaged equipment 4. Update insurance claims

#### Scenario 4: Pandemic

**Description:** Widespread illness affecting workforce **Likelihood:** Medium  
**Impact:** Medium

**Response:** 1. Activate remote work for all 2. Communicate health guidelines  
3. Adjust staffing if needed 4. Prioritize critical functions

**Recovery:** 1. Monitor health situation 2. Gradual return to normal operations  
3. Update policies based on learnings

#### Scenario 5: Key Vendor Failure

**Description:** Critical vendor (AWS, etc.) unavailable **Likelihood:** Low **Impact:** High

**Response:** 1. Activate vendor-specific runbook 2. Failover to alternate provider (if applicable) 3. Communication to customers 4. Monitor vendor status

**Recovery:** 1. Assess vendor stability 2. Plan return to primary 3. Review vendor dependency

---

### Recovery Procedures

#### Technology Recovery

**Cloud Infrastructure (AWS Primary) Failover to Secondary Region:**  
1. Verify secondary region health 2. Update Route 53 DNS (automatic for critical services) 3. Scale secondary region resources 4. Verify application functionality 5. Communicate status

**Recovery Time:** < 1 hour for automated failover

**Database Recovery Primary:** AWS RDS Multi-AZ - Automatic failover to standby - Recovery Time: < 2 minutes

**Backup Restore:** 1. Identify target restore point 2. Create new instance from backup 3. Update application connection strings 4. Verify data integrity

**Recovery Time:** 30 minutes - 2 hours depending on database size

## Application Recovery

1. Deploy from latest container images
2. Restore configuration from SecureVault
3. Verify connectivity to dependencies
4. Run smoke tests
5. Gradually restore traffic

## Communication Recovery

**Internal Communication Primary:** Slack **Backup:** Microsoft Teams, Email **Emergency:** Phone tree, SMS

**If Slack unavailable:** 1. Activate Microsoft Teams 2. Email blast with Teams instructions 3. Phone tree for critical personnel

**Customer Communication Channels:** - Status page ([status.novatech.com](https://status.novatech.com))  
- In-app notifications - Email - Twitter (@NovaTechStatus)

**Templates:** Pre-written templates in Confluence

## Personnel Recovery

**Remote Work:** - All employees can work remotely - VPN and collaboration tools accessible - Hardware shipped to home (laptops)

**Key Personnel Backup:** - Cross-trained for critical functions - Documented procedures - Succession plans for leadership

---

## Roles and Responsibilities

### Crisis Management Team

Role	Primary	Backup
Incident Commander	CEO	COO
Operations Lead	VP Engineering	Sr. Director SRE
Communications Lead	VP Marketing	PR Manager
Customer Lead	VP Customer Success	Director Support
Legal/Compliance	General Counsel	Outside Counsel
HR Lead	Chief People Officer	HR Director

## Responsibilities

**Incident Commander:** - Overall decision authority - Resource allocation - External communication approval - Declare/end emergency

**Operations Lead:** - Technical recovery - Coordinate engineering teams - Status updates - Vendor coordination

**Communications Lead:** - Customer communications - Internal communications - Media relations - Status page updates

---

## Communication Plan

### Internal Communication

Audience	Channel	Frequency
Crisis team	Slack + Phone	Continuous
All employees	Slack + Email	Every 2 hours
Board	Email + Call	Daily during crisis

### External Communication

Audience	Channel	Frequency
Affected customers	Email	Immediately + updates
All customers	Status page	Continuous
Media	Press release	As needed
Partners	Email	As needed

## Communication Templates

### Initial Customer Notice:

Subject: NovaTech Service Update

We are currently experiencing [brief description]. Our team is working to resolve this issue.

Current Status: [status]

Estimated Resolution: [time or "investigating"]

We will provide updates every [frequency].

For urgent issues, contact support@novatech.com.

We apologize for any inconvenience.

#### **Resolution Notice:**

Subject: NovaTech Service Restored

The issue affecting [services] has been resolved as of [time].

Root Cause: [brief description]

Duration: [time]

We are conducting a thorough review and will share learnings.

Thank you for your patience.

---

## **Testing and Maintenance**

### **Testing Schedule**

Test Type	Frequency	Scope
Tabletop exercise	Quarterly	Crisis team walkthrough
Failover test	Semi-annual	Cloud region failover
Backup restore	Monthly	Random system restore
Communication test	Quarterly	Contact trees, tools
Full DR test	Annual	Complete recovery simulation

### **Test Documentation**

Each test must document: - Test scenario - Participants - Steps executed - Issues identified - Improvement actions - Time to recovery (actual vs target)

### **Plan Maintenance**

**Review Triggers:** - Annually (minimum) - After any activation - After significant system changes - After test findings - After organizational changes

**Update Process:** 1. Identify changes needed 2. Draft updates 3. Review by stakeholders 4. Approve by leadership 5. Communicate changes 6. Update training

---

## Backup Strategy

### Data Backup

Data Type	Backup Frequency	Retention	Location
Production databases	Continuous (replication)	30 days	Multi-region
Database snapshots	Daily	90 days	Cross-region
Object storage	Real-time replication	365 days	Multi-region
Configuration	On change	Unlimited	Git + SecureVault
Logs	Real-time	90 days	Separate region

### Backup Verification

- Automated backup monitoring
  - Weekly restore tests (random selection)
  - Monthly full restore verification
  - Annual DR restore test
- 

## Vendor Dependencies

### Critical Vendors

Vendor	Service	Backup Plan
AWS	Primary cloud	GCP (warm standby)
Okta	Authentication	Local auth cache, manual access
Stripe	Payments	Backup processor on standby
Datadog	Monitoring	CloudWatch, self-hosted fallback
Slack	Communication	Microsoft Teams

## Vendor Contact

Emergency contacts for all critical vendors maintained in SecureVault:  
`/emergency/vendor-contacts`

---

## Financial Considerations

### Insurance Coverage

- Business interruption insurance
- Cyber liability insurance
- Property insurance

**Contact:** CFO or Finance Director for claims

### Emergency Funds

- Authorized emergency spending: Up to \$100,000 without board approval
  - Credit facilities available for larger needs
- 

## Training

### Required Training

Audience	Training	Frequency
Crisis team	BCP procedures, tabletop	Quarterly
All managers	BCP awareness	Annual
All employees	Emergency procedures	Annual
New hires	BCP overview	Onboarding

---

## Document Control

**Owner:** VP Operations **Review Cycle:** Annual **Distribution:** Crisis team, leadership, stored in Confluence

---

## Appendices

### Appendix A: Contact Lists

Maintained in SecureVault: `/emergency/contact-lists`

### Appendix B: Runbooks

Detailed runbooks in Confluence: Engineering → Runbooks → DR

### Appendix C: Vendor Agreements

SLAs and agreements in Legal repository

### Appendix D: Insurance Policies

Policy documents with Finance team

---

*Related Documents: Incident Response Plan (IT-SEC-010), Disaster Recovery Runbook (ENG-OPS-010), Crisis Communication Plan (COM-INT-015)*