Disaster Recovery Procedures

Document ID: COM-INT-010 **Version:** 2.0 **Effective Date:** January 1, 2024 **Last Reviewed:** March 2024 **Owner:** Engineering & Operations **Classification:** Confidential

Purpose

This document provides detailed procedures for recovering NovaTech's critical systems and data in the event of a disaster or major outage.

Recovery Objectives

By Service Tier

Tier	Services	RTO	RPO
1 - Critical	CloudForge, DevPipeline, SecureVault, DataLens	15 min	1 min
2 - Essential	Customer Portal, Billing, Support Systems	4 hrs	1 hr
3 - Important	Internal Tools, Analytics, Marketing	24 hrs	4 hrs
4 - Non-Critical	Development, Testing Environments	72 hrs	24 hrs

Definitions

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

Infrastructure Architecture

Multi-Region Setup

```
                    Global Load Balancer



              US-WEST (Primary)        US-EAST (DR)

              Kubernetes              Kubernetes
              Cluster                 Cluster


              RDS Primary          RDS Replica


              Redis Cluster        Redis Replica
```

Data Replication

Data Type	Replication Method	Lag Target
PostgreSQL	Streaming replication	<1 second
Redis	Redis Cluster replication	<1 second
S3	Cross-region replication	<15 minutes
Elasticsearch	Cross-cluster replication	<5 minutes

Automated Failover

Health Checks

Check	Frequency	Failure Threshold
Application health	10 seconds	3 consecutive
Database connectivity	30 seconds	2 consecutive
API response time	10 seconds	p99 > 5s for 1 min
Error rate	10 seconds	>5% for 1 min

Automated Actions

Tier 1 Services (Automatic): 1. Health check failures detected 2. Traffic automatically routes to DR region 3. DNS TTL: 60 seconds 4. Failover completes in <2 minutes 5. Alert sent to on-call team

Tier 2+ Services (Semi-Automatic): 1. Health check failures detected 2. Alert sent to on-call team 3. On-call initiates failover 4. Manual verification required

---

Manual Failover Procedures

CloudForge Failover

Pre-requisites: - [ ] Confirm primary region is unavailable - [ ] Notify stakeholders - [ ] Confirm DR region is healthy

Procedure:

```
# 1. Verify DR region health
cloudforge dr status --region us-east

# 2. Promote DR database
cloudforge db promote --region us-east --database production

# 3. Update DNS
cloudforge dns failover --service cloudforge --target us-east

# 4. Verify services
cloudforge health check --region us-east

# 5. Confirm customer traffic
cloudforge traffic status
```

Verification: - [ ] API responding in DR region - [ ] Dashboard accessible - [ ] Deployments functional - [ ] Customer notifications sent

Estimated Time: 15 minutes

DevPipeline Failover

Procedure:

```
# 1. Stop accepting new builds in primary
devpipeline maintenance enable --region us-west

# 2. Verify DR runners healthy
devpipeline runners status --region us-east

# 3. Update queue routing
devpipeline queue redirect --to us-east

# 4. Update DNS
devpipeline dns failover --target us-east

# 5. Resume build acceptance
devpipeline maintenance disable --region us-east
```

Verification: - [ ] Build queue processing - [ ] Webhooks receiving - [ ] Runners executing jobs - [ ] Artifacts accessible

Estimated Time: 20 minutes

SecureVault Failover

Critical: SecureVault requires careful handling

Procedure:

```
# 1. Verify DR vault status
securevault status --cluster us-east

# 2. Promote DR to primary
securevault dr promote --cluster us-east

# 3. Verify seal status
securevault seal-status --cluster us-east

# 4. Update application configurations
securevault config update --cluster us-east

# 5. Verify secret access
securevault verify --sample-paths
```

Verification: - [ ] Vault unsealed - [ ] Authentication working - [ ] Secrets readable - [ ] Dynamic secrets generating

Estimated Time: 10 minutes

DataLens Failover

Procedure:

```
# 1. Verify data replication status
datalens replication status

# 2. Stop ingestion in primary
datalens ingestion pause --region us-west

# 3. Promote DR region
datalens failover --to us-east

# 4. Resume ingestion in DR
datalens ingestion resume --region us-east

# 5. Update DNS
datalens dns failover --target us-east
```

Verification: - [ ] Dashboards loading - [ ] Queries executing - [ ] Alerts functional - [ ] Data ingestion working

Estimated Time: 25 minutes

Database Recovery

PostgreSQL Point-in-Time Recovery

```
# 1. Identify target time
TARGET_TIME="2024-07-25 14:30:00 UTC"

# 2. Create recovery instance
aws rds restore-db-instance-to-point-in-time \
  --source-db-instance-identifier production-db \
  --target-db-instance-identifier recovery-db \
  --restore-time $TARGET_TIME

# 3. Verify data
psql -h recovery-db.xxx.rds.amazonaws.com -c "SELECT count(*) FROM critical_table"

# 4. Promote or swap (based on verification)
```

Backup Restoration

```
# 1. List available backups
aws rds describe-db-snapshots --db-instance-identifier production-db

# 2. Restore from snapshot
aws rds restore-db-instance-from-db-snapshot \
  --db-instance-identifier restored-db \
  --db-snapshot-identifier rds:production-db-2024-07-25

# 3. Verify and promote
```

Data Recovery

S3 Object Recovery

```
# Recover deleted objects (versioning enabled)
aws s3api list-object-versions \
  --bucket production-data \
  --prefix important/

# Restore specific version
aws s3api copy-object \
  --bucket production-data \
  --copy-source production-data/important/file.json?versionId=xxx \
  --key important/file.json
```

Elasticsearch Recovery

```
# List snapshots
curl -X GET "elasticsearch:9200/_snapshot/backup/_all"

# Restore index
curl -X POST "elasticsearch:9200/_snapshot/backup/snapshot_1/_restore" \
  -H "Content-Type: application/json" \
  -d '{"indices": "important-index"}'
```

Communication During DR

Internal Communication

1. **Slack #incident-response:** Primary channel
2. **PagerDuty:** Escalation and on-call
3. **Email:** Formal updates to stakeholders
4. **Bridge call:** For extended incidents

External Communication

1. **Status page:** status.novatech.com (automated)
2. **Email to customers:** Major incidents only
3. **Twitter @NovatechStatus:** Quick updates
4. **Support ticket updates:** For active tickets

Communication Templates

Initial Notification:

```
[INVESTIGATING] We are investigating reports of [service] issues
in [region]. We will provide updates every 15 minutes.
```

Failover Initiated:

```
[UPDATE] We are failing over [service] to our disaster recovery
site. Customers may experience brief disruption. ETA: [time]
```

Recovery Complete:

```
[RESOLVED] [service] has been restored. All systems operational.
A post-incident report will be published within 48 hours.
```

Post-Recovery Procedures

Verification Checklist

- ☐ All services responding
- ☐ Data integrity verified
- ☐ No ongoing errors in logs
- ☐ Performance within normal range
- ☐ Customer-reported issues resolved
- ☐ Monitoring alerts cleared

Failback Planning

After primary region is restored:

1. **Assess primary region** (1-2 hours)
2. **Resync data** to primary (time varies)
3. **Schedule maintenance window** for failback
4. **Execute failback** during low-traffic period
5. **Verify primary** region operation
6. **Resume normal DR** posture

Post-Incident Review

Within 48 hours: - Document timeline - Identify root cause - Assess response effectiveness - Develop improvement actions - Publish incident report

---

DR Testing

Monthly Tests

- Backup restoration verification
- Replication lag checks
- Runbook review

Quarterly Tests

- Partial failover (single service)
- Communication test
- Contact list verification

Annual Tests

- Full DR exercise
- Extended operation in DR
- Failback procedure test

Test Documentation

All tests documented with: - Date and participants - Scope of test - Results and timing - Issues discovered - Remediation actions

---

Contacts

Escalation Path

Level	Contact	Response Time
L1	On-call SRE	Immediate
L2	Engineering Lead	15 minutes
L3	VP Engineering	30 minutes
L4	CEO	1 hour

Vendor Contacts

Vendor	Support Level	Contact
AWS	Enterprise	TAM or Support Case
CloudFlare	Enterprise	Enterprise Portal
PagerDuty	-	In-app support

Classification: Confidential Distribution: Engineering, Operations, Executive Team