Surface3D Disaster Recovery Plan (DRP)

Document Version: 1.0
Effective Date: March 31, 2026
Last Reviewed: March 31, 2026
Owner: Surface3D Engineering & Operations
Classification: Internal / Shareable with Clients Under NDA

---

1. Purpose

This Disaster Recovery Plan (DRP) defines the technical procedures and responsibilities for recovering Surface3D's IT systems, data, and infrastructure following a disaster or major disruption. This plan complements the Business Continuity Plan (BCP) by focusing specifically on the technical recovery of systems and data.

---

2. Scope

This plan covers the recovery of all production systems and data that comprise the Surface3D platform:

- Application code and deployment infrastructure
- Databases (Supabase/PostgreSQL, Firebase/Firestore)
- File storage (Firebase Cloud Storage)
- Authentication systems (Firebase Auth)
- Third-party service integrations (AI providers, Stripe, Resend)
- DNS and domain configuration
- Environment configuration and secrets

---

3. Recovery Objectives

3.1 Recovery Targets by System

System	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Recovery Priority
DNS / Domain	30 minutes	0	P0
Web Application (Vercel)	1 hour	0 (deployed from Git)	P0
Firebase Authentication	2 hours	0 (Google-managed)	P0
Supabase PostgreSQL	2 hours	1 hour (PITR)	P0
Firebase Cloud Storage	4 hours	24 hours (daily export)	P1
Firebase Firestore	4 hours	24 hours (daily export)	P1
AI Generation Services	4 hours	N/A (stateless)	P2
Stripe Integration	4 hours	0 (Stripe-managed)	P2
Email Services (Resend)	8 hours	N/A	P3

3.2 Recovery Tiers

- **P0 (Critical)**: Must be restored first. Platform is non-functional without these systems. Target: 0-2 hours.
- **P1 (High)**: Platform operates in degraded mode without these. Target: 2-4 hours.
- **P2 (Medium)**: Specific features are unavailable but core functionality works. Target: 4-8 hours.
- **P3 (Low)**: Non-essential services. Target: 8-24 hours.

---

4. Backup Strategy

4.1 Backup Inventory

Data Source	Backup Method	Frequency	Retention	Storage Location	Encryption
Supabase PostgreSQL	Supabase automated backups + PITR	Continuous (PITR) + daily snapshots	Per Supabase plan (7-30 days)	Supabase-managed (same region)	AES-256 at rest
Firebase Firestore	Automated export to Cloud Storage	Daily	30 days	Google Cloud Storage bucket	Google-managed encryption

Data Source	Backup Method	Frequency	Retention	Storage Location	Encryption
Firebase Cloud Storage	Google Cloud Storage replication	Continuous (multi-AZ)	N/A (inherent redundancy)	Google Cloud (multi-zone)	Google-managed encryption
Application Source Code	Git (GitHub)	Continuous (every commit)	Indefinite	GitHub servers (distributed)	In transit (TLS)
Environment Variables	Vercel environment settings + encrypted backup	On change	Current + 1 previous	Vercel + secure offline backup	AES-256
Stripe Configuration	Stripe-managed	Continuous	Indefinite	Stripe infrastructure	Stripe-managed
Firebase Auth Users	Firebase-managed + periodic export	Google-managed + weekly export	Indefinite (managed) + 30 days (export)	Google Cloud + backup storage	Google-managed encryption

4.2 Backup Testing

Test	Frequency	Procedure	Success Criteria
Supabase Backup Restore	Monthly	Restore latest backup to staging project; run data integrity checks	All tables restored; row counts match; sample queries return expected data
Firestore Export Restore	Quarterly	Import latest export to test Firestore instance; verify document counts	All collections present; document counts match production
Application Deployment from Git	Quarterly	Deploy from Git to fresh Vercel project; run smoke tests	Application loads; API routes respond; auth flow works
Environment Recovery	Semi-annually	Restore environment variables from encrypted backup to new Vercel project	All API integrations functional
Full Disaster Recovery Drill	Annually	Complete end-to-end recovery simulation	All systems recovered within RTO; data loss within RPO

---

5. Disaster Scenarios and Recovery Procedures

5.1 Scenario: Application Deployment Failure

Trigger: Bad deployment causes application errors or outage.

Step	Action	Responsible	Time
1	Identify failed deployment via Vercel dashboard or monitoring alerts	On-call Engineer	0-5 min
2	Initiate instant rollback to previous deployment via Vercel CLI: `vercel rollback`	On-call Engineer	5-10 min
3	Verify application is operational via health checks and smoke tests	On-call Engineer	10-15 min
4	Investigate root cause in failed deployment; fix and redeploy	Engineering Lead	15 min - 2 hrs

Estimated Recovery Time: 10-15 minutes

5.2 Scenario: Supabase Database Failure / Data Corruption

Trigger: Database unavailable, data corruption detected, or accidental data deletion.

Step	Action	Responsible	Time
1	Confirm database issue via Supabase dashboard and direct connection test	On-call Engineer	0-10 min
2	If Supabase platform issue: check Supabase status page; open support ticket	On-call Engineer	10-15 min
3	If data corruption/loss: initiate point-in-time recovery via Supabase dashboard to timestamp before corruption	Engineering Lead	15-45 min
4	If full database recovery needed: create new Supabase project and restore from latest backup	Engineering Lead	45-90 min

Step	Action	Responsible	Time
5	Update application environment variables to point to recovered database	Engineering Lead	5-10 min
6	Run data integrity verification queries (row counts, referential integrity, sample records)	Engineering Lead	15-30 min
7	Redeploy application with updated configuration	Engineering Lead	5-10 min
8	Verify full application functionality via smoke tests	On-call Engineer	10-15 min

Estimated Recovery Time: 1-2 hours

5.3 Scenario: Firebase Services Outage

Trigger: Firebase Authentication, Firestore, or Cloud Storage unavailable.

Step	Action	Responsible	Time
1	Confirm Firebase outage via Firebase console and status dashboard	On-call Engineer	0-10 min
2	Check Firebase status page (status.firebase.google.com) for known issues	On-call Engineer	5 min
3	If Auth outage: existing user sessions remain valid for token TTL; new logins will fail. Communicate to users.	Operations Lead	15-30 min
4	If Storage outage: users cannot upload new assets. Existing loaded/cached assets continue to function.	On-call Engineer	Immediate
5	If Firestore outage: legacy data reads fail; primary Supabase operations continue normally.	On-call Engineer	Immediate
6	Monitor Firebase status for resolution; Google SRE manages recovery	On-call Engineer	Ongoing

Step	Action	Responsible	Time
7	If prolonged (4+ hours): evaluate migration to alternative services per BCP	Engineering Lead	4+ hours

Estimated Recovery Time: Dependent on Google/Firebase (typically 1-4 hours for major incidents)

5.4 Scenario: Complete Infrastructure Loss

Trigger: Catastrophic failure affecting multiple systems simultaneously (extremely unlikely given distributed architecture).

Step	Action	Priority	Time
1	**Declare disaster recovery event**; assemble recovery team	P0	0-15 min
2	**Restore DNS**: Verify domain configuration via Namecheap; update DNS records if needed	P0	15-30 min
3	**Deploy application**: Deploy latest Git commit to new Vercel project; configure environment variables from encrypted backup	P0	30-60 min
4	**Restore authentication**: Firebase Auth is Google-managed and should recover independently. If not, provision new Firebase project and import user export.	P0	60-120 min
5	**Restore database**: Create new Supabase project; restore from latest backup; run all migrations	P0	60-120 min
6	**Restore file storage**: Provision new Firebase Cloud Storage bucket; restore from daily export	P1	2-4 hrs

Step	Action	Priority	Time
7	**Restore Firestore**: Import from latest daily export to new Firestore instance	P1	2-4 hrs
8	**Reconfigure integrations**: Update Stripe webhook URLs, AI provider API keys, Resend configuration	P2	1-2 hrs
9	**Verify all systems**: Run comprehensive integration tests; verify data integrity	All	1-2 hrs
10	**Communicate recovery**: Notify customers of restoration; provide incident report	--	Post-recovery

Estimated Total Recovery Time: 4-8 hours

5.5 Scenario: Security Breach / Compromised Credentials

Trigger: Suspected or confirmed unauthorized access to systems or data.

Step	Action	Responsible	Time
1	**Isolate**: Revoke compromised API keys and tokens immediately	On-call Engineer	0-15 min
2	**Assess scope**: Determine which systems and data were accessed	Engineering Lead	15-60 min
3	**Rotate all credentials**: Generate new API keys for all services (Firebase, Supabase, AI providers, Stripe, Resend)	Engineering Lead	30-60 min
4	**Update environment**: Deploy application with new credentials	Engineering Lead	15-30 min
5	**Audit access logs**: Review Supabase activity logs, Firebase audit logs, Vercel access logs	Engineering Lead	1-4 hrs

Step	Action	Responsible	Time
6	**Force password resets**: If user credentials compromised, force password reset for affected users via Firebase Admin SDK	Engineering Lead	30-60 min
7	**Notify affected parties**: If personal data exposed, notify affected customers within 72 hours per GDPR	Operations Lead	Within 72 hrs
8	**Post-incident review**: Document findings, root cause, and remediation actions	All	1-2 weeks

---

6. Environment Recovery Reference

6.1 Required Environment Variables

The following environment variables must be configured for a full application recovery:

Category	Variables	Source
Firebase Client	NEXT_PUBLIC_FIREBASE_API_KEY, NEXT_PUBLIC_FIREBASE_AUTH_DOMAIN, NEXT_PUBLIC_FIREBASE_PROJECT_ID, NEXT_PUBLIC_FIREBASE_STORAGE_BUCKET, NEXT_PUBLIC_FIREBASE_MESSAGING_SENDER_ID, NEXT_PUBLIC_FIREBASE_APP_ID	Firebase Console
Firebase Admin	FIREBASE_ADMIN_* credentials	Firebase Console > Service Accounts
Supabase	NEXT_PUBLIC_SUPABASE_URL, NEXT_PUBLIC_SUPABASE_ANON_KEY, SUPABASE_SERVICE_ROLE_KEY	Supabase Dashboard
Google AI	GOOGLE_AI_API_KEY	Google Cloud Console
OpenAI	OPENAI_API_KEY	OpenAI Dashboard
Replicate	REPLICATE_API_TOKEN	Replicate Dashboard

Category	Variables	Source
Stripe	STRIPE_SECRET_KEY, NEXT_PUBLIC_STRIPE_PUBLISHABLE_KEY, STRIPE_WEBHOOK_SECRET	Stripe Dashboard
Resend	RESEND_API_KEY	Resend Dashboard
Namecheap	NAMECHEAP_API_USER, NAMECHEAP_API_KEY	Namecheap Account

6.2 Encrypted Backup of Secrets

- All environment variables are backed up in an encrypted file stored securely offline
- Backup is updated whenever environment variables change
- Access to the encrypted backup requires two-factor authentication
- Decryption key is held by designated recovery personnel only

---

7. Communication During Disaster Recovery

7.1 Internal Communication

Event	Channel	Audience	Timing
Disaster declared	Phone / Slack	Recovery team	Immediate
Recovery progress updates	Slack	All engineering	Every 30 minutes
Recovery complete	Slack + Email	All staff	Upon completion

7.2 External Communication

Event	Channel	Audience	Timing
Service disruption confirmed	Status page + Email	All customers	Within 1 hour
Recovery progress	Status page	All customers	Every 2 hours
Service restored	Status page + Email	All customers	Upon restoration
Post-incident report	Email	Affected customers	Within 5 business days

8. Roles and Responsibilities

Role	Primary Responsibility	Backup
Incident Commander	Overall disaster recovery coordination; decision authority	CTO / Co-founder
Engineering Lead	Technical recovery execution; system restoration	Senior Engineer
Operations Lead	Customer communication; vendor coordination; SLA tracking	Product Manager
Security Lead	Security incident assessment; credential rotation	Engineering Lead

9. Post-Recovery Validation Checklist

After any disaster recovery event, the following must be verified before declaring recovery complete:

- ■ Application loads and renders correctly
- ■ User authentication (login/register) works
- ■ Database queries return expected data
- ■ File storage (upload/download) functions correctly
- ■ AI generation produces results
- ■ Stripe payment flow completes
- ■ Email notifications send successfully
- ■ All API endpoints respond with correct status codes
- ■ Credit system (deduction, balance, purchase) works correctly
- ■ Organization management (create, join, manage members) works
- ■ Data integrity checks pass (row counts, referential integrity)
- ■ SSL/TLS certificates are valid
- ■ Monitoring and alerting is operational

10. Plan Maintenance

Activity	Frequency	Responsible
Review and update this plan	Quarterly	Engineering Lead
Backup restoration test	Monthly	On-call Engineer
Deployment rollback test	Quarterly	Engineering Lead
Full disaster recovery drill	Annually	Incident Commander
Update environment variable backup	On every change	Engineering Lead
Review third-party provider SLAs	Semi-annually	Operations Lead

---

11. Document Control

Version	Date	Author	Changes
1.0	March 31, 2026	Surface3D Engineering	Initial version

This document is maintained by Surface3D Engineering & Operations and is subject to periodic review and updates.