Surface3D Business Continuity Plan (BCP)

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 Business Continuity Plan (BCP) defines Surface3D's strategy, procedures, and responsibilities for maintaining and restoring critical business operations in the event of a disruption. The goal is to minimize downtime, protect customer data, and ensure continuity of service for all customers and stakeholders.

---

2. Scope

This plan covers all systems, services, and operations critical to the delivery of the Surface3D platform:

- Web application (Next.js frontend and API routes)
- Database services (Supabase/PostgreSQL, Firebase/Firestore)
- File storage (Firebase Cloud Storage)
- AI generation services (Google Gemini, OpenAI, Replicate)
- Authentication services (Firebase Authentication)
- Payment processing (Stripe)
- Email services (Resend)
- Hosting and deployment (Vercel)

---

3. Business Impact Analysis (BIA)

3.1 Critical Systems Classification

System	Criticality	Maximum Tolerable Downtime (MTD)	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)
Web Application (Vercel)	Critical	4 hours	1 hour	0 (stateless, deployed from Git)
Supabase (PostgreSQL)	Critical	4 hours	2 hours	1 hour
Firebase Cloud Storage	Critical	8 hours	4 hours	24 hours
Firebase Authentication	Critical	4 hours	2 hours	0 (managed service)
AI Generation APIs	High	24 hours	4 hours	N/A (stateless)
Stripe Payments	High	24 hours	4 hours	0 (managed service)
Email (Resend)	Medium	48 hours	8 hours	N/A

3.2 Business Impact of Disruption

Duration	Impact
0-1 hour	Minimal -- users may experience temporary errors; most operations recoverable
1-4 hours	Moderate -- active design sessions may be interrupted; new generations unavailable
4-24 hours	Significant -- customers unable to create or edit designs; business operations impaired
24+ hours	Severe -- customer trust impacted; SLA breaches; potential revenue loss

---

4. Continuity Strategies

4.1 Application Hosting (Vercel)

- **Strategy**: Vercel provides automatic global CDN distribution, serverless function redundancy, and instant rollback to previous deployments
- **Redundancy**: Application is deployed across multiple Vercel edge locations globally
- **Recovery**: Rollback to last known good deployment via Vercel dashboard or CLI in under 5 minutes
- **Source of Truth**: All application code is version-controlled in Git; full redeployment possible from any commit

4.2 Primary Database (Supabase/PostgreSQL)

- **Strategy**: Supabase provides managed PostgreSQL with automated daily backups, point-in-time recovery, and high availability
- **Backup Frequency**: Automated daily backups with point-in-time recovery (PITR) within the retention window
- **Backup Testing**: Monthly backup restoration tests to a staging environment to verify data integrity and recovery procedures
- **Recovery**: Restore from backup via Supabase dashboard; failover to read replica if available on plan tier
- **Data Residency**: Data hosted in the configured Supabase region

4.3 Secondary Database (Firebase/Firestore)

- **Strategy**: Firestore provides automatic multi-region replication and 99.999% availability SLA
- **Backup Frequency**: Automated daily exports
- **Recovery**: Restore from Firestore export; Google-managed infrastructure provides automatic failover

4.4 File Storage (Firebase Cloud Storage)

- **Strategy**: Firebase Cloud Storage (backed by Google Cloud Storage) provides automatic data replication across multiple availability zones
- **Backup Frequency**: Objects are automatically replicated; supplemental daily export for critical assets
- **Recovery**: Data is inherently redundant; in case of bucket-level issue, restore from export

4.5 AI Generation Services

- **Strategy**: Multi-provider architecture provides built-in redundancy

- **Failover Path**: If primary provider (Google Gemini) is unavailable, system can route to alternative providers (OpenAI DALL-E, Flux via Replicate, Recraft)
- **Graceful Degradation**: If all AI providers are unavailable, users can still access existing designs, upload custom textures, and perform non-AI editing operations
- **Credit Protection**: Automatic credit refunds if generation fails due to provider outage

4.6 Authentication (Firebase Auth)

- **Strategy**: Firebase Authentication is a fully managed Google Cloud service with 99.95% uptime SLA
- **Failover**: Google-managed multi-region infrastructure with automatic failover
- **Recovery**: No action required; service is managed by Google. In extreme scenarios, session tokens remain valid for their TTL, allowing continued access

4.7 Payment Processing (Stripe)

- **Strategy**: Stripe provides 99.99%+ uptime with built-in redundancy
- **Failover**: Stripe manages its own infrastructure redundancy
- **Impact of Outage**: Users cannot purchase credits during a Stripe outage but can continue using existing credits. Webhook events are queued and replayed by Stripe upon recovery

---

5. Personnel and Communication

5.1 Key Roles

Role	Responsibility
Incident Commander	Declares business continuity event; coordinates response; communicates with stakeholders
Engineering Lead	Assesses technical impact; executes recovery procedures; validates system restoration
Operations Lead	Manages customer communication; coordinates with third-party providers; tracks SLA impact

5.2 Communication Plan

Audience	Channel	Timing	Responsible
Internal Team	Slack / Phone	Immediate upon incident detection	Incident Commander
Customers (Critical)	Email / Status Page	Within 1 hour of confirmed disruption	Operations Lead
Customers (All)	Status Page / In-App Banner	Within 2 hours of confirmed disruption	Operations Lead
Partners / Vendors	Email	Within 4 hours if vendor action required	Operations Lead

5.3 Escalation Path

1. **Automated monitoring** detects anomaly (Vercel, Supabase, or custom health checks)
2. **On-call engineer** investigates and classifies severity
3. **Incident Commander** is notified if severity is High or Critical
4. **Business continuity event** is declared if MTD thresholds are at risk
5. **Recovery procedures** are initiated per this plan

---

6. Business Continuity Procedures

6.1 Procedure: Application Outage

1. Verify outage via Vercel status dashboard and health check endpoints
2. If deployment issue: rollback to previous known-good deployment via Vercel CLI
3. If Vercel platform issue: monitor Vercel status page; communicate estimated recovery to customers
4. If prolonged (4+ hours): evaluate temporary deployment to alternative hosting (e.g., AWS Amplify, Netlify)

6.2 Procedure: Database Outage

1. Verify outage via Supabase dashboard and database connection checks
2. If Supabase-managed issue: monitor Supabase status; engage Supabase support
3. If data corruption: initiate point-in-time recovery to last known good state

4. If prolonged (4+ hours): restore from most recent backup to a new Supabase project
5. Update application environment variables to point to restored database
6. Verify data integrity and notify affected customers

6.3 Procedure: AI Provider Outage

1. Verify outage by testing API endpoint directly
2. Route generation requests to alternative AI provider automatically (multi-provider failover)
3. If all providers down: disable generation feature with user-facing message; existing functionality remains available
4. Monitor provider status pages; re-enable primary provider when restored
5. Process any pending credit refunds for failed generations

6.4 Procedure: Storage Outage

1. Verify via Firebase console and storage health checks
2. If Firebase Storage is unavailable: users cannot upload new assets but can continue editing with cached/loaded assets
3. If prolonged: communicate timeline to customers; prioritize restoration of storage access
4. If data loss suspected: restore from daily export backups

---

7. Testing and Maintenance

7.1 Testing Schedule

Test Type	Frequency	Description
Backup Restoration	Monthly	Restore Supabase backup to staging; verify data integrity
Deployment Rollback	Quarterly	Practice rollback to previous Vercel deployment
AI Failover	Quarterly	Simulate primary AI provider outage; verify fallback routing
Communication Drill	Semi-Annually	Practice customer notification procedures

Test Type	Frequency	Description
Full BCP Tabletop Exercise	Annually	Walk through complete disruption scenario with all key personnel

7.2 Plan Maintenance

- This plan is reviewed and updated **quarterly** or upon any significant infrastructure change
- All updates are version-controlled and communicated to key personnel
- Lessons learned from actual incidents and test exercises are incorporated into plan updates

---

8. Dependencies and Third-Party Services

Provider	Service	Criticality	SLA	Alternatives
Vercel	Application hosting	Critical	99.99%	AWS Amplify, Netlify
Supabase	Primary database	Critical	Per plan tier	Self-hosted PostgreSQL, AWS RDS
Google Cloud (Firebase)	Auth, Storage, Firestore	Critical	99.95%-99.999%	AWS Cognito (auth), AWS S3 (storage)
Google AI (Gemini/Imagen)	AI generation	High	Per Vertex AI SLA	OpenAI, Replicate
OpenAI	AI generation (alternate)	Medium	99.9%	Google Gemini, Replicate
Replicate	AI generation (alternate)	Medium	Best effort	Google Gemini, OpenAI
Stripe	Payment processing	High	99.99%+	N/A (migration complexity)
Resend	Transactional email	Medium	99.9%	SendGrid, AWS SES

---

9. Compliance and Reporting

- All business continuity incidents are documented with root cause analysis

- Incident reports are retained for a minimum of 3 years
- BCP effectiveness metrics are reported to leadership quarterly
- Backup test results are documented and retained for audit purposes

---

10. 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.