STYLDOD, INC.

Business Continuity and Disaster Recovery Policy

Enterprise Policy Document

Document ID	BCDR-001
Version	v1.0
Effective Date	June 2026
Document Owner	Senior Leadership / Engineering Leadership
Applies To	Enterprise embedded integrations, customer data, production systems, and all authorized personnel

Purpose and Scope

This policy describes Styldod's approach to business continuity, disaster recovery, resilience, backup, recovery coordination, and customer-impacting service disruption response for enterprise embedded integrations and production services. It applies to systems, data, workflows, cloud services, vendors, and personnel required to deliver enterprise customer services.

Continuity Objectives

- Protect customer data and maintain service reliability.
- Restore critical customer-facing services after disruption.
- Minimize customer impact from infrastructure, application, vendor, database, or operational failures.
- Maintain communication and escalation paths during material incidents.
- Document lessons learned and corrective actions after significant continuity events.

Critical Services and Dependencies

Area	Examples	Continuity Considerations
Application services	Iframe/widget/API workflow, frontend services, backend services.	Deployments validated in dev/stage where applicable; rollback or remediation paths available.
Cloud infrastructure	AWS Lambda, S3, SQS, CloudFront/API Gateway, WAF, logging.	Use cloud-provider resilience features, monitoring, IAM restrictions, and configuration review.
Database	MongoDB Atlas / hosted MongoDB in AWS US West 2.	Use managed database backup and recovery capabilities where available; restrict access.
Storage	Input images, generated outputs, temporary processing files.	Use cloud storage lifecycle, access restrictions, and deletion/retention controls.
Vendors / infrastructure providers	Cloud, database, monitoring, security, support, and operational tools.	Review vendor resilience and incident notices; identify alternatives or mitigations where appropriate.

Backup and Recovery Approach

- Backups and recovery mechanisms are primarily supported through managed cloud-provider and database-provider capabilities (AWS S3 versioning, MongoDB Atlas automated backups).
- Backup scope, frequency, and retention may vary by system and customer-specific deployment.

- Customer-specific RPO/RTO requirements must be agreed in the contract, DPA, or Statement of Work before production launch. Styldod does not commit to a universal RPO/RTO for all enterprise customers unless specifically agreed in writing.
- Where a recovery event occurs, engineering leadership coordinates restoration, validation, and post-recovery monitoring.
- Backup deletion follows applicable retention periods, cloud-provider mechanisms, and contractual requirements.

Continuity and Disaster Recovery Process

1. Detect disruption through monitoring alerts, cloud-provider notices, customer reports, or internal review.
2. Triage severity, affected services, impacted customers, data risk, and operational impact.
3. Activate incident response if customer data, production systems, security controls, or material service availability are involved.
4. Contain the issue and prevent further customer or data impact where possible.
5. Recover service using rollback, redeployment, cloud-provider recovery, database recovery, configuration remediation, vendor escalation, or other appropriate steps.
6. Validate restored service functionality, data integrity, access controls, and monitoring.
7. Communicate internally and, where required, externally through agreed customer channels.
8. Complete post-incident review, corrective actions, and documentation.

Communication and Escalation

- Engineering leadership owns technical recovery and validation.
- CXO/senior leadership approves customer escalation and material business decisions.
- Legal/compliance advisors are consulted for contractual, privacy, regulatory, or notification obligations where required.
- Enterprise customer communications follow the applicable agreement, Statement of Work, DPA, or agreed operational contacts.

Testing and Review

Styldod reviews continuity and recovery procedures as needed and after material incidents. Customer-specific recovery requirements, testing, evidence, or recovery playbooks should be agreed separately where required.

Limitations and Customer-Specific Requirements

Styldod does not currently commit to a universal RPO/RTO for all enterprise customers unless specifically agreed in writing. Any customer-specific uptime, recovery, data residency, backup, or disaster recovery requirements must be agreed before production launch.