

Business Continuity Plan

Last Updated: 10 Aug 2026

1. Purpose

This Business Continuity and Disaster Recovery Plan describes how Crowd Favorite maintains and restores its ability to serve clients during significant operational disruptions.

The plan addresses events including:

- Loss or degradation of a critical technology provider
- Loss of access to systems or data
- Cybersecurity incidents impacting company performance
- Personnel or key-person unavailability
- Regional infrastructure failures
- Severe weather or natural disasters
- Widespread public-health events
- Other events that materially affect Crowd Favorite's ability to deliver services

Crowd Favorite operates as a fully distributed, cloud-first digital agency. As a result, our continuity strategy focuses on preserving access to people, communications, source code, credentials, documentation, and client systems rather than recovering a physical office or company-owned data center.

Client production environments are generally operated using managed hosting or cloud infrastructure. Those environments are additionally protected by the backup, availability, security, and disaster-recovery capabilities of the applicable hosting provider and the specific configuration established for the client.

2. Scope

This plan applies to Crowd Favorite's internal operations and its ability to deliver services to clients.

It covers:



- Client communication and account management
- Software development and technical delivery
- Source-code access and version control
- Internal documentation and email
- Credential and access management
- Access to client infrastructure
- Project-management and operational systems
- Coordination with managed hosting and cloud providers
- Personnel continuity

3. Operating Model and Continuity Strategy

Crowd Favorite is a fully distributed organization with personnel working from multiple geographic locations.

There is no central office, company-owned data center, local file server, or single physical location that must remain available for Crowd Favorite to operate.

Core business functions are delivered using established cloud-based systems, including platforms used for:

- Email and collaboration
- Document storage
- Source-code management
- Credential management
- Project management
- Client communications
- Managed web hosting and cloud infrastructure

This operating model provides geographic redundancy at the workforce level.

A disruption affecting a single office location, employee workspace, ISP, city, or region does not ordinarily prevent Crowd Favorite from continuing operations as a whole.

4. Business Continuity Objectives



Crowd Favorite uses continuity and recovery objectives to prioritize restoration of critical business functions.

These are internal operational targets. Recovery of a third-party platform itself remains the responsibility of that provider.

Critical function	Continuity / Recovery objective	Primary recovery strategy
Critical client communication	Within 4 business hours	Alternate communication channels and account contacts
Normal client delivery capability	Within 1 business day	Distributed workforce, cloud systems, staff reassignment
Access to client source code	Within 4 business hours	Source control, existing authorized working copies, recovery procedures
Access to critical credentials	Within 4 business hours	Managed encrypted credential platform and administrative recovery procedures
Internal documents and operational information	Within 1 business day	Cloud-based collaboration systems and available recovery mechanisms
Client production environments	Client and provider specific	Managed-hosting backup and recovery capabilities
Critical cybersecurity response	Immediate escalation	Crowd Favorite Incident Response procedures as noted in our InfoSec Policy

5. Roles and Responsibilities

Plan Owner

The **Director of Operations** owns this plan and is responsible for:



- Maintaining the plan
- Coordinating periodic review and testing
- Assessing whether a significant event requires activation of continuity procedures
- Coordinating technical recovery activity
- Ensuring corrective actions identified through testing or incidents are tracked

Incident Coordinator

For a significant operational event, an Incident Coordinator is assigned to:

- Coordinate response activities
- Maintain an incident record
- Assign recovery actions
- Track operational status
- Escalate risks and decisions
- Coordinate handoff between technical, operational, and client-facing teams

The Incident Coordinator may vary depending on the nature of the event.

Any further required oversight is managed by the owner of this Plan. Recovery Contacts are listed in Appendix A, which is confidential and not provided with this document.

6. Critical Service Dependencies

Crowd Favorite relies on a limited number of critical cloud and technology providers to support business operations and client delivery.

Key categories include:

Google Workspace

Used for functions including:

- Email
- Calendar
- Business documents

- Collaboration
- Internal and client communications

Crowd Favorite relies on Google's infrastructure availability and redundancy for the underlying service. We maintain an external email address to allow for communication when our domain instance is impaired (crowdfavorite@gmail.com).

During a significant Google Workspace outage, Crowd Favorite may use available alternate communication channels, including phone, conferencing, project-management, and other approved collaboration systems.

GitHub

Used for:

- Source-code repositories
- Version control
- Development collaboration
- Change history
- Code review and release workflows

Local authorized Git working copies may allow development, investigation, or analysis to continue during a temporary GitHub service disruption.

Activities requiring the authoritative remote repository may be delayed until service is restored unless an approved emergency process is available.

Credential Management

Crowd Favorite uses a managed encrypted credential-management platform for controlled access to client and internal credentials.

Administrative recovery processes are maintained for authorized personnel.

Access changes that cannot safely be completed during an outage are deferred unless required for emergency response.

Managed Hosting and Cloud Infrastructure



Client applications may operate on managed hosting or cloud platforms such as:

- WP Engine
- Amazon Web Services
- Kinsta
- Other client-approved hosting providers

Backup retention, infrastructure redundancy, regional availability, restoration procedures, and recovery capabilities are determined by the applicable provider and the configuration selected for the client.

Crowd Favorite coordinates recovery activity with the provider and client as appropriate.

Other SaaS Platforms

Crowd Favorite also uses cloud-based project-management, communications, development, monitoring, and business systems.

An interruption to an individual non-critical SaaS platform may reduce efficiency or temporarily affect a particular workflow but does not ordinarily prevent the company from operating.

7. Data Protection and Recovery

Source Code

- Client application code is maintained using Git-based version control.
- Git's distributed architecture means authorized developers may maintain working copies of repositories as part of ordinary development activity.
- The authoritative repository remains the designated source-control platform.
- Recovery objectives are based on the most recent successfully committed and synchronized version of the code available through approved systems.

Business Documents and Email

- Business documents, communications, and collaboration data are maintained primarily within managed cloud platforms such as Google Workspace.
- Crowd Favorite relies on the provider's underlying infrastructure resilience, retention capabilities, and administrative recovery functionality.
- Where additional contractual backup or retention requirements exist for a client, those requirements are addressed separately.

8. Communication and Escalation

Clear communication is a central component of Crowd Favorite's continuity strategy.

Internal Communication - Implementation in 1 hour

For a significant event:

1. The event is escalated to the appropriate operational or technical owner.
2. An Incident Coordinator is assigned where necessary.
3. Relevant personnel are informed of:
 - Known impact
 - Required actions
 - Current priorities
 - Communication expectations
4. Status is updated as material information changes.

Client Communication - Implementation in 2 hours

Clients are notified when an event materially affects:

- Availability of their service
- Crowd Favorite's ability to perform contracted work
- Security of their environment or information
- A significant committed milestone
- A contractual notification requirement

Client communications should include, where known:

- Nature of the disruption
- Known impact
- Actions underway
- Any action required from the client
- Expected timing of the next update

Information that has not been validated should not be presented as fact.

9. Prioritization During a Major Disruption

During a disruption affecting multiple clients or business functions, Crowd Favorite prioritizes activities according to:

1. Safety and security
2. Active cybersecurity incidents
3. Production availability and material client impact
4. Protection of client or company information
5. Contractual or regulatory obligations
6. Critical production releases or deadlines
7. Normal project delivery
8. Internal or non-critical administrative activity

Executive management may adjust priorities based on the circumstances of the incident.

10. Return to Normal Operations

Before an incident is considered resolved, the responsible team confirms as appropriate that:

- Critical systems are available
- Data integrity has been validated
- Required credentials and access function correctly
- Deferred changes have been reconciled
- Client production services are functioning as expected
- Relevant clients have received a final or stabilization update
- Temporary processes introduced during the disruption have been retired or documented
- Outstanding corrective actions have been recorded

A post-incident review is conducted for significant disruptions and a report is produced and maintained on records for 3 years.

11. Testing and Maintenance

This plan is reviewed:

- At least annually
- Following a significant business-continuity event
- Following a material change to Crowd Favorite's technology or operating model
- When major critical service providers change
- When testing identifies a material gap

Crowd Favorite conducts periodic business-continuity exercises appropriate to its operating model.

Identified gaps are assigned an owner and tracked to resolution. A testing report is produced and maintained on records for 3 years.

12. Third-Party Provider Review

Critical technology providers are periodically reviewed as part of Crowd Favorite's security, technology, or vendor-management processes.

The review may consider:

- Importance of the service to client delivery

- Provider security practices
- Availability and service history
- Backup or recovery capabilities
- Administrative recovery procedures
- Authentication and access controls
- Multi-factor authentication support
- Contractual commitments
- Ability to export or recover information
- Availability of alternative operating methods

Crowd Favorite does not assume that provider redundancy alone eliminates business-continuity risk.

Where a provider represents a critical dependency, Crowd Favorite considers the operational impact of a prolonged outage and identifies reasonable continuity measures.

13. Plan Activation

This plan may be activated when an event:

- Prevents a critical business function from operating normally
- Is expected to materially affect client service
- Creates significant risk of data loss
- Affects a critical service provider for an extended period
- Results in significant personnel unavailability
- Requires coordination across multiple Crowd Favorite teams
- Requires invocation of alternate operating procedures

Formal activation is **not required** for routine outages that can be resolved through normal operational support procedures.