

OPERATIONS

PROOF Incident Response and Business Continuity Statement

How PROOF assesses incidents, communicates impact and supports service recovery.

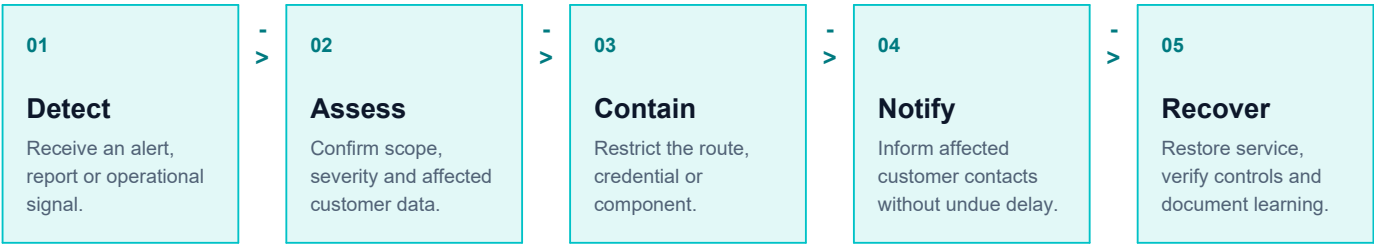
PROCUREMENT DOCUMENT

Version 1.1 | 20 September 2026 | proofhq.io/trust

The current signed agreement controls where it differs from this document.

Confirmed customer-impacting incidents are communicated without undue delay.

PROOF investigates security events, contains impact, preserves evidence and provides rolling updates to the nominated customer contact.



Communication	Content
Initial notice	Known nature of the incident, affected services, immediate containment and named contact.
Rolling update	Material changes to scope, impact, recovery or customer action.
Closure summary	Confirmed impact, recovery, root cause where known and corrective actions.

The service is designed to recover without becoming the only copy of governed state.

Daily backups and point-in-time recovery support restoration. Backups remain in-region. Governed outcomes already published to the customer's CRM remain in that system.

Database resilience Supabase and AWS provide managed database availability, backup and recovery capabilities.	Application resilience Vercel provides managed application hosting and delivery capabilities.
Customer continuity Published CRM state remains in the customer's system of record during a PROOF interruption.	Recovery verification Recovery procedures and protected data paths are exercised through release and operational controls.

Customer actions

Customers should maintain current incident contacts, preserve their own connected-system controls and notify PROOF promptly of suspected credential misuse or unauthorised access.

Security contact
Report suspected vulnerabilities or incidents to security@proofhq.io. Do not include unnecessary customer data in the initial report.