Business Continuity & Disaster Recovery (BCDR) Summary

Version:2.0
Last Updated: 1st September 2026
Classification: Public

Business Continuity & Disaster Recovery (BCDR) Summary

This document describes Concord's Business Continuity and Disaster Recovery program — the measures supporting continuity of critical operations and recovery of customer services following a disruptive event. Read together with the Security Overview, Infrastructure & Architecture Overview, and the applicable Service Level Agreement.

Objectives

Protect the availability of customer services, minimize operational disruption, safeguard customer information, support timely recovery of critical business functions, maintain effective incident communications, and continuously improve operational resilience.

Governance

Business continuity and disaster recovery activities are overseen through documented policies and defined roles and responsibilities, covering identification of critical services, risk assessment, recovery strategy, and periodic review of recovery capability.

Business Continuity Planning

Concord maintains plans addressing cloud infrastructure disruption, cybersecurity incidents, loss of key systems, third-party service interruption, workforce disruption, and network connectivity failure. Plans are reviewed and updated periodically.

Disaster Recovery Strategy

Recovery procedures prioritize customer-facing services and critical operational functions, and cover recovery planning, data backup, infrastructure restoration, service validation, operational communication, and post-recovery review.

Backup Strategy

Customer data is backed up automatically on a daily schedule, with backup encryption, integrity verification, and periodic restoration testing.

Recovery Objectives

Formal Recovery Time Objective (RTO) and Recovery Point Objective (RPO) commitments are scoped per engagement, based on a customer's specific requirements and service tier, and documented in the applicable Service Level Agreement or contract where offered. We're happy to discuss target RTO/RPO for your use case during procurement — Concord does not publish a single generic RTO/RPO figure that would apply uniformly to every deployment, tier, or customer.

High Availability

Redundant, managed cloud services, automated health monitoring, load balancing, fault isolation, and elastic scaling reduce the likelihood and impact of service interruption.

Incident Response Integration

BCDR activities are integrated with incident response: detection, impact assessment, response-team activation, containment, service restoration, customer communication where appropriate, and post-incident review, with lessons learned feeding back into future planning.

Crisis Management

Defined roles and responsibilities coordinate executive decision-making, internal and customer communications, vendor coordination, and recovery oversight during a significant operational event.

Third-Party Dependencies

Certain services rely on reputable third-party providers — cloud infrastructure, identity services, and AI providers (see section subprocessor of Privacy data protection overview). Critical vendors are evaluated and monitored as part of ongoing operational risk management.

Recovery Testing

BCDR capability is periodically evaluated through backup restoration testing, recovery exercises, and lessons-learned review, feeding directly back into recovery procedures.

Customer Communication

Where a disruption materially affects customer services, Concord provides timely communication appropriate to the nature of the event — status updates, estimated recovery timelines where available, and a post-incident summary where appropriate.

Shared Responsibility

Concord is responsible for: platform recovery, infrastructure restoration, backup management, disaster recovery planning, and incident coordination.

Customers are responsible for: endpoint security, user access management, retaining exported business records where appropriate, and their own business continuity planning.

Additional Information

Available on request, subject to confidentiality obligations: Security Overview, Infrastructure & Architecture Overview, Service Level Agreement, and an incident response documentation summary.
