

Service Overview

Misco Data Protection & Cyber Resilience Services provide organisations with structured, ongoing support to protect critical data, maintain service continuity, and recover effectively from cyber incidents, system failures, or data loss events. The service focuses on strengthening resilience across backup, recovery, and continuity capabilities rather than delivering a single technology or platform.

The service is vendor-agnostic and can incorporate a range of data protection, backup, disaster recovery, and cyber resilience technologies depending on customer requirements.

Service Scope

The service supports organisations in maintaining reliable, secure, and recoverable data environments. It is designed to complement existing infrastructure, cloud platforms, and operational processes, helping customers reduce data loss risk and improve recovery readiness. Service scope is defined at call-off and may vary based on data volumes, environments, and resilience objectives.

What the Service Includes

- Management and oversight of backup and recovery processes
- Support for cyber-resilient backup and immutable storage approaches
- Monitoring of data protection jobs and recovery points
- Incident support for data loss, corruption, or ransomware events
- Recovery planning, testing, and restoration guidance
- Reporting on backup health, coverage, and recovery readiness
- Advisory services aligned to business continuity and resilience goals
- A named service or technical account manager

Service Delivery Model

The service is delivered remotely using secure management tools, integrations with customer environments, and collaboration with customer IT and security teams.

Delivery includes defined operational procedures for monitoring, escalation, and response.

Recovery scenarios are supported through guided processes to minimise downtime and data loss.

Support Model

Support is provided using a severity-based approach. Incidents impacting data availability or recovery capability are prioritised based on business impact. Support coverage may include business-hours support or enhanced coverage, including out-of-hours response for critical incidents, depending on the agreed service level.

Security and Assurance

Security controls are applied throughout service delivery, including access restrictions, least-privilege principles, and secure handling of backup data and credentials. Resilience and recovery practices are aligned to recognised industry best practices and frameworks.

Detailed technical and security controls are available on request under appropriate confidentiality arrangements.

Commercials

Pricing is based on the agreed service scope, data volumes, environments supported, and support coverage. All costs are defined at call-off, with no hidden onboarding fees unless explicitly agreed.

Exit and Offboarding

At service termination, access to customer systems and data protection tooling is withdrawn in a controlled manner. Any customer data handled as part of service delivery is securely removed or returned in line with contractual and data protection requirements.

Misco Data Protection & Cyber Resilience Services provide practical, ongoing capability to protect critical data, strengthen recovery readiness, and support organisations in responding effectively to data loss and cyber incidents.