Service Brief

Dell Cyber Recovery Vault

Managed Services

This document outlines the scope, deliverables, responsibilities, and terms governing Redesign's Dell Cyber Recovery Vault Managed Services. This service provides continuous monitoring, validation, and support for the Dell Cyber Recovery Vault platform to ensure it remains operationally resilient, securely isolated, and ready to support ransomware recovery objectives.

This engagement is governed by this Service Brief and asThis engagement is governed by this Service Brief and associated with SKU: MS-VAULT. The quantity defined in the quote reflects the number of Dell Cyber Recovery Vaults to be actively managed.

Table of Contents

01. Services Overview

Redesign's Dell Backup & Restore Managed Services deliver continuous management Redesign's managed service for Dell Cyber Recovery Vault environments provides proactive monitoring and operational oversight to ensure the vault remains in a validated state of isolation and recoverability.

02. Offer Structure

Primary Service

- Vault job and infrastructure monitoring
- Secure Copy and air gap health verification
- Alert management and incident triage
- Policy and retention compliance reviews
- Documentation upkeep

Optional Add-Ons

Separate SOW

- Recovery, Forensics, and Incident Response

03. Project Scope

This engagement includes the ongoing management of the Dell Cyber Recovery Vault environment(s) defined at the start of the engagement. Scope includes review and validation of:

- **Dell Cyber Recovery software platform**
- **Associated Data Domain and Secure Copy workflows**
- **Vault access controls and separation enforcement**

04. Quantity & Effort Model

- **Service SKU**: MS-VAULT
- **Quantity:** Number of Dell Cyber Recovery Vault environments to be supported

Each unit includes monitoring and validation of the Cyber Recovery Vault and associated components.

- This service includes up to the number of hours specified in the associated quote for operational support per month, limited to the activities defined in this Service Brief. Unused hours do not carry over to subsequent months. Additional support hours may require a revised quote or a separate Statement of Work (SOW).

05. Services & Key Activities

Onboarding Process (30 Days)

- Conduct kickoff session with customer stakeholders to confirm vault scope, access methods, and security requirements
- Validate connectivity and access to Cyber Recovery and CyberSense environments
- Review current vault configuration, isolation logic, and retention policies
- Baseline Secure Copy schedules, sync processes, and alert thresholds
- Establish reporting framework for vault health, anomalies, and recovery validation
- Provide knowledge transfer on Redesign's vault operations model, escalation paths, and incident handling

Continuous Activities

- Monitor vault job execution, Secure Copy health, and access activity Identify
- sync or copy failures and alert on access anomalies
- Report vault-related alerts from Cyber Recovery and CyberSense
- Track backup job completion into the vault to ensure CyberSense is analyzing complete backups
- Maintain configuration and security documentation for vault environment
- Update vault documentation and recovery workflows

Annual Activities

- Review Cyber Recovery strategy and alignment with recovery targets

06. Deliverables

Redesign will deliver all scoped services within the monthly support hour limit defined in the quote. Fixed deliverables (e.g., scheduled reports or platform reviews) will be prioritized.

Support beyond the allocated hours is not guaranteed and may require a change order.

Monthly vault health and compliance reports

Alert and incident summary

Configuration and access control documentation

Annual vault status report and strategy review

Monthly Service Review
(virtual, 1 hour)

07. Services Scope Changes

Changes to vault architecture, integration with production DR workflows, or enhanced compliance reporting may require a revised quote or separate SOW.

08. Services Scope Exclusions

This engagement does not include:

- Vault software or hardware deployment (available under separate scope)
- CyberSense installation
- Licensing or provisioning of Dell components
- Forensic or cyber incident recovery support

09. Customer Responsibilities

- Maintain valid Dell licensing and support agreements
- RECON DataDiodes are installed in the Vault and are confirmed to be operational
- Provide Redesign with remote access to vault management consoles and logs
- Assign internal stakeholder for coordination
- Communicate infrastructure or security changes affecting vault operations
- Failure to meet these requirements will prevent Redesign from delivering the services outlined in this Service Brief.

10. Services Schedule

- **Start Date:** Upon signed quote and kickoff
- **Completion:** End date specified in the quote

11. Terms and Conditions

This engagement will be governed by the Seller's terms and conditions located at:

www.redesign-group.com/legal

Services will not begin until the following prerequisites are met:

- Signed quote referencing **SKU: MS-VAULT** and quantity
- Access to the vault platform validated
- Stakeholders assigned and kickoff scheduled
- DataDiodes are installed in the Vault and are confirmed to be operational
- Failure to meet these requirements will prevent Redesign from delivering the services outlined in this Service Brief.

[re]DESIGN

The future belongs
to the curious.