SHARED RESPONSIBILITY MATRIX

Version 2026-08-16

Operational roles for managed security, backup, continuity, and information-technology controls

Purpose and Scope

Neatoware does not guarantee that Client will never experience a Security Incident, data loss, system failure, or service disruption. Client remains responsible for its overall security posture, risk acceptance, business decisions, users, data classification, legal and regulatory obligations, and systems or controls outside the contracted scope. Neatoware is responsible for performing the Managed Services included in the selected tier or otherwise expressly contracted. This Matrix identifies the parties' operational roles and does not expand liability beyond the Agreement.

Responsibility Designations

Lead means the party responsible for coordinating and performing the primary operational activities within the contracted scope. Supporting means the party responsible for providing information, access, approvals, cooperation, or related assistance. Decision Authority means the party with final authority over the identified material decision. Client generally retains Decision Authority for material business, legal, regulatory, notification, restoration, shutdown, remediation, continuity, and risk-acceptance decisions. Neatoware may take routine, preauthorized, or emergency containment actions within scope when reasonably necessary to prevent imminent harm, preserve evidence, protect systems or data, or limit a Security Incident, with notice to Client as soon as reasonably practicable.

Control Area	Lead	Supporting	Decision Authority	Responsibilities
Identity and Access Management	Neatoware	Client	Client	Neatoware configures and maintains contracted identity and access-management tools. Client defines roles, approves access, authorizes privileged accounts, manages personnel lifecycle decisions, and establishes access policies.

Control Area	Lead	Supporting	Decision Authority	Responsibilities
User Administration	Neatoware	Client	Client	Neatoware performs authorized user additions, changes, disabling, and deletions within scope. Client submits timely requests, approves privileged access, and promptly informs Neatoware of terminations and role changes.
Endpoint Protection and Antivirus	Neatoware	Client	Neatoware for routine tool operation; Client for material remediation decisions	Neatoware deploys, configures, monitors, and maintains the contracted endpoint-protection solution on managed devices. Client ensures devices remain available, connected, supported, and within scope.
Endpoint Detection and Response	Neatoware	Client	Client for material remediation decisions	Neatoware deploys, configures, monitors, and responds to alerts from the contracted EDR platform. Neatoware may isolate devices or take other preauthorized containment actions when reasonably necessary. Client approves material remediation, shutdown, restoration, or business-impacting actions unless immediate action is reasonably necessary to prevent imminent harm.

Control Area	Lead	Supporting	Decision Authority	Responsibilities
Patch Management	Neatoware	Client	Client for high-risk or business-impacting changes	Neatoware evaluates and deploys approved operating-system and application patches on managed devices according to applicable policies. Client approves high-impact changes, maintenance windows, and exceptions and remains responsible for unsupported, excluded, or unavailable systems.
Firewall and Network Configuration	Neatoware	Client	Client	Neatoware manages and monitors contracted network devices and configurations. Client authorizes material rule changes, remote-access policies, segmentation decisions, and changes affecting business operations or third-party connectivity.
Security Monitoring and Alert Triage	Neatoware	Client	Neatoware for alert classification; Client for material response decisions	Neatoware monitors contracted systems and triages alerts within the selected tier. Client provides requested information, access, and cooperation and identifies business-critical systems and operational constraints.

Control Area	Lead	Supporting	Decision Authority	Responsibilities
Security Incident Containment and Technical Response	Neatoware	Client	Client for material remediation and business decisions	Neatoware investigates, contains, isolates, preserves available evidence, and performs authorized technical response activities within scope. Client determines whether to shut down systems, restore data, engage legal counsel, retain forensic specialists, incur third-party response costs, or accept continuing risk.
Security Incident Notification to Client	Neatoware	Client	Neatoware under the DPA	Neatoware notifies Client of a Security Incident in accordance with the Data Processing Addendum. Information may be provided in phases as the investigation proceeds.
Regulatory, Individual, Insurer, and Law-Enforcement Notifications	Client	Neatoware	Client	Client determines whether notification to regulators, affected individuals, insurers, law enforcement, or other parties is legally or contractually required. Neatoware provides reasonable information and assistance within scope and as required by the DPA.

Control Area	Lead	Supporting	Decision Authority	Responsibilities
Backup Selection and Scope	Client	Neatoware	Client	Client identifies the systems, applications, files, data, and recovery priorities to be protected. Neatoware provides recommendations and implements the backup scope expressly selected by Client.
Backup Operation, Monitoring, and Retention	Neatoware	Client	Client for retention and recovery objectives	Neatoware configures, monitors, and manages contracted backup jobs, retention settings, off-site replication, storage utilization, alerts, and exceptions. Client approves retention periods, recovery objectives, protected data, exclusions, and additional storage charges.

Control Area	Lead	Supporting	Decision Authority	Responsibilities
Backup Integrity and Restoration Readiness	Neatoware	Client	Neatoware for routine validation; Client for production restoration decisions	Neatoware uses available job-status reporting, integrity checks, backup-chain validation, storage-health monitoring, alerting, and other verification mechanisms to assess contracted backups. Neatoware reviews exceptions, takes corrective action within scope, and performs restores in the ordinary course of implementation, troubleshooting, migration, incident response, disaster recovery, and Client-requested restoration. No fixed periodic representative restore-test schedule applies unless expressly stated in a custom Schedule.

Control Area	Lead	Supporting	Decision Authority	Responsibilities
Backup Restoration	Neatoware	Client	Client for production restoration and business-impacting decisions	Neatoware performs authorized restoration activities within scope and the applicable tier. Client identifies the desired recovery point, validates restored data and application functionality, provides required credentials and application knowledge, and approves production-impacting decisions. Recovery time depends on data volume, infrastructure, connectivity, third-party systems, and the event.
Disaster-Recovery Technical Planning	Neatoware	Client	Client	Where included or separately contracted, Neatoware leads technical recovery planning, documentation, architecture, and recovery procedures. Client provides business priorities, acceptable downtime, recovery objectives, staffing, facilities, communications requirements, and approvals. No fixed annual tabletop or disaster-recovery exercise is required unless expressly included in a custom Schedule or separately authorized.

Control Area	Lead	Supporting	Decision Authority	Responsibilities
Cybersecurity Awareness Training	Neatoware	Client	Client	Neatoware provides or facilitates the contracted training platform and content. Client assigns training, requires participation, addresses noncompliance, and enforces personnel and acceptable-use policies.
Data Classification and Retention Policies	Client	Neatoware	Client	Client determines data classifications, retention periods, legal holds, regulatory requirements, and disposal rules. Neatoware implements contracted technical settings based on Client's documented instructions.
Physical Security	Each party for its own facilities	Not applicable	Each party for its own facilities	Client is responsible for physical security of its premises, equipment, users, and facilities. Neatoware is responsible for physical security of its own facilities and equipment.

Control Area	Lead	Supporting	Decision Authority	Responsibilities
Unsupported, Legacy, or Excluded Systems	Client	Neatoware	Client	Client retains responsibility for systems, applications, devices, or services outside the contracted scope. Neatoware may provide recommendations or separately billable assistance when agreed but is not obligated to manage or remediate unsupported or excluded systems.
Third-Party Vendor Coordination	Neatoware	Client	Client	Neatoware coordinates with third-party vendors within scope. Client provides authorizations, account access, vendor contacts, and cooperation and retains Decision Authority over vendor selection, contracts, licensing, fees, approvals, and material third-party decisions unless otherwise agreed.

Control Area	Lead	Supporting	Decision Authority	Responsibilities
Business Continuity and Risk Acceptance	Client	Neatoware	Client	Neatoware provides technical recommendations and contracted continuity support. Client establishes business priorities, acceptable downtime, recovery objectives, insurance coverage, risk tolerance, and final continuity decisions.

Conflicts and Scope Limitations

If a responsibility in this Matrix conflicts with another document forming part of the Agreement, the order of precedence in the Product and Services Agreement controls. Neatoware's designation as Lead does not make Neatoware responsible for systems, devices, data, users, vendors, or controls outside the contracted scope. Client's failure to provide timely approvals, access, information, credentials, equipment, or cooperation may delay or prevent performance. Backup status, integrity checks, monitoring, verification, and successful prior restorations reduce risk but do not guarantee recovery from every failure, corruption event, cyberattack, hardware condition, third-party outage, or other circumstance.