



SCHEDULE OF SERVICES

CARE Services, Service Toolkits, and Technology Subscriptions | Draft for legal review

Effective August 06, 2026. These Service Descriptions supersede and replace all prior versions.

1. Scope and Structure

The Managed Services to be provided by Provider are identified in the applicable Order. Additional Services may only be added through a mutually executed Order or amendment.

Certain CARE Services and CARE Service Toolkits include cybersecurity-related activities intended to support the security, stability, and operational integrity of Client's technology environment. Depending on the Services and Toolkits selected by Client, these activities may include patch management, firmware management, endpoint protection, firewall security services, security awareness training, phishing simulation testing, email security, dark web monitoring, security event monitoring, alert review, vulnerability identification, and remediation of supported security-related events. Such activities are limited to the monitoring, management, and remediation services described in the applicable CARE Services and Toolkits.

Where security alerts, suspicious activity, malware detections, unauthorized access attempts, security misconfigurations, vulnerabilities, or other security-related conditions are identified through Provider-managed systems, Provider may investigate, prioritize, escalate, and perform reasonable remediation activities consistent with the Services and Toolkits subscribed to by Client.

Examples of remediation activities that may be included within the CARE Services include application of security updates, correction of security-related configuration issues, blocking known malicious websites, email senders, domains, or IP addresses, isolating or removing known malware from managed systems, initiating account security actions such as password resets or account disablement, and investigating alerts generated by Provider-managed security systems.

Unless expressly identified in an applicable Order, Statement of Work, or other written agreement, the CARE Services do not include dedicated cybersecurity monitoring, threat hunting, digital forensic investigations, incident response services, cyber breach recovery services, penetration testing, security consulting engagements, security assessments, or other specialized cybersecurity services. Activities beyond routine monitoring, management, and remediation may require additional services and fees.

A CARE Service Toolkit is a bundled collection of software subscriptions, cloud services, and technology components utilized by Provider to support delivery of the associated CARE Service. Components of a CARE Service Toolkit may be added, removed, replaced, or modified by Provider from time to time provided substantially equivalent functionality is maintained.

2. Technology Subscriptions

Provider may offer software subscriptions, cloud services, telecommunications services, backup services, security services, domain services, and other technology products ("Technology Subscriptions"). Technology Subscriptions may be provided directly by Provider or through third-party vendors.

Technology Subscriptions are distinct from CARE Services and are intended to provide Client with access to technology platforms, software, hardware subscriptions, telecommunications services, or cloud-based services. Unless expressly identified in an applicable Order, purchase of a Technology Subscription does not include ongoing monitoring, management, administration, remediation, consulting, support, or other recurring labour services.

Support, configuration, administration, troubleshooting, remediation, consulting, project work, or other labour associated with Technology Subscriptions may be billed separately in accordance with Provider's then-current time and materials rates unless covered by an applicable CARE Service.

Examples of Technology Subscriptions include, without limitation:

- Voice over Internet Protocol (VoIP) and business telecommunications services
- Email signature services
- Backup and disaster recovery subscriptions
- Cloud backup services
- Endpoint and email security subscriptions
- Domain registration and SSL certificate services
- Software licensing subscriptions
- Artificial intelligence and productivity platforms
- Other software-as-a-service (SaaS) offerings

The foregoing examples are illustrative only and do not represent an exhaustive list of Technology Subscriptions offered by Provider.

3. Backup and Recovery Responsibilities

Certain CARE Service Toolkits and Technology Subscriptions may include technologies intended to facilitate backup, replication, retention, recovery, restoration, disaster recovery, or business continuity activities.

Client acknowledges that backup and recovery technologies are designed to reduce risk but do not eliminate the possibility of data loss, corruption, ransomware, hardware failure, software defects, malicious activity, human error, service interruption, or other events affecting the availability, integrity, or recoverability of data and systems.

Unless expressly identified in an applicable Order, Statement of Work, or other written agreement, Provider does not warrant or guarantee the recoverability of data, the success of any restoration effort, the availability of backup data, the achievement of any recovery time objective (RTO), recovery point objective (RPO), business continuity objective, or disaster recovery objective.

Client remains responsible for determining the adequacy of its backup, retention, business continuity, disaster recovery, legal hold, regulatory compliance, and data protection requirements, and for notifying Provider of any changes to such requirements.

Backup-related monitoring, administration, restoration assistance, recovery testing, disaster recovery planning, and other backup or recovery activities are limited to those Services, Toolkits, Technology

Subscriptions, Orders, or Statements of Work specifically purchased by Client. Services beyond the scope of Client's subscribed Services may require additional services and fees.

4. Third-Party Services and Vendors

Certain CARE Service Toolkits and Technology Subscriptions may utilize software, hardware, cloud services, telecommunications services, hosting services, security services, artificial intelligence services, or other technologies provided by third-party vendors.

Client acknowledges that such third-party services may be subject to separate license agreements, end-user license agreements, terms of use, service limitations, feature changes, pricing changes, service interruptions, outages, vendor-imposed restrictions, or discontinuation by the applicable third-party provider.

Provider does not own or control such third-party services and does not warrant or guarantee their availability, compatibility, performance, functionality, security, or continued operation. Provider shall not be responsible for the acts, omissions, failures, service interruptions, outages, security incidents, product changes, licensing changes, pricing changes, or discontinuation of services by third-party vendors.

Where applicable, Client agrees to comply with the licensing terms, acceptable use policies, end-user agreements, and other requirements imposed by third-party providers.

Provider reserves the right to add, remove, replace, or substitute third-party technologies utilized within a CARE Service Toolkit where reasonably necessary due to product discontinuation, licensing changes, service availability concerns, security considerations, vendor relationships, or other business or technical reasons, provided substantially equivalent functionality is maintained.

5. CARE Service Administration

Provider utilizes a service management platform to administer, coordinate, document, and track activities associated with CARE Services. Incidents, service requests, alerts, maintenance activities, changes, and other service-related activities may be recorded and managed through Provider's service management systems.

Provider may generate, update, assign, escalate, prioritize, and close service tickets as necessary to deliver the CARE Services.

Alerts generated by Provider-managed systems may automatically generate service tickets and may be investigated, remediated, escalated, or closed by Provider without separate authorization when such actions are reasonably necessary to deliver the subscribed CARE Services.

6. Projects and Non-Recurring Services

CARE Services are intended to provide recurring monitoring, management, maintenance, administration, support, remediation, and advisory activities associated with covered systems, users, technologies, and environments. Unless expressly identified in an applicable Order, Statement of Work, or other written agreement, Projects and Non-Recurring Services are excluded from CARE Services.

Projects and Non-Recurring Services may include, but are not limited to:

- Implementation of new systems, technologies, software, or services.
- Hardware deployments, replacements, refreshes, or upgrades.

SYSOFT COMPUTER CONSULTANTS LIMITED

- Software deployments, migrations, major version upgrades, or application implementations.
- Cloud migrations, tenant migrations, data migrations, or workload migrations.
- Network redesigns, infrastructure redesigns, or significant configuration changes.
- Security remediation initiatives requiring substantial engineering effort.
- Cybersecurity incident response, breach recovery, forensic investigations, or threat hunting activities.
- Technology assessments, audits, consulting engagements, or strategic planning initiatives.
- Compliance remediation projects, certification preparation activities, or implementation of new compliance controls.
- Disaster recovery planning, disaster recovery testing, business continuity planning, or recovery exercises.
- Relocations, office moves, expansions, consolidations, or facility-related technology projects.
- Any activity requiring dedicated project management, engineering, consulting, planning, coordination, documentation, implementation, or training resources beyond the routine administration and support activities included within the subscribed CARE Services.

Provider shall determine, acting reasonably, whether a request, activity, initiative, or remediation effort constitutes a Project or Non-Recurring Service. Where an activity falls outside the scope of the subscribed CARE Services, Provider may provide such services pursuant to a separate Order, Statement of Work, fixed-fee project agreement, or time and materials engagement.

7. CARE Services

7.1 UserCARE Service

Provider will provide end-user help desk services for authorized users through Provider's support portal, email, and telephone support channels, including incident and service request management, troubleshooting of supported hardware, software, and cloud services, remote desktop support and assistance, user account administration and password reset assistance, and coordination with approved third-party vendors as required to resolve support issues. Unless otherwise specified in an Order, the Service includes unlimited remote support for covered users during Provider's standard support hours. The Service Fee does not include end-user training, consulting engagements, support for unsupported hardware or software, or Projects and Non-Recurring Services as described in this Schedule unless expressly identified in an Order.

7.1 UserCARE Service Toolkit

The UserCARE Service Toolkit consists of a bundled collection of software subscriptions, cloud services, and technology components selected by Provider to support delivery of the UserCARE Service. Toolkit components may include technologies related to end-user productivity, support, security, backup, monitoring, awareness training, phishing testing, and related user-focused services. Provider may add, remove, replace, or modify Toolkit components from time to time provided substantially equivalent functionality is maintained.

7.2 EndpointCARE Service

Provider will provide proactive monitoring, management, and support of covered workstations and endpoint devices, including continuous monitoring of endpoint health and performance, alert review, triage, and remediation, operating system patch management, manufacturer-recommended firmware and driver

updates where supported, configuration backup and recovery capabilities where applicable, performance reporting and asset monitoring, and remote troubleshooting and remediation of covered devices. The Service Fee does not include hardware replacement, new device deployments, operating system upgrades, data migration services, or Projects and Non-Recurring Services as described in this Schedule unless expressly identified in an Order.

7.2 EndpointCARE Service Toolkit

The EndpointCARE Service Toolkit consists of a bundled collection of software subscriptions, cloud services, and technology components selected by Provider to support delivery of the EndpointCARE Service. Toolkit components may include technologies related to endpoint monitoring, device management, operating system maintenance, patch management, endpoint security, automation, configuration management, and related endpoint-focused services. Provider may add, remove, replace, or modify Toolkit components from time to time provided substantially equivalent functionality is maintained.

7.3 FirewallCARE Service

Provider will provide proactive monitoring, management, and support of covered firewall appliances, including firewall configuration management, implementation and maintenance of firewall traffic policies, firmware management and updates where supported by the manufacturer, review and implementation of authorized configuration changes, alert monitoring and remediation, performance monitoring, and troubleshooting of supported firewall services. Where licensed and maintained by Client through the applicable vendor subscription, Provider will configure, manage, and monitor available security services including Intrusion Prevention Services (IPS), URL Filtering, Gateway Antivirus, application control, and other supported security features provided by the firewall platform. The Service Fee does not include hardware or firewall replacement, major firewall upgrades, architecture or network redesigns, migration or implementation of new network environments, remediation of security incidents, penetration testing, compliance assessments, or Projects and Non-Recurring Services as described in this Schedule unless expressly identified in an Order.

7.3 FirewallCARE Service Toolkit

The FirewallCARE Service Toolkit consists of a bundled collection of software subscriptions, cloud services, and technology components selected by Provider to support delivery of the FirewallCARE Service. Toolkit components may include technologies related to firewall management, network security, threat prevention, web filtering, malware protection, monitoring, reporting, and related firewall-focused services. Provider may add, remove, replace, or modify Toolkit components from time to time provided substantially equivalent functionality is maintained.

7.4 ServerCARE Service

Provider will provide proactive monitoring, management, and support of covered servers, including continuous monitoring of server health, availability, and performance, alert review, triage, and remediation, operating system patch management and maintenance, backup monitoring and management for supported backup solutions, performance reporting and capacity monitoring, remote troubleshooting and remediation of covered systems, and escalation and prioritization of critical incidents. The Service Fee does not include major hardware upgrades, hardware replacement, operating system migrations, application upgrades, new server deployments, or Projects and Non-Recurring Services as described in this Schedule unless expressly identified in an Order.

7.4 ServerCARE Service Toolkit

The ServerCARE Service Toolkit consists of a bundled collection of software subscriptions, cloud services, and technology components selected by Provider to support delivery of the ServerCARE Service. Toolkit components may include technologies related to server monitoring, administration, maintenance, backup oversight, performance management, automation, and related server-focused services. Provider may add, remove, replace, or modify Toolkit components from time to time provided substantially equivalent functionality is maintained.

7.5 HypervisorCARE Service

Provider will provide proactive monitoring, management, and support of covered virtualization platforms, including continuous monitoring of hypervisor availability, health, and performance, alert review, triage, and remediation, configuration monitoring and management, capacity planning and performance reporting, remote troubleshooting and remediation of supported hypervisor environments, and escalation and prioritization of critical infrastructure incidents. The Service Fee does not include new hypervisor deployments, major version upgrades, hardware replacement, migration projects, disaster recovery testing projects, or Projects and Non-Recurring Services as described in this Schedule unless expressly identified in an Order.

7.5 HypervisorCARE Service Toolkit

The HypervisorCARE Service Toolkit consists of a bundled collection of software subscriptions, cloud services, and technology components selected by Provider to support delivery of the HypervisorCARE Service. Toolkit components may include technologies related to virtualization management, infrastructure monitoring, capacity planning, performance reporting, automation, and related hypervisor-focused services. Provider may add, remove, replace, or modify Toolkit components from time to time provided substantially equivalent functionality is maintained.

7.6 EnvironmentCARE Service

Provider will provide ongoing management and administration of Client's technology environment, including software license management, domain management, dark web monitoring, maintenance of technology asset inventories, coordination of environment-level administrative activities, review of technology environment changes, reporting on technology environment status, and recommendations intended to improve the overall health, security, and operational integrity of Client's technology environment. The Service Fee does not include implementation of new systems, licensing costs, domain registration fees, consulting engagements, vendor professional services, remediation work requiring significant engineering effort, or Projects and Non-Recurring Services as described in this Schedule unless expressly identified in an Order.

Pricing Note: This Service is organization-based. Fees are charged per legal entity or operating organization and are intended to support the ongoing administration and management of Client's technology environment.

7.6 EnvironmentCARE Service Toolkit

The EnvironmentCARE Service Toolkit consists of a bundled collection of software subscriptions, cloud services, and technology components selected by Provider to support delivery of the EnvironmentCARE Service. Toolkit components may include technologies related to domain administration, software license management, technology asset management, dark web monitoring, environment-wide administration, and

related organization-focused services. Provider may add, remove, replace, or modify Toolkit components from time to time provided substantially equivalent functionality is maintained.

7.7 ComplianceCARE Service

Provider will provide ongoing technology compliance management services, including maintenance of technology-related compliance documentation, periodic review of technical and administrative controls, tracking of compliance obligations, requirements, and deadlines, coordination of compliance evidence collection and record retention, compliance reporting and status reviews, support for audit and assessment preparation activities, guidance regarding cybersecurity, privacy, cyber insurance, and industry compliance requirements, and recommendations for corrective actions and continuous improvement of technology compliance programs. The Services are limited to information technology, cybersecurity, and related administrative controls and may include policies, standards, procedures, system configurations, technical safeguards, evidence collection, and control validation activities. The Service Fee does not include audit execution, certification or attestation services, legal or regulatory advice, independent compliance assessments, preparation of regulatory filings, representation before regulatory bodies, or Projects and Non-Recurring Services as described in this Schedule unless expressly identified in an Order.

Pricing Note: This Service is organization-based. Fees are charged per legal entity or operating organization and are intended to support the ongoing management and maintenance of the organization's technology compliance program.

7.7 ComplianceCARE Service Toolkit

The ComplianceCARE Service Toolkit consists of a bundled collection of software subscriptions, cloud services, and technology components selected by Provider to support delivery of the ComplianceCARE Service. Toolkit components may include technologies related to compliance management, documentation management, evidence collection, reporting, policy administration, control validation, and related compliance-focused services. Provider may add, remove, replace, or modify Toolkit components from time to time provided substantially equivalent functionality is maintained.

7.8 CPCSCCARE Service

Provider will provide ongoing technology compliance management services focused on maintaining Canadian Program for Cyber Security Certification (CPCSC) Level 1 requirements, including maintenance of CPCSC-related compliance documentation, periodic review of CPCSC technical and administrative controls, tracking of CPCSC compliance obligations, requirements, and deadlines, coordination of CPCSC evidence collection and record retention, compliance reporting and readiness reviews, support for CPCSC assessment and audit preparation activities, guidance regarding CPCSC Level 1 cybersecurity requirements, and recommendations for corrective actions and continuous improvement of Client's CPCSC compliance program. The Services are limited to information technology, cybersecurity, and related administrative controls required to support CPCSC Level 1 compliance and may include policies, standards, procedures, system configurations, technical safeguards, evidence collection, control validation activities, and support for the protection of Sensitive Information (SI). The Service Fee does not include audit execution, certification or attestation services, legal or regulatory advice, independent compliance assessments, preparation of regulatory filings, representation before regulatory bodies, guarantees of CPCSC certification or assessment outcomes, or Projects and Non-Recurring Services as described in this Schedule unless expressly identified in an Order.

Pricing Note: This Service is organization-based. Fees are charged per legal entity or operating organization and are intended to support the ongoing management and maintenance of the organization's CPCSC Level 1 compliance program. Additional services related to higher certification levels, expanded assessment scope, Secure Room operations, or specialized Sensitive Information (SI) handling requirements may require additional fees.

7.8 CPCSCCARE Service Toolkit

The CPCSCCARE Service Toolkit consists of a bundled collection of software subscriptions, cloud services, and technology components selected by Provider to support delivery of the CPCSCCARE Service. Toolkit components may include technologies related to CPCSC compliance management, documentation management, evidence collection, reporting, assessment readiness, control validation, and related CPCSC-focused services. Provider may add, remove, replace, or modify Toolkit components from time to time provided substantially equivalent functionality is maintained.

8. Legal Review

This draft is provided for review and approval by legal counsel. Defined terms, order-of-precedence provisions, limitation-of-liability language, notice requirements, amendment rights, and other agreement-wide governance terms should be read together with the Master Services Agreement and applicable Order.