**DEFENDIT SERVICES**

**MASTER MANAGED SERVICES AGREEMENT**

**Version 1.0**

This Master Managed Services Agreement ("Agreement") is entered into by and between **DefendIT Services** ("DefendIT") and the customer identified in the applicable Statement of Work or Managed Services Schedule ("Client"). This Agreement establishes the terms and conditions governing the delivery of managed information technology, cybersecurity, cloud, consulting, and related professional services.

This Agreement is intended to create a long-term technology partnership by clearly defining the rights, responsibilities, and expectations of both parties

**Table of Contents**

26. Termination
27. Early Termination
28. Transition and Offboarding
29. Force Majeure
30. Dispute Resolution
31. General Provisions
32. Signature Page

**Exhibits**

- Exhibit A – Service Level Agreement
- Exhibit B – Cybersecurity Addendum
- Exhibit C – Shared Responsibility Matrix
- Exhibit D – Microsoft Licensing Addendum

**Guiding Principles**

**1. Purpose**

DefendIT Services believes technology should enable business growth, reduce operational risk, and provide organizations with confidence in their daily operations. This Agreement establishes the framework for a professional relationship centered on trust, transparency, accountability, and shared responsibility.

The parties acknowledge that effective technology management requires cooperation. While DefendIT Services provides managed IT and cybersecurity services using commercially reasonable practices and industry standards, successful outcomes also depend on the Client maintaining appropriate internal processes, making timely business decisions, and implementing recommended safeguards.

This Agreement is intended to:

- Clearly define the Services to be provided.
- Establish measurable service expectations.
- Describe the responsibilities of each party.

- Protect the confidentiality and security of information.
- Create a fair allocation of business and operational risks.
- Provide procedures for resolving issues efficiently.
- Support a long-term technology partnership.

Nothing in this Agreement should be interpreted as a guarantee that any technology environment will be free from interruptions, failures, cyberattacks, or other events beyond the reasonable control of either party. Instead, the parties agree to work collaboratively to reduce risk, respond appropriately to incidents, and continuously improve the Client's technology environment over the course of the engagement.

**ARTICLE II – SCOPE OF SERVICES**

**Purpose:** This Article defines the nature of the Services provided by DefendIT Services, establishes the contractual framework for future Statements of Work and Service Schedules, and clarifies what is and is not included under this Agreement.

**2.1 General Scope**

DefendIT Services ("DefendIT") shall provide the managed information technology, cybersecurity, cloud, consulting, professional, and related services described in one or more Statements of Work ("SOW"), Managed Services Schedules ("MSS"), Service Level Agreements ("SLA"), or other written addenda executed by the parties (collectively, the "Service Documents").

This Agreement establishes the legal terms governing the relationship between the parties. No specific Service is required to be provided unless expressly identified in an applicable Service Document.

**2.2 Service Documents**

Each Service Document shall identify, as applicable:

- The Services to be provided;
- The covered locations, users, devices, or environments;
- Applicable service levels;
- Fees and billing terms;
- Project deliverables and milestones, if applicable;
- Assumptions, exclusions, and Client dependencies;

- Any special terms that supplement this Agreement.

If there is a conflict between this Agreement and a Service Document, the Service Document shall control only with respect to the specific Services addressed therein, unless it expressly states that it modifies this Agreement.

**2.3 Managed Services**

Managed Services are recurring operational services intended to support, maintain, monitor, secure, and optimize the Client's technology environment on an ongoing basis.

Unless otherwise stated in the applicable Service Document, Managed Services may include activities such as:

- Remote monitoring and management;
- Endpoint administration;
- Patch and update management;
- Microsoft 365 administration;
- Identity and access management;
- Backup monitoring;
- Firewall and network management;
- Endpoint detection and response;
- Security monitoring;
- Help desk support;
- Vendor coordination;
- Technology planning and consulting.

The exact scope of Managed Services shall be defined in the applicable Managed Services Schedule.

**2.4 Professional Services**

Professional Services consist of project-based or non-recurring work that falls outside the recurring Managed Services described in the applicable Managed Services Schedule.

Examples include:

- Office relocations;

- Cloud migrations;
- Server deployments;
- Network redesigns;
- Wireless implementations;
- Security assessments;
- Compliance consulting;
- Infrastructure upgrades;
- Major software implementations;
- Custom engineering services.

Unless otherwise agreed in writing, Professional Services are billed separately from recurring Managed Services.

**2.5 Excluded Services**

Unless expressly included in an applicable Service Document, the following are excluded from the Services:

- Custom software development;
- Electrical or building cabling work;
- Construction-related services;
- Manufacturer warranty repairs;
- Data entry;
- Legal, accounting, or regulatory consulting;
- Recovery of data that cannot be restored through supported backup solutions;
- Forensic investigations;
- Expert witness services;
- Incident response beyond the scope of the Client's service plan.

Additional services requested by the Client may be provided under a separate Statement of Work or Change Order.

**2.6 Third-Party Products and Services**

Many Services depend upon products, software, cloud platforms, telecommunications providers, internet service providers, manufacturers, or other third parties.

DefendIT does not own or control such third-party products or services and cannot guarantee their continued availability, performance, pricing, or functionality.

DefendIT will use commercially reasonable efforts to assist the Client in working with third-party providers but is not responsible for the acts, omissions, outages, security incidents, licensing decisions, or service interruptions of third parties.

**2.7 Changes to Services**

Technology requirements evolve over time. Either party may request modifications to the Services.

Changes affecting scope, pricing, service levels, deliverables, or recurring fees must be documented in a written Change Order, amended Statement of Work, or other mutually executed amendment before becoming effective, unless emergency action is reasonably necessary to protect the Client's environment or respond to a Security Incident.

**2.8 Service Availability**

Unless otherwise specified in the applicable Service Document or SLA:

- Remote support will be provided during Business Hours.
- After-hours support is subject to availability and applicable emergency rates unless included in the Client's service plan.
- Response and resolution objectives are governed exclusively by the applicable Service Level Agreement.

**2.9 No Guarantee of Continuous Operation**

The Client acknowledges that information technology systems are subject to interruption, degradation, hardware failure, software defects, cyber threats, utility outages, telecommunications failures, and other events beyond DefendIT's reasonable control.

Accordingly, DefendIT does not warrant that any technology environment will operate without interruption or that all security incidents, outages, vulnerabilities, or failures can be prevented. DefendIT's obligation is to perform the Services in a professional and workmanlike manner using commercially reasonable practices consistent with the applicable Service Documents.

**ARTICLE III**

**CLIENT RESPONSIBILITIES**

**Purpose:** This Article establishes the Client's responsibilities that are essential to DefendIT Services' ability to deliver the Services. The parties acknowledge that effective managed IT and cybersecurity services require active cooperation, timely communication, and shared responsibility.

**3.1 General Cooperation**

The Client shall cooperate in good faith with DefendIT Services and provide the information, access, personnel, approvals, and assistance reasonably necessary for DefendIT to perform the Services.

The Client acknowledges that delays in providing requested information, approvals, access, or resources may delay project completion, affect service levels, or increase costs.

**3.2 Authorized Contacts**

The Client shall designate one or more Authorized Contacts who are empowered to:

- Submit service requests.
- Approve quotations and Statements of Work.
- Authorize emergency work.
- Request changes to Services.
- Receive security notifications.
- Approve invoices when applicable.

DefendIT may rely upon instructions received from an Authorized Contact unless DefendIT has actual knowledge that such authorization has been revoked.

**3.3 Administrative Access**

The Client shall provide DefendIT with administrative access reasonably necessary to perform the Services, including access to:

- Microsoft 365 tenant administration
- Azure subscriptions
- Network infrastructure

- Firewalls
- Wireless controllers
- Servers
- Endpoints
- Backup systems
- Domain registrars
- DNS management
- Cloud platforms
- Line-of-business applications, where applicable

The Client represents that it has the legal authority to grant such access.

**3.4 Supported Technology Standards**

The Client acknowledges that the quality and security of the Services depend upon maintaining technology that meets DefendIT's supported standards.

Accordingly, the Client agrees to maintain, replace, or upgrade hardware, software, operating systems, firmware, subscriptions, and related technology as reasonably recommended by DefendIT to address end-of-support, security vulnerabilities, compatibility issues, or operational risks.

DefendIT may decline to provide certain Services or modify applicable service levels for Unsupported Technology as defined in Article I.

**3.5 Security Responsibilities**

The Client retains responsibility for the security decisions affecting its business operations.

Unless expressly delegated in writing, the Client is responsible for:

- User hiring and termination notifications
- User account approval
- Password confidentiality
- Physical security of facilities
- Employee policy enforcement

- Business process approvals
- Regulatory compliance
- Cyber insurance procurement
- Data classification
- Retention requirements
- Approval of security recommendations

DefendIT shall not be responsible for security risks arising from the Client's refusal to implement commercially reasonable security recommendations after written notice.

**3.6 Timely Decisions**

The Client agrees to make business decisions and provide requested approvals within a commercially reasonable period.

Where the Client delays approval of security updates, hardware replacements, licensing changes, or project milestones, DefendIT shall not be responsible for delays or resulting impacts that are reasonably attributable to such delay.

**3.7 Software Licensing**

The Client is responsible for maintaining valid software licenses unless DefendIT expressly agrees in writing to procure and manage such licensing on the Client's behalf.

The Client shall not knowingly direct DefendIT to install, copy, or use software in violation of applicable license agreements.

**3.8 Backup Verification**

Where backup monitoring is included within the Services, DefendIT will monitor the operational status of supported backup systems as described in the applicable Service Documents.

Unless expressly stated otherwise, the Client remains responsible for:

- Determining appropriate backup retention periods.
- Identifying critical systems and data.
- Reviewing backup and disaster recovery objectives.
- Participating in periodic restoration testing.

- Verifying that restored data satisfies the Client's operational requirements.

**3.9 Incident Reporting**

The Client agrees to promptly notify DefendIT upon becoming aware of:

- Suspected ransomware.
- Phishing attacks.
- Unauthorized account access.
- Lost or stolen devices.
- Security policy violations.
- Data loss.
- Wire fraud attempts.
- Business Email Compromise.
- Any event reasonably believed to affect the confidentiality, integrity, or availability of the Client's systems or data.

Prompt notification enables DefendIT to respond more effectively and may reduce the impact of a security incident.

**3.10 Safe Working Environment**

Where Services are performed at the Client's premises, the Client shall provide a reasonably safe working environment and disclose known hazards that may affect DefendIT personnel.

**3.11 Compliance Responsibility**

Unless expressly stated in a signed Statement of Work, DefendIT does not serve as the Client's legal counsel, auditor, or regulatory compliance advisor.

Although the Services may assist the Client in supporting cybersecurity or regulatory initiatives, the Client remains solely responsible for determining and maintaining compliance with applicable laws, regulations, contractual obligations, and industry standards.

**3.12 Failure to Perform Client Responsibilities**

If the Client fails to perform its responsibilities under this Agreement and such failure materially affects DefendIT's ability to provide the Services, DefendIT may:

- Suspend affected Services upon reasonable notice where appropriate.
- Adjust project schedules.
- Invoice for additional work required due to the delay or failure.
- Modify applicable service level commitments for the affected Services until the issue is resolved.

DefendIT will use commercially reasonable efforts to notify the Client of the issue and provide an opportunity to remedy it before taking such action, except where immediate action is reasonably necessary to protect systems, data, or personnel.

**ARTICLE IV**

**FEES, BILLING, PAYMENT TERMS, AND PRICE ADJUSTMENTS**

**Purpose:** This Article establishes the financial terms governing the Services, including invoicing, payment obligations, recurring fees, project billing, price adjustments, taxes, and remedies for late or non-payment.

**4.1 Fees**

Client agrees to pay DefendIT Services ("DefendIT") the fees set forth in the applicable Statement of Work, Managed Services Schedule, Quote, Order Form, or other mutually executed Service Document (collectively, the "Fee Schedule").

Unless otherwise stated, all fees are stated in U.S. Dollars and are exclusive of applicable sales, use, excise, value-added, or similar taxes, which shall be the responsibility of the Client unless a valid tax exemption certificate is provided.

**4.2 Monthly Recurring Services**

Fees for Monthly Recurring Services ("MRS") shall be invoiced in advance on a monthly basis unless otherwise stated in the applicable Service Document.

Recurring Services begin on the Service Commencement Date identified in the applicable Service Document and continue until terminated in accordance with this Agreement.

Partial months may be prorated at DefendIT's discretion.

**4.3 Professional Services**

Professional Services shall be billed as specified in the applicable Statement of Work.

Unless otherwise agreed, Professional Services may be invoiced:

- On a fixed-fee basis;
- On a time-and-materials basis;
- Based upon project milestones; or
- Upon project completion.

Travel, lodging, shipping, third-party expenses, and other approved reimbursable costs may be invoiced separately.

**4.4 Payment Terms**

Unless otherwise stated in writing:

- Monthly Recurring Service invoices are due upon receipt.
- Professional Services invoices are due within fifteen (15) calendar days of the invoice date.
- Hardware, software, licensing, cloud subscriptions, and third-party products may require payment prior to procurement.

Failure to timely pay any invoice constitutes a material breach of this Agreement.

**4.5 Automatic Payment (Optional)**

DefendIT may require payment by Automated Clearing House (ACH), electronic funds transfer (EFT), or other approved automatic payment method for recurring Managed Services.

If automatic payment is required under the applicable Service Document, the Client agrees to maintain valid payment information throughout the Term of this Agreement.

**4.6 Late Payments**

Amounts not paid when due may accrue interest at the lesser of:

- One and one-half percent (1.5%) per month; or
- The maximum lawful rate permitted under applicable Texas law.

DefendIT may also recover reasonable costs incurred in collecting delinquent amounts, including attorneys' fees, court costs, arbitration costs, and collection agency fees, to the extent permitted by law.

Acceptance of a late payment does not waive DefendIT's rights under this Agreement.

**4.7 Disputed Charges**

If the Client disputes an invoice, the Client shall notify DefendIT in writing within fifteen (15) calendar days after the invoice date, identifying the specific disputed charges and the basis for the dispute.

The undisputed portion of the invoice shall remain due and payable according to the original payment terms.

The parties shall work in good faith to resolve disputed charges promptly.

**4.8 Price Adjustments**

To account for increased labor costs, software licensing, cloud services, cybersecurity requirements, inflation, and other operational expenses, DefendIT may adjust recurring fees no more than once during any twelve (12)-month period.

DefendIT shall provide at least sixty (60) days' prior written notice of any recurring fee adjustment.

Unless otherwise specified in the applicable Service Document, annual recurring fee adjustments shall not exceed the greater of:

- Five percent (5%); or
- The annual percentage increase in the U.S. Consumer Price Index (CPI-U), All Urban Consumers, for the most recently published twelve-month period.

This limitation does not apply to:

- Increases imposed by third-party vendors or cloud providers;
- Changes requested by the Client;
- Changes in the number of supported users, devices, or locations;
- Material changes to the scope of Services.

**4.9 Third-Party Licensing and Vendor Costs**

The Client acknowledges that software licenses, cloud subscriptions, telecommunications services, security platforms, and other third-party products may be subject to pricing, billing, renewal, and contractual requirements established by their respective providers.

If a third-party provider increases pricing or modifies licensing requirements, DefendIT may pass through such increases upon reasonable notice, unless otherwise prohibited by a written agreement.

**4.10 Taxes**

The Client is responsible for all applicable federal, state, and local taxes arising from the Services, excluding taxes based solely upon DefendIT's net income.

**4.11 Returned Payments**

Returned checks, rejected ACH transactions, chargebacks, or other failed payment transactions may be subject to a reasonable administrative fee, together with any actual bank charges incurred by DefendIT.

**4.12 Credit Holds and Suspension**

If any invoice remains unpaid beyond the applicable payment terms, DefendIT may, after providing written notice and a reasonable opportunity to cure (except where immediate action is warranted), suspend procurement, project work, administrative changes, or other Services until the Client's account is brought current.

Emergency cybersecurity response services intended to protect the Client's environment may continue at DefendIT's discretion and may be billed separately.

**4.13 No Right of Setoff**

Except as required by applicable law or as agreed in writing by the parties, the Client shall not withhold payment, deduct amounts, or offset invoices against any claim it may have against DefendIT.

**4.14 Billing Errors**

DefendIT may correct clerical, mathematical, or administrative billing errors discovered after an invoice has been issued. Any such correction shall be explained to the Client and reflected on a subsequent invoice or credit memorandum.

**4.15 Survival**

The Client's obligation to pay amounts earned or incurred prior to termination, together with any accrued interest, collection costs, or other payment obligations that survive by their nature, shall remain in effect following expiration or termination of this Agreement.

## ARTICLE V

## TERM, RENEWAL, AND TERMINATION

**Purpose.** This Article establishes the duration of the parties' contractual relationship, the commercial commitment for Managed Services, renewal procedures, and the circumstances under which either party may terminate the Agreement or a Service Document.

### 5.1 Effective Date

This Agreement becomes effective on the Effective Date identified on the signature page ("Effective Date") and shall remain in effect until terminated in accordance with this Agreement.

This Agreement serves as the legal framework governing all Services provided by DefendIT Services ("DefendIT") under any current or future Service Document.

### 5.2 Evergreen Master Agreement

The parties acknowledge that this Master Managed Services Agreement is intended to remain in effect on an ongoing basis.

Termination of an individual Statement of Work, Managed Services Schedule, or other Service Document shall not automatically terminate this Agreement unless all Service Documents have been terminated and either party provides written notice terminating this Agreement.

### 5.3 Initial Term of Managed Services

Unless otherwise stated in the applicable Managed Services Schedule, Managed Services shall commence on the Service Commencement Date and continue for an initial term of **thirty-six (36) months** ("Initial Term").

The Initial Term reflects the parties' acknowledgment that DefendIT invests substantial resources in onboarding, documentation, engineering, security configuration, automation, licensing, and personnel to support the Client's environment.

### 5.4 Automatic Renewal

Upon expiration of the Initial Term, each Managed Services Schedule shall automatically renew for successive **twelve (12) month** renewal terms unless either party provides written notice of non-renewal at least **ninety (90) days** before the expiration of the then-current term.

During each renewal term, all provisions of this Agreement and the applicable Service Documents shall remain in full force and effect unless modified by a written amendment signed by both parties.

**5.5 Additional Services**

The parties may execute additional Statements of Work, Change Orders, Managed Services Schedules, or Addenda at any time during the Term.

Unless expressly stated otherwise, such documents shall become part of this Agreement and shall not modify the Initial Term applicable to existing Managed Services.

**5.6 Termination for Cause**

Either party may terminate this Agreement or an applicable Service Document upon written notice if the other party:

a. Materially breaches this Agreement and fails to cure such breach within thirty (30) days after receiving written notice describing the breach;

b. Becomes insolvent, files for bankruptcy protection, makes an assignment for the benefit of creditors, or ceases substantially all business operations; or

c. Engages in unlawful conduct that materially affects the other party's ability to perform under this Agreement.

If the breach cannot reasonably be cured within thirty (30) days, the breaching party shall not be in default if it commences corrective action within the cure period and diligently pursues completion.

**5.7 Immediate Termination**

DefendIT may immediately suspend or terminate affected Services, in whole or in part, if continued performance would reasonably be expected to:

- Violate applicable law;
- Jeopardize the security of DefendIT's systems or those of other clients;
- Expose DefendIT personnel to unsafe working conditions;

- Require DefendIT to participate in unlawful activity; or
- Create a substantial and imminent cybersecurity risk.

DefendIT shall provide written notice as soon as reasonably practicable under the circumstances.

**5.8 Client-Initiated Early Termination**

The Client may request termination of a Managed Services Schedule before the expiration of the Initial Term by providing written notice.

If DefendIT accepts such early termination, the Client shall pay the Early Termination Payment described in **Article VI (Early Termination Payment)**.

The parties acknowledge that the Early Termination Payment is intended to reasonably compensate DefendIT for anticipated losses resulting from the premature conclusion of the Managed Services relationship and is not intended as a penalty. The specific formula for calculating the payment is set forth in Article VI.

**5.9 Effect of Non-Renewal**

Expiration or non-renewal of a Managed Services Schedule shall not affect:

- Payment obligations incurred before termination;
- Confidentiality obligations;
- Intellectual property rights;
- Indemnification obligations;
- Limitations of liability;
- Dispute resolution provisions; or
- Any provision that, by its nature, is intended to survive termination.

**5.10 Transition Services**

Following expiration or termination, DefendIT may provide transition or offboarding assistance at the Client's written request.

Unless otherwise specified in a Service Document, transition services:

- Are not included within Monthly Recurring Services;
- Shall be billed at DefendIT's then-current Professional Services rates;

- Are subject to DefendIT's scheduling availability; and
- Shall be governed by the terms of this Agreement.

**5.11 Return of Property**

Upon termination, each party shall promptly return or securely destroy the other party's Confidential Information as required by this Agreement, except where retention is required by law or reasonably necessary to enforce contractual rights.

Client-owned equipment, credentials, documentation, and other property shall be returned in accordance with the applicable Offboarding Policy and any applicable Statement of Work.

**5.12 No Waiver**

Termination of this Agreement shall not waive any claim or remedy that accrued before the effective date of termination.

**5.13 Survival**

The following Articles shall survive expiration or termination of this Agreement:

- Fees and Payment Obligations
- Confidentiality
- Intellectual Property
- Data Protection
- Limitation of Liability
- Indemnification
- Dispute Resolution
- Governing Law
- Collection Costs
- Any other provision that by its nature is intended to survive termination.

**ARTICLE VI**

**EARLY TERMINATION FEE**

**6.1 General**

The parties acknowledge that Defend IT Services ("Defend IT") makes substantial investments in personnel, onboarding, implementation, training, infrastructure, software licensing, vendor commitments, and other resources in reliance upon the Client's agreement to the Initial Term and any Renewal Term established in the applicable Managed Services Schedule ("MSS").

The parties further acknowledge that the actual damages resulting from an early termination by the Client would be difficult to determine with precision at the time this Agreement is executed. Accordingly, the parties agree that the Early Termination Fee set forth in this Article constitutes a reasonable estimate of the damages Defend IT is expected to incur and is intended as liquidated damages and not as a penalty.

**6.2 Early Termination by Client Without Cause**

If the Client terminates the applicable Managed Services Schedule or materially reduces the contracted scope of recurring Managed Services before the expiration of the then-current contractual term, other than as expressly permitted by this Agreement, the Client shall pay Defend IT an Early Termination Fee.

The Early Termination Fee shall become immediately due and payable upon the effective date of termination and shall be in addition to all other amounts then due under this Agreement.

**6.3 Calculation of Early Termination Fee**

The Early Termination Fee shall consist of:

**(a)** One hundred percent (100%) of the Monthly Recurring Charges ("MRC") that would have become due for the remainder of the then-current Initial Term or Renewal Term, calculated from the effective date of termination through the last day of the applicable contractual term;

PLUS

**(b)** All non-cancelable or non-refundable third-party costs, subscription commitments, licensing obligations, cloud service commitments, software agreements, equipment financing obligations, telecommunications commitments, or other contractual liabilities incurred by Defend IT on the Client's behalf that remain payable after termination;

PLUS

**(c)** Any unpaid invoices, reimbursable expenses, taxes, late charges, interest, or other amounts accrued prior to the effective date of termination.

**6.4 Renewal Terms**

The Early Termination Fee described in this Article applies equally during:

the Initial Term; and

each successive Renewal Term.

For purposes of calculating the Early Termination Fee, the remaining balance shall be measured only through the end of the then-current contractual term and shall not include future renewal periods.

**6.5 Third-Party Subscription Commitments**

The Client acknowledges that Defend IT may enter into non-cancelable agreements with third-party providers in order to deliver the Services, including but not limited to:

- Microsoft Cloud Solution Provider (CSP) subscriptions;
- Microsoft New Commerce Experience (NCE) commitments;
- Managed Detection and Response (MDR) services;
- Endpoint Detection and Response (EDR) licensing;
- Security Information and Event Management (SIEM) platforms;
- Backup and disaster recovery services;
- Cloud infrastructure services;
- Internet and telecommunications services; and
- Other software or service subscriptions purchased for the Client's benefit.

The Client remains responsible for all non-cancelable commitments incurred on its behalf through the applicable commitment period, regardless of whether the underlying Managed Services are terminated.

**6.6 No Early Termination Fee**

No Early Termination Fee shall apply if:

1. Defend IT materially breaches this Agreement and fails to cure such breach within the applicable cure period;
2. The parties execute a written agreement terminating or replacing the applicable MSS that expressly waives the Early Termination Fee;

3. Termination is expressly authorized elsewhere in this Agreement without payment of an Early Termination Fee; or
4. Applicable law prohibits enforcement of the Early Termination Fee.

**6.7 Effect of Payment**

- Payment of the Early Termination Fee shall not relieve the Client of responsibility for:
- Returning Defend IT property;
- Cooperating in an orderly transition of Services;
- Paying any undisputed invoices that became due before termination; or
- Satisfying any obligations that expressly survive termination.

**6.8 Exclusive Early Termination Remedy**

The Early Termination Fee is intended to compensate Defend IT for anticipated losses arising from an early termination of recurring managed services. Except for unpaid invoices, reimbursement of non-cancelable third-party commitments, interest, attorneys' fees where recoverable under this Agreement, and other remedies expressly preserved herein, Defend IT shall not seek duplicative recovery for the same anticipated recurring service revenue covered by the Early Termination Fee.

**6.9 Survival**

The obligations set forth in this Article shall survive the expiration or termination of this Agreement until all amounts due have been paid in full.

**ARTICLE VII**

**SUSPENSION OF SERVICES**

**Purpose.** The parties acknowledge that certain circumstances may require DefendIT Services ("DefendIT") to temporarily suspend some or all Services to protect the security, integrity, or stability of the Client's environment, DefendIT's systems, or other customers. Suspension is intended to be a temporary operational remedy and does not, by itself, terminate this Agreement or any applicable Service Document.

**7.1 Right to Suspend Services**

DefendIT may suspend all or any portion of the Services upon written notice to Client if:

a. Client fails to pay undisputed invoices in accordance with Article IV and does not cure such non-payment within the applicable cure period;

b. Client materially breaches this Agreement or any applicable Service Document and fails to cure the breach within the required cure period;

c. Client's systems, networks, accounts, or technology environment present a material cybersecurity risk to Client, DefendIT, or any third party;

d. Continued performance would require DefendIT to violate applicable law, regulation, court order, licensing requirement, or professional obligation;

e. Client directs DefendIT to perform work that DefendIT reasonably believes would materially compromise the security, integrity, or availability of Client's systems or data; or

f. DefendIT reasonably determines that suspension is necessary to protect its personnel, infrastructure, management platforms, or other customers.

**7.2 Emergency Suspension**

Notwithstanding Section 7.1, DefendIT may immediately suspend affected Services without prior notice when DefendIT reasonably believes immediate action is necessary to:

- Contain or mitigate a Security Incident;
- Prevent unauthorized access;
- Stop the spread of malware, ransomware, or other malicious activity;
- Protect Confidential Information;
- Preserve the integrity or availability of systems managed by DefendIT;
- Comply with a lawful governmental order or other legal obligation.

DefendIT shall notify Client as soon as reasonably practicable following an Emergency Suspension.

**7.3 Notice and Opportunity to Cure**

Except in cases of Emergency Suspension, DefendIT shall provide written notice describing:

- The basis for the proposed suspension;
- The actions reasonably necessary to restore Services;
- Any applicable cure period; and
- The anticipated effective date of suspension if the issue is not corrected.

Client shall use commercially reasonable efforts to remedy the condition within the stated cure period.

**7.4 Effect of Suspension**

Unless otherwise agreed in writing:

a. Suspension shall not terminate this Agreement or any applicable Service Document.

b. Monthly Recurring Service Fees shall continue to accrue during any suspension resulting from Client's breach, non-payment, or failure to satisfy its obligations under this Agreement.

c. DefendIT shall have no responsibility for delays, missed service levels, outages, data loss, security events, or other consequences directly resulting from the suspension or from the underlying condition that necessitated the suspension.

d. Any work reasonably required to restore Services following suspension that falls outside the scope of the Managed Services may be billed as Professional Services at DefendIT's then-current rates.

**7.5 Restoration of Services**

DefendIT shall use commercially reasonable efforts to restore suspended Services after:

- The condition giving rise to the suspension has been corrected;
- Required payments have been received;
- Required security measures have been implemented, where applicable;
- Client has provided any requested information or approvals reasonably necessary to restore Services.

If restoration requires substantial engineering work, migration activities, or remediation efforts beyond the scope of the Managed Services, DefendIT may require execution of a Statement of Work before restoration activities commence.

**7.6 Client Security Exceptions**

If Client declines or elects to defer a written security recommendation that DefendIT reasonably determines is necessary to reduce a material cybersecurity risk, DefendIT may:

- Document the recommendation and Client's decision;

- Require Client to acknowledge the associated risks in writing;
- Modify applicable Service Level commitments for systems directly affected by the declined recommendation; and
- Decline responsibility for Security Incidents that are directly attributable to the specific risk identified in the declined recommendation, to the extent permitted by applicable law.

Nothing in this Section relieves DefendIT of its obligation to perform the Services expressly included within the applicable Service Documents.

**7.7 No Waiver**

DefendIT's decision not to suspend Services in response to a particular breach, security condition, or payment default shall not constitute a waiver of its right to suspend Services for the same or any future occurrence.

**7.8 Reservation of Rights**

Suspension of Services is cumulative of, and not exclusive of, any other rights or remedies available to DefendIT under this Agreement, at law, or in equity, including the right to terminate this Agreement pursuant to Article VIII.

**ARTICLE VIII**

**DEFAULT AND TERMINATION**

**8.1 Events of Default**

The occurrence of any of the following shall constitute an **Event of Default** under this Agreement:

a. Failure to pay any undisputed amount due under this Agreement within the applicable cure period;

b. A material breach of this Agreement or any applicable Service Document that remains uncured after written notice;

c. A material misrepresentation made by either party in connection with this Agreement;

d. The unauthorized use, disclosure, or misuse of Confidential Information resulting in material harm to the non-breaching party;

e. Repeated violations of Client's obligations under this Agreement that materially impair DefendIT's ability to perform the Services;

f. Insolvency, bankruptcy, assignment for the benefit of creditors, appointment of a receiver, or cessation of substantially all business operations by either party; or

g. Any other material failure to perform obligations under this Agreement that substantially deprives the non-defaulting party of the benefit of the Agreement.

**8.2 Notice of Default**

Except where immediate termination is expressly permitted under this Agreement, the non-defaulting party shall provide written notice describing:

- The nature of the alleged default;
- The contractual provisions involved;
- The actions reasonably required to cure the default; and
- The applicable cure period.

Notice may be delivered in accordance with Article XX (General Provisions).

**8.3 Cure Period**

Unless a different period is expressly provided elsewhere in this Agreement:

- Payment defaults shall be subject to a **ten (10) Business Day** cure period.
- All other material breaches shall be subject to a **thirty (30) calendar day** cure period.

If the breach cannot reasonably be cured within thirty (30) days, the breaching party shall not be deemed in default if it:

1. Begins corrective action within the cure period;
2. Continues such efforts diligently; and
3. Completes the cure within a commercially reasonable period.

**8.4 Termination for Cause**

If an Event of Default is not cured within the applicable cure period, the non-defaulting party may terminate this Agreement or the affected Service Document by written notice.

Unless otherwise stated, termination shall become effective on the date specified in the notice.

**8.5 Immediate Termination**

DefendIT may terminate this Agreement or any affected Service Document immediately upon written notice if:

a. Continued performance would violate applicable law;

b. Client intentionally compromises the security of DefendIT's systems or management platforms;

c. Client knowingly directs DefendIT to engage in unlawful conduct;

d. Client repeatedly refuses to implement minimum security requirements required to safely deliver the contracted Services, after documented notice and reasonable opportunity to address the issue;

e. DefendIT reasonably determines that continuing the engagement presents an unacceptable legal, regulatory, or cybersecurity risk.

**8.6 Effect of Termination**

Termination shall not affect:

- Amounts earned prior to termination;
- Outstanding invoices;
- Approved project work;
- Third-party licensing commitments;
- Hardware purchases;
- Early Termination Payment obligations under Article VI;
- Confidentiality obligations;
- Intellectual Property rights;
- Indemnification obligations;
- Limitation of Liability provisions;
- Any provision intended to survive termination.

**8.7 Client Responsibilities Upon Termination**

Upon termination, Client shall:

- Pay all outstanding amounts due;

- Cooperate in the orderly transition of Services;
- Provide reasonable access necessary to complete agreed transition activities;
- Return any DefendIT-owned equipment, credentials, or property in its possession; and
- Designate an authorized transition contact.

**8.8 DefendIT Transition Assistance**

Upon Client's written request, DefendIT may provide reasonable transition assistance to facilitate migration to Client or a successor service provider.

Unless otherwise stated in a Service Document:

- Transition Services are not included within Monthly Recurring Services.
- Transition Services are Professional Services.
- Transition Services shall be billed at DefendIT's then-current hourly rates.
- DefendIT is not obligated to begin transition work until all undisputed invoices are paid or satisfactory payment arrangements have been made.

**8.9 Client Data**

Subject to applicable law and any mutually agreed transition plan:

- Client retains ownership of its Client Data.
- DefendIT will make Client Data available in a commercially reasonable format if it is in DefendIT's possession and not otherwise available to the Client.
- After completion of transition services, DefendIT may securely delete or destroy retained copies of Client Data in accordance with its documented retention policies, unless retention is required by law or agreed in writing.

**8.10 No Waiver**

Termination or expiration of this Agreement shall not waive any rights, claims, or remedies that accrued prior to the effective date of termination.

**8.11 Survival**

The following Articles shall survive termination or expiration:

- Fees and Payment Obligations
- Early Termination Payment
- Confidentiality
- Intellectual Property
- Data Protection
- Limitation of Liability
- Indemnification
- Governing Law
- Dispute Resolution
- Collection Costs
- Any other provision that by its nature survives termination

**ARTICLE IX**

**SERVICE LEVELS AND SUPPORT**

**9.1 General**

DefendIT Services ("DefendIT") shall provide support and Managed Services in accordance with the applicable Managed Services Schedule, Service Level Agreement ("SLA"), Statement of Work, and this Agreement.

The response objectives set forth in the applicable SLA are operational targets intended to facilitate efficient service delivery. Unless expressly stated otherwise, such objectives are not warranties or guarantees of resolution within a specified time.

**9.2 Service Desk**

Unless otherwise specified in the applicable Service Documents, DefendIT shall provide technical support during its published Business Hours.

Support may be requested through any approved communication channel, including:

- Client Portal
- Email
- Telephone
- Remote Support Platform
- Other methods designated by DefendIT

DefendIT may modify its support methods upon reasonable notice to Client.

**9.3 Incident Priorities**

Support requests shall be assigned a priority level based upon DefendIT's reasonable assessment of the operational impact to Client.

**Priority 1 – Critical**

An issue resulting in a complete or near-complete interruption of critical business operations, including but not limited to:

- Complete network outage
- Server failure affecting all users
- Ransomware attack
- Widespread Microsoft 365 outage
- Firewall failure
- Internet outage affecting the entire organization
- Critical line-of-business application unavailable for all users

**Priority 2 – High**

A significant impairment affecting multiple users or a critical business function where a reasonable workaround is not available.

Examples include:

- Email unavailable for a department
- VPN unavailable for multiple users
- Network degradation affecting productivity
- Major printing infrastructure failure

- Significant cloud application outage

**Priority 3 – Medium**

Issues affecting individual users or non-critical business functions where reasonable workarounds may exist.

Examples include:

- Individual workstation issues
- Software errors
- Printer problems
- User account issues
- Remote access issues affecting a single user

**Priority 4 – Low**

Routine requests, informational inquiries, administrative requests, scheduled work, and service requests that do not materially affect business operations.

Examples include:

- New user setup
- Password changes
- Software installation
- Equipment relocation
- General consulting
- Documentation requests

**9.4 Response Objectives**

DefendIT shall use commercially reasonable efforts to respond to support requests within the response objectives established in the applicable Service Level Agreement.

Response time means the time between DefendIT's receipt of a properly submitted support request and the initial acknowledgment by an authorized DefendIT representative.

Response time does not mean resolution time.

**9.5 Resolution Targets**

Resolution times vary based upon:

- Complexity of the issue
- Availability of Client personnel
- Third-party vendor involvement
- Hardware availability
- Manufacturer support
- Internet service providers
- Cloud providers
- Other circumstances beyond DefendIT's reasonable control

Accordingly, DefendIT does not guarantee that any issue will be resolved within a specific period unless expressly stated in a Service Document.

**9.6 Scheduled Maintenance**

DefendIT may perform routine maintenance necessary to support the Services, including:

- Security updates
- Patch deployment
- Firmware upgrades
- System optimization
- Infrastructure maintenance
- Monitoring platform maintenance

Where commercially reasonable, DefendIT shall provide advance notice of scheduled maintenance that is expected to materially affect Client operations.

**9.7 Emergency Maintenance**

DefendIT may perform emergency maintenance without prior notice when reasonably necessary to:

- Address a Security Incident;
- Mitigate an active cyber threat;
- Prevent imminent service disruption;

- Apply critical security updates;
- Protect Client Data; or
- Preserve the integrity of managed systems.

DefendIT will notify Client as soon as reasonably practicable following emergency maintenance.

**9.8 On-Site Support**

Unless otherwise specified in the applicable Managed Services Schedule, DefendIT may determine, in its reasonable discretion, whether a support issue can be resolved remotely or requires an on-site visit.

On-site support outside the scope of the Managed Services may be billed as Professional Services.

**9.9 Client Responsibilities Affecting Service Levels**

DefendIT's ability to meet service objectives depends upon Client's cooperation.

Client shall:

- Provide timely access to systems and facilities;
- Designate Authorized Contacts;
- Maintain supported hardware and software;
- Implement required security controls;
- Promptly respond to requests for information or approval; and
- Maintain internet connectivity and electrical power necessary to support the Services.

Failure to satisfy these responsibilities may affect response or resolution times.

**9.10 Service Level Exclusions**

Unless expressly included in the applicable SLA, service level commitments do not apply to delays resulting from:

- Client-caused delays;
- Third-party vendor outages;
- Internet service provider failures;

- Cloud provider outages;
- Force Majeure events;
- Cyberattacks beyond DefendIT's reasonable control;
- Unsupported Technology;
- Hardware manufacturer defects;
- Delays in obtaining replacement equipment;
- Waiting for Client approval or required information.

**9.11 Escalation**

DefendIT shall maintain internal escalation procedures for support requests requiring additional technical expertise or management involvement.

Client may request management review of unresolved support issues in accordance with DefendIT's published escalation procedures.

**9.12 Continuous Improvement**

The parties acknowledge that technology environments evolve over time.

DefendIT may recommend changes to infrastructure, security controls, licensing, staffing, or operational processes that are intended to improve service quality, reduce operational risk, or enhance cybersecurity.

Such recommendations do not modify the scope of Services unless accepted by Client in writing.

**9.13 Separate Service Level Agreement**

The detailed service levels applicable to the Services, including response objectives, support hours, maintenance windows, severity classifications, communication procedures, and any service credits (if applicable), shall be set forth in the Service Level Agreement attached as **Exhibit A**, which is incorporated into this Agreement by reference.

If there is a conflict between this Article and Exhibit A regarding operational service levels, **Exhibit A shall control** with respect to those operational matters.

**ARTICLE X**

**CYBERSECURITY AND SHARED RESPONSIBILITY**

**10.1 Purpose**

DefendIT Services ("DefendIT") provides managed cybersecurity services designed to reduce operational risk, improve security posture, and assist Client in protecting its technology environment.

The parties acknowledge that cybersecurity is a shared responsibility. No technology, software, monitoring service, or security program can eliminate all cybersecurity risk or guarantee the prevention, detection, or successful remediation of every threat, vulnerability, or Security Incident.

Accordingly, both DefendIT and Client agree to fulfill their respective responsibilities as described in this Agreement and the applicable Service Documents.

**10.2 Scope of Cybersecurity Services**

Cybersecurity Services shall consist only of those services expressly identified in the applicable Managed Services Schedule, Statement of Work, or other Service Document.

Depending upon Client's selected service plan, Cybersecurity Services may include:

- Endpoint Detection and Response (EDR)
- Managed Antivirus
- Managed Firewall Administration
- Security Monitoring
- Vulnerability Scanning
- Patch Management
- Multi-Factor Authentication (MFA) Administration
- Microsoft 365 Security Administration
- DNS Filtering
- Email Security
- Security Awareness Training
- Dark Web Monitoring
- Backup Monitoring
- Security Reporting
- Security Consulting

- Incident Response Coordination

No service shall be deemed included unless specifically identified in the applicable Service Documents.

**10.3 Shared Responsibility**

The parties acknowledge that effective cybersecurity requires cooperation.

Unless expressly delegated in writing, DefendIT is responsible only for the security services specifically identified in the applicable Service Documents.

Client remains responsible for:

- Business decisions
- Employee supervision
- Hiring and termination notifications
- Physical security
- Financial approval processes
- Wire transfer verification
- Regulatory compliance
- Data classification
- Internal policies
- User conduct
- Security awareness participation
- Timely approval of recommended security improvements

**10.4 Minimum Security Standards**

To maintain a secure and supportable technology environment, Client agrees to maintain minimum security standards reasonably required by DefendIT.

Unless otherwise approved in writing, these standards may include:

- Supported operating systems
- Vendor-supported hardware
- Multi-Factor Authentication for privileged accounts

- Endpoint protection approved by DefendIT
- Disk encryption on supported mobile devices and laptops
- Current security updates
- Supported firewall platforms
- Modern web browsers
- Secure Wi-Fi encryption
- Password policies consistent with current industry practices

DefendIT may update its Technology Standards Manual from time to time upon reasonable notice to Client.

Failure to maintain minimum standards may affect support eligibility, response objectives, or the ability of DefendIT to deliver certain Services.

**10.5 Security Recommendations**

DefendIT may provide written recommendations intended to improve the security, reliability, or resilience of Client's technology environment.

Recommendations may include:

- Hardware replacement
- Operating system upgrades
- Security configuration changes
- Software updates
- Backup improvements
- Network segmentation
- Identity and access controls
- Additional security products or services

Client acknowledges that such recommendations are based on information reasonably available at the time they are made and should not be interpreted as a guarantee against future Security Incidents.

**10.6 Client Decisions Regarding Security Recommendations**

For each material security recommendation, Client may:

- Accept the recommendation;
- Request that implementation be deferred;
- Decline the recommendation; or
- Request additional information.

DefendIT may document Client's decision within its service management system, client portal, or other business records maintained in the ordinary course of business.

If Client declines or indefinitely defers a recommendation that DefendIT reasonably believes is necessary to address a material security risk, DefendIT may request written acknowledgment of the associated risks. Such documentation is intended to clarify the parties' understanding of the identified risk and does not, by itself, relieve either party of obligations expressly assumed under this Agreement.

**10.7 Unsupported Technology**

DefendIT may designate hardware, software, operating systems, firmware, or cloud services as Unsupported Technology if they have reached end-of-life, are no longer supported by the manufacturer, or present material operational or cybersecurity risks.

DefendIT may decline to install, support, or modify Unsupported Technology or may require Client to execute a written risk acknowledgment before continuing to support such systems.

**10.8 Security Incidents**

Client shall notify DefendIT promptly after becoming aware of any suspected or actual:

- Malware infection
- Ransomware
- Unauthorized access
- Credential compromise
- Business Email Compromise
- Phishing attack
- Wire fraud attempt
- Data breach

- Loss or theft of a managed device
- Other event that could materially affect the confidentiality, integrity, or availability of Client's systems or data

Upon notification, DefendIT shall use commercially reasonable efforts to respond in accordance with the applicable Service Level Agreement and the Services purchased by Client.

**10.9 Incident Response Services**

Unless Incident Response Services are expressly included within Client's Managed Services Schedule, forensic investigations, malware eradication, ransomware recovery, legal support, breach notification assistance, regulatory reporting, and other specialized incident response activities shall be performed only pursuant to a separate Statement of Work or emergency services authorization and may be billed as Professional Services.

**10.10 No Guarantee of Cybersecurity**

Client acknowledges that cybersecurity threats continuously evolve and that no security program can guarantee the prevention, detection, or successful mitigation of every attack.

Accordingly, DefendIT does not warrant or guarantee that:

- All cyberattacks will be prevented;
- All vulnerabilities will be identified;
- All malware will be detected;
- All phishing attempts will be blocked;
- All unauthorized access will be prevented;
- Data loss will never occur; or
- Client's environment will remain free from Security Incidents.

DefendIT's obligation is to perform the contracted Services in a professional and workmanlike manner using commercially reasonable practices consistent with the applicable Service Documents.

**10.11 Business Email Compromise and Financial Fraud**

Client acknowledges that fraud schemes—including business email compromise, vendor impersonation, AI-generated voice or video impersonation, social engineering, and fraudulent payment instruction attacks—may bypass technical security controls.

Client remains responsible for implementing appropriate financial controls, including independent verification of payment instructions, changes to banking information, and high-risk financial transactions.

Unless expressly agreed in writing, DefendIT is not responsible for approving or authorizing Client financial transactions.

**10.12 Cyber Insurance**

DefendIT recommends that Client maintain appropriate cyber liability insurance and review coverage periodically with its insurance advisor.

Unless expressly agreed in writing, DefendIT does not procure, maintain, or administer cyber insurance on Client's behalf and makes no representation regarding the adequacy of any insurance coverage.

**10.13 Compliance Assistance**

Services provided under this Agreement may assist Client in supporting cybersecurity or regulatory initiatives, including those relating to recognized frameworks or industry standards.

Unless expressly stated in a signed Statement of Work, DefendIT does not represent that its Services alone will make Client compliant with any law, regulation, contractual obligation, or industry framework. Client remains responsible for determining and maintaining its own compliance obligations.

**ARTICLE XI**

**THIRD-PARTY PRODUCTS, CLOUD SERVICES, AND LICENSING**

**11.1 Third-Party Products and Services**

In performing the Services, DefendIT Services ("DefendIT") may recommend, procure, configure, administer, or support hardware, software, cloud platforms, telecommunications services, subscriptions, security solutions, or other products and services provided by third parties ("Third-Party Products").

Unless expressly stated in a Service Document, DefendIT is not the manufacturer, publisher, developer, telecommunications provider, cloud service provider, or licensor of any Third-Party Product.

**11.2 Client Selection and Authorization**

Client authorizes DefendIT to procure, configure, renew, administer, or otherwise manage Third-Party Products identified in the applicable Service Documents or otherwise approved by Client.

Client acknowledges that many Third-Party Products are subject to separate license agreements, subscription terms, acceptable use policies, and privacy policies established by the applicable vendor.

Client agrees to comply with such third-party terms to the extent they apply to Client's use of the applicable products or services.

**11.3 Vendor Terms Control**

The use of any Third-Party Product remains subject to the applicable vendor's licensing and contractual terms.

Nothing in this Agreement modifies, replaces, or supersedes the contractual obligations between Client and the applicable third-party vendor.

Where a conflict exists between this Agreement and mandatory vendor licensing requirements, the applicable vendor licensing requirements shall control with respect to that Third-Party Product.

**11.4 Availability of Third-Party Services**

DefendIT does not control the operation, availability, security, maintenance schedules, pricing, or future development of Third-Party Products.

Accordingly, DefendIT shall not be responsible for delays, interruptions, degradation of service, outages, discontinued products, licensing changes, or other events resulting from the acts or omissions of third-party vendors.

Examples include, without limitation:

- Cloud service outages;
- Internet service provider failures;
- Software defects;
- Manufacturer recalls;
- Vendor maintenance windows;
- API changes;
- Licensing modifications;

- Product discontinuation;
- Changes to vendor support policies.

**11.5 Licensing**

Unless expressly agreed otherwise in writing:

a. Client is the licensee of all software licenses, cloud subscriptions, and vendor agreements purchased for Client's benefit.

b. Client is responsible for maintaining sufficient licensing to support its users, devices, and workloads.

c. DefendIT may rely upon information supplied by Client or the applicable vendor when administering licenses.

d. DefendIT is not responsible for vendor licensing audits or penalties arising from inaccurate information supplied by Client or from Client's unauthorized use of licensed software.

**11.6 Microsoft and Cloud Services**

Where DefendIT provides services involving Microsoft 365, Microsoft Azure, Google Workspace, Amazon Web Services, or other cloud platforms, DefendIT shall provide only those management and administration services expressly identified in the applicable Service Documents.

Client acknowledges that:

- cloud providers retain control over their platforms;
- platform functionality may change without notice to DefendIT;
- vendors may discontinue features or products;
- pricing and licensing may change during the term of this Agreement; and
- vendor outages may occur despite commercially reasonable efforts by both DefendIT and the vendor.

**11.7 Vendor Changes**

DefendIT may recommend replacing or migrating Third-Party Products when, in its reasonable judgment:

- a product reaches end of life;
- vendor support is discontinued;
- significant security concerns arise;
- licensing materially changes;
- operational reliability materially declines; or
- a replacement is reasonably necessary to continue delivering the contracted Services.

Implementation of replacement products may require Client approval and may be subject to additional fees unless otherwise included in the applicable Service Documents.

**11.8 Hardware Procurement**

Unless otherwise agreed in writing:

- Hardware purchases are non-cancelable after an order has been submitted to the manufacturer or distributor.
- Delivery dates are estimates only.
- Shipping delays remain the responsibility of the applicable supplier.
- Manufacturer warranties are provided solely by the manufacturer unless DefendIT expressly agrees otherwise in writing.

Risk of loss shall transfer to Client upon delivery to Client's designated location or authorized recipient.

**11.9 Third-Party Warranties**

DefendIT does not independently warrant Third-Party Products.

Any warranties applicable to Third-Party Products are provided solely by the applicable manufacturer, publisher, cloud provider, or other vendor.

To the extent commercially reasonable, DefendIT will assist Client in coordinating warranty claims covered by a vendor's warranty, provided such assistance is within the scope of the Services or is otherwise authorized as Professional Services.

**11.10 Subscription Renewals**

Where DefendIT manages recurring subscriptions on Client's behalf, Client authorizes DefendIT to renew such subscriptions as required to avoid interruption of Services, unless

Client provides written notice of non-renewal within the notice period specified in the applicable Service Documents or vendor agreement.

Client remains responsible for all vendor-imposed minimum commitments, non-cancelable subscription terms, and early termination charges associated with Third-Party Products.

**11.11 Open Source Software**

Certain Third-Party Products may include or depend upon open-source software licensed under separate open-source license terms.

Nothing in this Agreement expands or restricts Client's rights or obligations under any applicable open-source license.

**11.12 Reservation of Rights**

DefendIT reserves the right to decline to procure, support, or administer any Third-Party Product that DefendIT reasonably determines:

- presents a material cybersecurity risk;
- is no longer commercially supported;
- is incompatible with Client's managed environment;
- materially interferes with DefendIT's ability to deliver the Services; or
- would require DefendIT to violate applicable law, licensing requirements, or professional obligations.

**ARTICLE XII**

**CONFIDENTIALITY**

**12.1 Definition of Confidential Information**

For purposes of this Agreement, **"Confidential Information"** means any non-public information disclosed by one party ("Disclosing Party") to the other party ("Receiving Party"), whether in written, electronic, oral, visual, or other form, that is designated as confidential or that reasonably should be understood to be confidential based on the nature of the information or the circumstances of its disclosure.

Confidential Information includes, without limitation:

- Business plans and strategies;

- Financial information;
- Customer and vendor information;
- Pricing and proposals;
- Technical documentation;
- Network diagrams;
- System configurations;
- Security policies and procedures;
- User credentials and authentication information;
- Encryption keys and certificates;
- Source code, software, and proprietary technology;
- Personal Information and protected data;
- Security assessments, audit reports, and vulnerability information;
- Incident reports and forensic findings; and
- Any information identified as confidential in the applicable Service Documents.

**12.2 Exclusions**

Confidential Information does not include information that the Receiving Party can demonstrate:

a. Was publicly available through no wrongful act of the Receiving Party;

b. Was lawfully known by the Receiving Party before disclosure;

c. Was independently developed without reference to the Disclosing Party's Confidential Information; or

d. Was lawfully obtained from a third party without restriction on disclosure.

**12.3 Confidentiality Obligations**

The Receiving Party shall:

- Use Confidential Information solely for purposes of performing or receiving the Services;

- Protect Confidential Information using at least the same degree of care it uses to protect its own confidential information of a similar nature, but no less than a commercially reasonable standard of care;
- Restrict access to those employees, contractors, or professional advisors who have a legitimate need to know and who are bound by confidentiality obligations no less protective than those contained in this Agreement; and
- Not disclose Confidential Information except as permitted by this Agreement or with the prior written consent of the Disclosing Party.

**12.4 Protection of Credentials**

Client acknowledges that DefendIT may receive administrative credentials, privileged access, encryption keys, certificates, and other sensitive authentication materials necessary to perform the Services.

DefendIT shall maintain commercially reasonable administrative, technical, and physical safeguards to protect such information from unauthorized access, use, or disclosure while in its possession or control.

**12.5 Permitted Disclosures**

The Receiving Party may disclose Confidential Information:

- To its employees, contractors, auditors, insurers, legal counsel, accountants, or other professional advisors who require access for purposes related to this Agreement and who are subject to appropriate confidentiality obligations;
- As required by applicable law, court order, subpoena, or governmental authority; or
- As otherwise expressly authorized in writing by the Disclosing Party.

Where legally permitted, the Receiving Party shall provide prompt notice of any legally compelled disclosure to allow the Disclosing Party an opportunity to seek a protective order or other appropriate remedy.

**12.6 Security of Confidential Information**

Each party shall implement and maintain commercially reasonable safeguards appropriate to the nature of the Confidential Information under its control.

Such safeguards may include, as appropriate:

- Access controls;
- Multi-factor authentication;
- Encryption where commercially reasonable;
- Secure credential management;
- Endpoint protection;
- Logging and monitoring;
- Personnel security practices; and
- Secure disposal procedures.

Neither party guarantees that its safeguards will prevent every unauthorized access or Security Incident.

**12.7 Security Incidents Involving Confidential Information**

If either party becomes aware of unauthorized access to the other party's Confidential Information that may materially affect the confidentiality, integrity, or availability of such information, that party shall notify the other without unreasonable delay after confirming the incident and shall cooperate in good faith regarding reasonable mitigation efforts, consistent with applicable law and contractual obligations.

**12.8 Return or Destruction of Confidential Information**

Upon termination of this Agreement or upon written request, the Receiving Party shall, within a commercially reasonable time:

- Return the Disclosing Party's Confidential Information;
- Securely destroy such information; or
- Continue to retain such information only to the extent required by applicable law, professional obligations, disaster recovery practices, backup retention schedules, or legitimate business recordkeeping requirements.

Routine backup copies created through automated backup processes may be retained until overwritten or deleted in the ordinary course of business, provided they remain subject to the confidentiality obligations of this Agreement.

**12.9 Ownership**

All Confidential Information remains the exclusive property of the Disclosing Party.

No license, ownership interest, intellectual property right, or other proprietary interest is transferred by the disclosure of Confidential Information except as expressly provided in this Agreement.

**12.10 Equitable Relief**

The parties acknowledge that unauthorized use or disclosure of Confidential Information may cause irreparable harm for which monetary damages alone may be an inadequate remedy.

Accordingly, in addition to any other remedies available at law or in equity, the injured party may seek temporary, preliminary, or permanent injunctive or other equitable relief to prevent or limit any actual or threatened unauthorized disclosure or misuse of Confidential Information, subject to applicable law.

**12.11 Survival**

The obligations contained in this Article shall survive the expiration or termination of this Agreement for a period of **five (5) years**, except that obligations relating to trade secrets shall continue for so long as such information remains protected as a trade secret under applicable law.

**ARTICLE XIII**

**DATA PROTECTION AND PRIVACY**

**13.1 Ownership of Client Data**

As between the parties, Client retains all right, title, and interest in and to its data, records, files, databases, electronic communications, and other information provided to or generated through the Services ("Client Data").

Except as expressly provided in this Agreement, nothing herein transfers ownership of Client Data to DefendIT Services ("DefendIT").

**13.2 Limited Right to Process Client Data**

Client grants DefendIT a limited, non-exclusive right to access, process, store, transmit, and otherwise use Client Data solely as reasonably necessary to:

- Perform the Services;
- Maintain and secure Client's technology environment;
- Troubleshoot and resolve technical issues;

- Provide monitoring and reporting;
- Perform backup and recovery services, if contracted;
- Comply with applicable law; and
- Fulfill other obligations expressly described in this Agreement or the applicable Service Documents.

DefendIT shall not use Client Data for marketing purposes or sell Client Data to third parties.

**13.3 Privacy Compliance**

Each party shall remain independently responsible for complying with privacy and data protection laws applicable to its own business activities.

Unless expressly agreed in a separate written agreement, including a Business Associate Agreement ("BAA") or Data Processing Addendum ("DPA"), DefendIT does not assume the role of a data controller, business associate, or similar regulated entity solely by providing the Services.

Where a BAA, DPA, or similar agreement is required by law or contract, the parties shall execute such agreement before DefendIT performs services requiring those obligations.

**13.4 Client Responsibilities**

Client is solely responsible for:

- Determining the legal basis for collecting and processing Client Data;
- Providing required privacy notices;
- Obtaining any necessary consents or authorizations;
- Responding to requests from data subjects, customers, employees, or regulators;
- Classifying the sensitivity of Client Data;
- Determining applicable legal, regulatory, and contractual requirements for its data.

DefendIT may reasonably rely upon Client's instructions regarding the handling of Client Data unless such instructions would violate applicable law.

**13.5 Security Measures**

DefendIT shall maintain commercially reasonable administrative, technical, and physical safeguards designed to protect Client Data against unauthorized access, use, alteration, disclosure, or destruction while under DefendIT's control.

Such safeguards may include, where appropriate:

- Multi-factor authentication;
- Encryption of data in transit using industry-standard protocols;
- Encryption of stored data where commercially reasonable and technically feasible;
- Role-based access controls;
- Logging and monitoring of administrative access;
- Endpoint protection;
- Secure credential management; and
- Security awareness training for personnel with access to Client Data.

The parties acknowledge that no security measures can guarantee absolute protection against all threats.

**13.6 Authorized Personnel and Subcontractors**

DefendIT may permit its employees, contractors, affiliates, and approved subcontractors to access Client Data only to the extent reasonably necessary to perform the Services.

DefendIT shall require such personnel and subcontractors to be bound by confidentiality and security obligations appropriate to the nature of the Services.

DefendIT remains responsible for the performance of its subcontractors to the same extent it would be responsible for its own personnel under this Agreement.

**13.7 Security Incidents Affecting Client Data**

If DefendIT becomes aware of a confirmed Security Incident involving Client Data under its control that is reasonably likely to require notification under applicable law, DefendIT shall notify Client without unreasonable delay after confirming the incident.

Such notice shall include, to the extent reasonably available:

- A general description of the incident;
- The categories of Client Data affected, if known;

- The measures taken or planned to contain and remediate the incident; and
- Information reasonably necessary to assist Client in meeting any legal notification obligations.

DefendIT shall cooperate with Client in responding to the incident, provided that such cooperation beyond the scope of the contracted Services may be treated as Professional Services.

**13.8 Regulatory Notifications**

Unless otherwise required by law or expressly agreed in writing, Client is solely responsible for:

- Determining whether regulatory notifications are required;
- Notifying affected individuals;
- Communicating with regulators;
- Communicating with customers, vendors, insurers, or other third parties; and
- Retaining legal counsel regarding any actual or suspected data breach.

DefendIT shall not make public statements or regulatory notifications on Client's behalf unless expressly authorized in writing or required by applicable law.

**13.9 Backup and Disaster Recovery**

Unless expressly included in the applicable Service Documents:

- DefendIT does not guarantee that all Client Data can be restored following a system failure, cyberattack, hardware failure, software corruption, or disaster.
- Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) apply only if expressly identified in the applicable Service Level Agreement or Statement of Work.
- Client is responsible for validating that backup retention schedules, recovery objectives, and disaster recovery capabilities satisfy its operational and regulatory requirements.

Where backup services are provided, Client agrees to participate in periodic restoration testing at intervals mutually agreed upon by the parties.

**13.10 Data Retention and Secure Deletion**

During the term of this Agreement, DefendIT shall retain Client Data only as reasonably necessary to perform the Services or as otherwise required by law, contractual obligation, or documented retention policies.

Following termination of the Agreement and completion of any agreed transition services:

- DefendIT may securely delete Client Data remaining in its systems after providing Client a reasonable opportunity to retrieve such data, unless continued retention is required by law or agreed in writing.
- Automated backup copies may remain until overwritten or deleted in accordance with normal backup retention cycles.

**13.11 Cross-Border Processing**

Unless otherwise agreed in writing, Client acknowledges that certain cloud providers, software vendors, and infrastructure providers used in connection with the Services may process or store Client Data in multiple geographic locations.

DefendIT shall use commercially reasonable efforts to select reputable service providers and to disclose material cross-border processing arrangements where required by applicable law or contract.

**13.12 Audit Requests**

If Client is subject to a legal, regulatory, or contractual audit relating to the Services, DefendIT shall reasonably cooperate by providing available documentation concerning its security and operational practices.

Unless otherwise included in the applicable Service Documents:

- extensive audit questionnaires;
- on-site assessments;
- custom compliance reporting; and
- participation in third-party audits

may be billed as Professional Services.

**13.13 Survival**

The obligations contained in this Article shall survive the expiration or termination of this Agreement for so long as DefendIT retains Client Data or is otherwise required by law or contract to protect such information.

**ARTICLE XIV**

**INTELLECTUAL PROPERTY**

**14.1 Ownership of Pre-Existing Intellectual Property**

Each party retains all right, title, and interest in and to its respective intellectual property, including any copyrights, trademarks, patents, trade secrets, software, documentation, methodologies, know-how, templates, processes, inventions, and other proprietary materials developed, owned, or licensed by that party prior to the Effective Date or independently of this Agreement ("Pre-Existing Intellectual Property").

Nothing in this Agreement transfers ownership of either party's Pre-Existing Intellectual Property except as expressly provided herein.

**14.2 Client Property**

As between the parties, Client retains all right, title, and interest in and to:

- Client Data;
- Client trademarks, trade names, logos, and branding;
- Client business records;
- Client documentation;
- Client-created software and content; and
- Any other intellectual property owned or licensed by Client prior to or independently of this Agreement.

Except as necessary to perform the Services, DefendIT acquires no ownership interest in Client's intellectual property.

**14.3 DefendIT Property**

DefendIT retains exclusive ownership of its:

- Service methodologies;
- Automation scripts;
- Security playbooks;
- Monitoring configurations;
- Standard operating procedures;

- Templates;
- Checklists;
- Documentation formats;
- Proprietary tools;
- Dashboards;
- Reporting formats;
- Internal knowledge base;
- Service management processes;
- Software developed by or for DefendIT; and
- Any improvements, enhancements, modifications, or derivative works thereof.

The use of DefendIT's intellectual property in providing the Services does not grant Client any ownership interest therein.

**14.4 Deliverables**

Upon payment in full of all amounts due, Client shall own the final deliverables specifically identified in an applicable Statement of Work as being transferred to Client, unless otherwise provided in that Statement of Work.

Unless expressly stated otherwise, deliverables do **not** include DefendIT's:

- Internal methodologies;
- Scripts;
- Automation tools;
- Proprietary software;
- Templates;
- Security procedures;
- Internal documentation;
- Monitoring configurations; or

- Other proprietary materials used in developing the deliverable.

DefendIT retains ownership of such materials even if incorporated into or used to create a deliverable.

**14.5 Limited License to Client**

During the term of this Agreement, DefendIT grants Client a limited, non-exclusive, non-transferable, revocable license to use documentation, reports, and other materials provided by DefendIT solely for Client's internal business operations and only in connection with the Services.

Client shall not:

- Copy, distribute, sublicense, or publish DefendIT's proprietary materials except for internal business purposes;
- Reverse engineer or attempt to extract DefendIT's proprietary methodologies;
- Remove proprietary notices; or
- Use DefendIT's intellectual property to provide services to third parties.

**14.6 License to DefendIT**

Client grants DefendIT a limited, non-exclusive license to use Client's trademarks, logos, trade names, documentation, software, and Client Data solely as reasonably necessary to perform the Services under this Agreement.

This license automatically terminates upon expiration or termination of the Agreement, except to the extent continued use is required to complete transition services, satisfy legal obligations, or comply with documented record-retention requirements.

**14.7 Feedback**

If Client voluntarily provides suggestions, recommendations, enhancement requests, or other feedback regarding the Services, DefendIT may use, modify, and incorporate such feedback into its services and operations without restriction or obligation, provided that doing so does not disclose Client's Confidential Information or identify Client without prior written consent.

**14.8 Open Source and Third-Party Software**

Nothing in this Agreement transfers ownership of any third-party or open-source software.

Use of such software remains subject to the applicable license terms established by the respective owner or licensor.

**14.9 Intellectual Property Infringement**

Each party represents that it has the authority to provide the intellectual property it supplies in connection with the Services.

If either party becomes aware of a claim alleging that materials it has provided infringe a third party's intellectual property rights, that party shall promptly notify the other and cooperate in good faith regarding the defense or resolution of the claim.

The parties' respective indemnification obligations relating to intellectual property claims are governed by **Article XVII (Indemnification)**.

**14.10 Reservation of Rights**

Except for the limited licenses expressly granted in this Agreement, no license, ownership interest, or other right in any intellectual property is granted by implication, estoppel, or otherwise.

All rights not expressly granted are reserved by the respective owner.

**14.11 Survival**

The ownership provisions, license restrictions, confidentiality obligations relating to intellectual property, accrued payment obligations, and any provisions that by their nature are intended to survive shall remain in effect following the expiration or termination of this Agreement.

**ARTICLE XV**

**WARRANTIES AND DISCLAIMERS**

**15.1 Professional Services Warranty**

DefendIT Services ("DefendIT") warrants that it will perform the Services in a professional and workmanlike manner, consistent with generally accepted industry standards applicable to managed information technology and cybersecurity service providers.

If Client believes DefendIT has materially failed to meet this warranty, Client shall provide written notice describing the alleged deficiency within thirty (30) days after discovering it.

DefendIT shall be afforded a reasonable opportunity to investigate and, if applicable, re-perform the affected Services or otherwise cure the deficiency.

The remedies described in this Section constitute Client's exclusive remedy for a breach of the foregoing warranty.

**15.2 Authorized Personnel**

DefendIT warrants that personnel assigned to perform the Services shall possess qualifications, training, and experience reasonably appropriate for the services being performed.

DefendIT may assign or replace personnel in its reasonable discretion, provided that such changes do not materially diminish the quality of the Services.

**15.3 Compliance with Law**

Each party represents that it shall perform its obligations under this Agreement in compliance with laws and regulations applicable to its own business activities.

Nothing in this Agreement shall be construed as a warranty that the Services alone will satisfy Client's legal, regulatory, contractual, insurance, or industry-specific compliance obligations unless expressly stated in a signed Statement of Work.

**15.4 Third-Party Products**

DefendIT does not manufacture, publish, operate, or control Third-Party Products used in connection with the Services.

Accordingly, DefendIT makes no warranty regarding:

- Third-party software;
- Cloud platforms;
- Internet services;
- Telecommunications services;
- Hardware manufacturers;
- Software publishers;
- Security vendors; or
- Other third-party products or services.

Any warranties relating to Third-Party Products are provided solely by the applicable vendor, manufacturer, or licensor.

**15.5 Availability of Services**

DefendIT shall use commercially reasonable efforts to provide the Services in accordance with the applicable Service Documents.

However, DefendIT does not warrant that:

- Services will be uninterrupted;
- Services will be continuously available;
- Services will be free from delays;
- All defects will be corrected immediately;
- Every issue can be resolved remotely; or
- Every support request can be completed within a particular timeframe unless expressly stated in the applicable Service Level Agreement.

Scheduled maintenance, emergency maintenance, third-party outages, and events beyond DefendIT's reasonable control may affect service availability.

**15.6 Cybersecurity**

Client acknowledges that cybersecurity threats continually evolve.

Accordingly, DefendIT does not warrant or guarantee that:

- Every cyberattack will be prevented;
- Every vulnerability will be discovered;
- Every malicious email will be blocked;
- Every phishing attempt will be detected;
- Every unauthorized access attempt will be prevented;
- Every Security Incident will be avoided;
- Every backup will be recoverable under all circumstances; or
- Client's systems will remain free from malware, ransomware, or other malicious activity.

DefendIT warrants only that it will perform the contracted cybersecurity services using commercially reasonable practices consistent with the applicable Service Documents.

**15.7 Client Environment**

DefendIT's ability to perform the Services depends upon the condition of Client's technology environment.

DefendIT does not warrant the performance, stability, compatibility, or security of:

- Unsupported hardware or software;
- End-of-life systems;
- Unlicensed software;
- Systems modified by unauthorized third parties;
- Client-developed applications;
- Third-party customizations;
- Internet connectivity provided by third parties; or
- Technology that Client has directed DefendIT not to upgrade, replace, or secure despite documented recommendations.

**15.8 No Warranty of Business Results**

DefendIT does not warrant that the Services will:

- Increase revenue;
- Prevent all business interruptions;
- Eliminate operational risk;
- Guarantee regulatory compliance;
- Ensure insurance coverage;
- Prevent financial fraud;
- Eliminate employee error; or
- Produce any particular business outcome.

Client remains responsible for its own business operations, management decisions, internal controls, and compliance obligations.

**15.9 Disclaimer of Implied Warranties**

**EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THIS AGREEMENT, THE SERVICES, SOFTWARE, DELIVERABLES, DOCUMENTATION, AND ALL RELATED MATERIALS ARE PROVIDED "AS IS" AND "AS AVAILABLE."**

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, DEFENDIT DISCLAIMS ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING ANY IMPLIED WARRANTIES OF:

- MERCHANTABILITY;
- FITNESS FOR A PARTICULAR PURPOSE;
- TITLE;
- NON-INFRINGEMENT; AND
- ANY WARRANTIES ARISING FROM COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE OF TRADE.

Nothing in this Agreement excludes any warranty that cannot lawfully be excluded under applicable law.

**15.10 Exclusive Remedies**

If DefendIT breaches an express warranty contained in this Agreement, DefendIT shall, at its option:

- Re-perform the affected Services;
- Correct the applicable deficiency;
- Provide a commercially reasonable workaround; or
- Refund the fees paid for the specific non-conforming Services.

These remedies constitute Client's exclusive remedies for any breach of warranty.

**15.11 Survival**

The disclaimers, limitations, and exclusive remedies contained in this Article shall survive the expiration or termination of this Agreement to the extent permitted by applicable law.

**ARTICLE XVI**

**LIMITATION OF LIABILITY**

**16.1 Allocation of Risk**

The parties acknowledge that the fees charged under this Agreement reflect the allocation of risk between the parties. The limitations, exclusions, and disclaimers contained in this Agreement are a material basis upon which the parties have entered into this Agreement and are an essential element of the pricing and commercial terms.

**16.2 Limitation of Liability**

**TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW**, THE AGGREGATE LIABILITY OF DEFENDIT SERVICES ("DEFENDIT"), ITS AFFILIATES, OWNERS, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, AND SUBCONTRACTORS ARISING OUT OF OR RELATING TO THIS AGREEMENT, WHETHER BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, STATUTE, OR ANY OTHER LEGAL THEORY, SHALL NOT EXCEED THE TOTAL RECURRING SERVICE FEES PAID BY CLIENT TO DEFENDIT UNDER THIS AGREEMENT DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM.

If the claim arises before twelve (12) months of Services have been provided, the liability cap shall equal the total fees actually paid by Client under this Agreement before the event giving rise to the claim.

**16.3 Excluded Damages**

TO THE MAXIMUM EXTENT PERMITTED BY LAW, DEFENDIT SHALL NOT BE LIABLE FOR ANY:

- Indirect damages;
- Incidental damages;
- Consequential damages;
- Special damages;
- Exemplary damages;
- Punitive damages;
- Loss of anticipated profits;
- Loss of revenue;
- Loss of business opportunity;
- Loss of goodwill;

- Loss of use;
- Loss of productivity;
- Loss of reputation;
- Loss of data, except to the extent directly caused by DefendIT's failure to perform contracted backup or data recovery services expressly included in the applicable Service Documents; or
- Costs associated with substitute technology, substitute services, or business interruption.

This exclusion applies regardless of whether DefendIT was advised of the possibility of such damages.

**16.4 Third-Party Events**

DefendIT shall not be liable for losses arising from the acts or omissions of third parties beyond DefendIT's reasonable control, including:

- Cloud service providers;
- Internet service providers;
- Telecommunications carriers;
- Software publishers;
- Hardware manufacturers;
- Managed service dependencies not provided by DefendIT;
- Utility providers; or
- Other third-party vendors.

**16.5 Cybersecurity Events**

Client acknowledges that cybersecurity threats cannot be completely eliminated.

Except to the extent caused by DefendIT's gross negligence, willful misconduct, or breach of an express contractual obligation, DefendIT shall not be liable for losses arising from:

- Zero-day vulnerabilities;
- Nation-state attacks;
- Ransomware;

- Malware;
- Phishing;
- Business Email Compromise;
- Social engineering;
- Credential theft;
- Insider threats;
- Distributed denial-of-service attacks;
- Artificial intelligence-enabled attacks; or
- Other malicious activities that could not reasonably have been prevented through the contracted Services performed in a professional and workmanlike manner.

**16.6 Client Decisions**

DefendIT shall not be liable for damages arising from:

- Client's failure to implement recommended security measures;
- Client's delay in approving recommended remediation;
- Client's continued use of Unsupported Technology;
- Client's failure to maintain appropriate backups where backup services are not included;
- Client's failure to follow documented security procedures;
- Unauthorized actions of Client personnel; or
- Client's failure to maintain appropriate internal financial or operational controls.

**16.7 Multiple Claims**

For purposes of applying the liability limitation contained in this Article, all claims arising out of the same event, series of related events, or substantially similar acts or omissions shall be treated as a single claim.

**16.8 Time Limitation for Claims**

To the maximum extent permitted by applicable law, no action arising out of or relating to this Agreement may be commenced more than **two (2) years** after the party bringing the claim knew or reasonably should have known of the facts giving rise to the claim.

This limitation shall not apply where a longer period is required by non-waivable law.

**16.9 Exceptions**

The limitations contained in this Article shall **not** apply to:

- A party's fraud or fraudulent misrepresentation;
- A party's willful misconduct;
- A party's gross negligence, to the extent such limitations are unenforceable under applicable law;
- A party's obligation to pay amounts properly due under this Agreement; or
- Any liability that cannot lawfully be limited or excluded.

The parties acknowledge that other obligations, including confidentiality and indemnification, may be subject to separate provisions elsewhere in this Agreement.

**16.10 Exclusive Allocation of Risk**

Client acknowledges that:

- The Services reduce operational and cybersecurity risk but cannot eliminate all risk;
- Client is responsible for maintaining appropriate insurance, including cyber liability insurance where appropriate;
- The pricing of the Services reflects the limitations of liability contained in this Agreement; and
- DefendIT would not enter into this Agreement on the same commercial terms without these limitations.

**16.11 Survival**

The provisions of this Article shall survive the expiration or termination of this Agreement and shall apply to any claim arising out of or relating to the Services provided under this Agreement, regardless of when such claim is asserted.

**ARTICLE XVII**

**INDEMNIFICATION**

**17.1 Mutual Indemnification**

Each party ("Indemnifying Party") shall indemnify, defend, and hold harmless the other party, together with its respective owners, officers, directors, employees, agents, successors, and permitted assigns ("Indemnified Party"), from and against any third-party claim, demand, action, proceeding, judgment, settlement, liability, damage, loss, fine, penalty, cost, or expense, including reasonable attorneys' fees, to the extent arising from:

- The Indemnifying Party's breach of this Agreement;
- The Indemnifying Party's gross negligence or willful misconduct;
- The Indemnifying Party's violation of applicable law; or
- Any matter for which indemnification is expressly provided elsewhere in this Agreement.

The obligations contained in this Article are subject to the procedures and limitations set forth below.

**17.2 Client Indemnification**

Client shall indemnify, defend, and hold harmless DefendIT Services ("DefendIT") and its affiliates, officers, directors, employees, agents, subcontractors, and representatives from and against any third-party claim arising out of or relating to:

- Client's breach of this Agreement or any Service Document;
- Client's violation of applicable law or regulation;
- Client's misuse of the Services;
- Client's unauthorized, unlawful, or infringing content, software, or data;
- Client's failure to obtain required licenses, permissions, or consents;
- Client's failure to implement required security measures after documented notice where such failure materially contributed to the claim;
- Client's negligence or willful misconduct; or
- Instructions provided by Client that DefendIT reasonably advised could create legal, operational, or cybersecurity risks, where Client nevertheless directed DefendIT to proceed.

**17.3 DefendIT Indemnification**

DefendIT shall indemnify, defend, and hold harmless Client and its officers, directors, employees, and agents from third-party claims arising directly from:

- DefendIT's gross negligence;
- DefendIT's willful misconduct;
- DefendIT's material violation of applicable law in performing the Services; or
- A claim that DefendIT's proprietary software or materials, when used by Client as authorized under this Agreement, infringe a United States patent, copyright, trademark, or trade secret.

DefendIT shall have no indemnification obligation for claims arising from:

- Client's modification of DefendIT materials;
- Combination of DefendIT materials with products or services not supplied or approved by DefendIT, where the combination gives rise to the claim;
- Client's continued use of materials after receiving notice of an alleged infringement and reasonable replacement alternatives have been offered;
- Third-Party Products; or
- Client's misuse of the Services.

**17.4 Intellectual Property Claims**

If a third party asserts that DefendIT's proprietary materials infringe its intellectual property rights, DefendIT may, at its option and expense:

- Obtain the right for Client to continue using the affected materials;
- Modify the affected materials so they become non-infringing while preserving substantially equivalent functionality;
- Replace the affected materials with functionally comparable materials; or
- Terminate the affected portion of the Services and refund any prepaid fees allocable to the unused portion of the affected Services.

These remedies constitute Client's exclusive remedies for third-party intellectual property infringement claims relating to DefendIT's proprietary materials.

**17.5 Conditions of Indemnification**

An Indemnified Party seeking indemnification shall:

a. Provide the Indemnifying Party with prompt written notice of the claim, provided that a failure to give prompt notice shall not relieve the Indemnifying Party of its obligations except to the extent it is materially prejudiced by the delay;

b. Permit the Indemnifying Party to assume control of the defense and settlement of the claim, subject to this Article; and

c. Provide reasonable cooperation, information, and assistance in the defense of the claim, at the Indemnifying Party's expense for reasonable out-of-pocket costs incurred at the Indemnifying Party's request.

**17.6 Control of Defense**

The Indemnifying Party shall have the right to control the defense and settlement of any indemnified claim using counsel of its choosing.

The Indemnified Party may participate in the defense with counsel of its own choosing at its own expense.

The Indemnifying Party shall not settle any claim in a manner that:

- Admits liability on behalf of the Indemnified Party;
- Requires the Indemnified Party to make any payment;
- Imposes ongoing obligations on the Indemnified Party; or
- Adversely affects the Indemnified Party's rights,

without the Indemnified Party's prior written consent, which shall not be unreasonably withheld, conditioned, or delayed.

**17.7 Exclusions**

Neither party shall have an obligation to indemnify the other for claims arising solely from:

- The negligence or willful misconduct of the Indemnified Party;
- Matters expressly assumed by the Indemnified Party under this Agreement;
- Third-party products or services not supplied or managed by the Indemnifying Party, except as otherwise expressly stated in this Agreement; or
- Events for which liability is otherwise excluded under Article XVI (Limitation of Liability), to the extent permitted by applicable law.

**17.8 Insurance and Indemnification**

Each party shall remain responsible for maintaining any insurance required under this Agreement.

The existence of insurance shall not limit or expand either party's indemnification obligations unless expressly stated in this Agreement.

**17.9 Exclusive Remedy for Third-Party Claims**

Except where prohibited by applicable law, this Article establishes the exclusive procedures and remedies between the parties for third-party claims subject to indemnification under this Agreement.

Nothing in this Article limits either party's right to pursue direct claims against the other for breach of this Agreement.

**17.10 Survival**

The obligations contained in this Article shall survive the expiration or termination of this Agreement with respect to claims arising from acts or omissions occurring during the term of this Agreement.

**ARTICLE XVIII**

**INSURANCE**

**18.1 Insurance Coverage**

Each party shall maintain, at its own expense, insurance coverage that is commercially reasonable and appropriate for the nature and size of its business operations.

Such coverage shall be maintained with insurers authorized to conduct business in the applicable jurisdiction or otherwise possessing a commercially reasonable financial rating.

**18.2 DefendIT Insurance**

During the term of this Agreement, DefendIT Services ("DefendIT") shall maintain commercially reasonable insurance coverage, which may include, as appropriate:

- Commercial General Liability Insurance;
- Technology Errors and Omissions (Professional Liability) Insurance;
- Cyber Liability Insurance;

- Workers' Compensation Insurance as required by applicable law; and
- Employer's Liability Insurance, where applicable.

The specific limits and terms of such insurance shall be determined by DefendIT in its reasonable business judgment.

**18.3 Client Insurance**

Client shall maintain insurance reasonably appropriate for its business operations and risk profile.

Depending upon Client's industry and operations, such insurance may include:

- Commercial General Liability;
- Property Insurance;
- Business Interruption Insurance;
- Cyber Liability Insurance;
- Crime or Employee Dishonesty Insurance;
- Professional Liability Insurance; and
- Any insurance required by applicable law or contractual obligation.

Client acknowledges that DefendIT is not acting as Client's insurance advisor and makes no representation regarding the adequacy of Client's insurance coverage.

**18.4 Cyber Liability Insurance**

Because cybersecurity incidents may result in substantial financial loss, regulatory obligations, business interruption, and third-party claims, DefendIT recommends that Client maintain cyber liability insurance appropriate to its operations.

Unless expressly agreed in writing, DefendIT does not procure, maintain, administer, or monitor insurance coverage on Client's behalf.

Client remains solely responsible for:

- Selecting appropriate insurance coverage;
- Reviewing policy limits and exclusions;
- Complying with policy conditions;
- Providing required notices to insurers; and

- Pursuing insurance claims.

**18.5 Certificates of Insurance**

Upon reasonable written request, either party shall provide a certificate of insurance or other reasonable evidence demonstrating the existence of insurance required under this Article, subject to the confidentiality obligations of this Agreement.

The obligation to provide evidence of insurance shall not require disclosure of policy terms, limits, deductibles, premiums, endorsements, or other proprietary insurance information except as required by law or mutually agreed in writing.

**18.6 No Limitation of Liability**

The existence or amount of insurance maintained by either party shall not:

- Expand that party's contractual obligations;
- Increase the liability of either party;
- Waive any limitation of liability or disclaimer contained in this Agreement; or
- Create any rights in favor of third parties.

Insurance is intended solely as a financial resource and shall not alter the allocation of risk established by this Agreement.

**18.7 Changes in Coverage**

Each party shall promptly notify the other if it becomes aware that insurance required by this Article has been materially reduced, canceled, or allowed to lapse in a manner that materially affects its ability to perform its obligations under this Agreement.

**18.8 Subcontractors**

DefendIT may satisfy portions of its insurance obligations through policies maintained by affiliated entities or by requiring subcontractors performing Services to maintain insurance appropriate to the services they provide.

DefendIT remains responsible for the performance of its subcontractors as provided elsewhere in this Agreement.

**18.9 Waiver of Subrogation**

To the extent permitted by applicable law and the parties' respective insurance policies, each party waives, and shall cause its insurers to waive, any rights of subrogation against

the other party for losses covered by insurance, except where such waiver would invalidate or materially impair available insurance coverage.

**18.10 Survival**

The obligations under this Article shall survive termination of this Agreement only to the extent necessary to address claims arising from acts or omissions occurring during the term of this Agreement.

**ARTICLE XIX**

**FORCE MAJEURE**

**19.1 Force Majeure Event**

Neither party shall be liable for any delay or failure in performing its obligations under this Agreement, other than the obligation to pay amounts properly due, to the extent such delay or failure is caused by a **Force Majeure Event** beyond the reasonable control of the affected party.

A **Force Majeure Event** includes, without limitation:

- Acts of God;
- Hurricanes, tornadoes, floods, earthquakes, fires, or other natural disasters;
- Severe weather events;
- Epidemics, pandemics, or public health emergencies;
- War, terrorism, civil unrest, riots, or acts of public enemies;
- Government actions, embargoes, sanctions, or changes in law that materially affect performance;
- Labor disputes, strikes, lockouts, or work stoppages not involving the affected party's own workforce;
- Widespread utility failures;
- Internet backbone failures;
- Regional or national telecommunications outages;
- Failures of public cloud infrastructure;
- Domain Name System (DNS) failures;

- Distributed denial-of-service (DDoS) attacks directed at infrastructure providers;
- Cyberattacks affecting third-party infrastructure or critical service providers;
- Supply chain disruptions materially affecting the availability of equipment or software; or
- Any other event beyond the reasonable control of the affected party that materially prevents or delays performance.

**19.2 Notice**

The party affected by a Force Majeure Event shall provide written notice to the other party within a commercially reasonable time after becoming aware that the event is materially affecting its ability to perform.

The notice shall, to the extent reasonably available:

- Describe the nature of the Force Majeure Event;
- Identify the obligations affected;
- Estimate the anticipated duration of the disruption, if known; and
- Describe reasonable mitigation efforts being undertaken.

Failure to provide prompt notice shall not eliminate the protections of this Article unless the delay materially prejudices the other party.

**19.3 Duty to Mitigate**

The affected party shall use commercially reasonable efforts to:

- Mitigate the effects of the Force Majeure Event;
- Resume performance as soon as reasonably practicable;
- Implement available business continuity or disaster recovery procedures, where appropriate; and
- Keep the other party reasonably informed regarding material developments affecting performance.

Neither party is required to settle labor disputes, incur commercially unreasonable expense, or take actions that would materially increase risk to persons, property, or information in order to avoid a Force Majeure Event.

**19.4 Suspension of Performance**

During the continuance of a Force Majeure Event:

- The affected party's obligations shall be suspended only to the extent performance is prevented or materially delayed by the Force Majeure Event.
- All obligations not directly affected shall continue.
- Client shall remain responsible for payment of Services already rendered and for recurring charges associated with Services that remain available unless otherwise agreed in writing.

**19.5 Third-Party Infrastructure**

The parties acknowledge that DefendIT Services ("DefendIT") relies on third-party infrastructure, including cloud providers, telecommunications carriers, internet service providers, software vendors, equipment manufacturers, data centers, and other service providers.

Outages, disruptions, or failures affecting such third-party infrastructure that materially impair DefendIT's ability to perform the Services may constitute a Force Majeure Event to the extent they are beyond DefendIT's reasonable control.

Nothing in this Section relieves DefendIT of its obligation to use commercially reasonable efforts to restore Services as soon as practicable.

**19.6 Cybersecurity Events**

A cyberattack or Security Incident shall not automatically constitute a Force Majeure Event.

However, a widespread cyber event affecting critical infrastructure, public cloud providers, telecommunications networks, internet backbone providers, or other essential third-party services may qualify if it materially prevents performance and is beyond the reasonable control of the affected party.

**19.7 Extended Force Majeure**

If a Force Majeure Event substantially prevents performance of the Services for a continuous period of **sixty (60) days** or more, either party may terminate the affected Service Document upon **thirty (30) days'** written notice if the Force Majeure Event remains unresolved.

Termination under this Section shall not constitute a default by either party.

Any fees accrued for Services performed prior to the effective date of termination shall remain payable.

**19.8 No Waiver**

A delay or failure to perform resulting from a Force Majeure Event shall not constitute:

- A breach of this Agreement;
- An Event of Default;
- Negligence; or
- A waiver of any rights under this Agreement.

Performance obligations shall resume when the Force Majeure Event no longer materially prevents performance.

**19.9 Survival**

This Article shall survive the expiration or termination of this Agreement to the extent necessary to govern any Force Majeure Event that commenced during the term of this Agreement and affects obligations that survive termination.

**ARTICLE XX**

**GENERAL PROVISIONS**

**20.1 Entire Agreement**

This Agreement, together with all applicable Managed Services Schedules, Statements of Work, Service Level Agreements, addenda, exhibits, amendments, and other documents expressly incorporated by reference (collectively, the "Service Documents"), constitutes the complete and exclusive agreement between the parties concerning its subject matter.

This Agreement supersedes all prior or contemporaneous proposals, negotiations, representations, understandings, and agreements, whether oral or written, relating to the Services.

**20.2 Order of Precedence**

In the event of a conflict among the Service Documents, the following order of precedence shall apply unless a document expressly states otherwise:

1. A written amendment signed by both parties that specifically references this Agreement;
2. The applicable Statement of Work, but only with respect to the Services described therein;
3. The applicable Managed Services Schedule;
4. Service-specific addenda (including, where applicable, Business Associate Agreements, Data Processing Addenda, or Microsoft Licensing Addenda);
5. The applicable Service Level Agreement with respect to operational service levels only;
6. This Master Services Agreement;
7. Any exhibits or attachments not expressly given higher priority.

No proposal, quote, purchase order, or Client-issued document shall modify this Agreement unless expressly accepted in writing by an authorized representative of DefendIT Services ("DefendIT").

**20.3 Amendments**

No amendment, modification, or waiver of this Agreement shall be effective unless made in writing and signed by authorized representatives of both parties.

Routine operational communications, support tickets, emails regarding scheduling, or other day-to-day correspondence shall not constitute an amendment to this Agreement unless they expressly state the parties' intent to modify contractual terms.

**20.4 Assignment**

Neither party may assign or transfer this Agreement, in whole or in part, without the prior written consent of the other party, which shall not be unreasonably withheld, conditioned, or delayed.

Notwithstanding the foregoing, DefendIT may assign this Agreement without Client's consent to:

- An affiliate;
- A successor by merger, consolidation, or reorganization;
- A purchaser of substantially all of DefendIT's assets or business; or
- Any entity acquiring control of DefendIT,

provided the assignee assumes DefendIT's obligations under this Agreement.

Any assignment in violation of this Section shall be void.

**20.5 Independent Contractors**

The parties are independent contractors.

Nothing contained in this Agreement creates or shall be construed as creating:

- A partnership;
- A joint venture;
- An agency relationship;
- A fiduciary relationship;
- An employment relationship; or
- Any authority for either party to bind the other except as expressly provided herein.

**20.6 Subcontractors**

DefendIT may utilize qualified subcontractors, consultants, or affiliated entities to perform portions of the Services.

DefendIT shall remain responsible for the performance of Services provided through its subcontractors to the same extent as if such Services were performed directly by DefendIT.

**20.7 Notices**

All notices required under this Agreement shall be in writing and shall be deemed given when:

- Personally delivered;
- Sent by nationally recognized overnight courier;
- Sent by certified U.S. Mail, return receipt requested; or
- Sent by electronic mail to the designated contractual notice addresses identified in the applicable Service Documents, with confirmation of transmission.

Either party may update its notice address by providing written notice to the other party.

Routine operational communications, invoices, support tickets, maintenance notifications, and service updates do not constitute formal contractual notice unless expressly identified as such.

**20.8 Waiver**

The failure of either party to enforce any provision of this Agreement shall not constitute a waiver of that provision or of any other provision.

Any waiver must be in writing and signed by the party granting the waiver.

A waiver of one breach shall not constitute a waiver of any prior, concurrent, or subsequent breach.

**20.9 Severability**

If any provision of this Agreement is determined by a court or arbitrator of competent jurisdiction to be invalid, illegal, or unenforceable, the remaining provisions shall remain in full force and effect.

The invalid or unenforceable provision shall be interpreted or modified, if possible, to most closely reflect the original intent of the parties while remaining enforceable under applicable law.

**20.10 No Third-Party Beneficiaries**

Except as expressly provided in this Agreement, nothing contained herein is intended to confer any rights, remedies, or benefits upon any person or entity other than the parties and their respective permitted successors and assigns.

**20.11 Cumulative Remedies**

Except where this Agreement expressly provides an exclusive remedy, the rights and remedies of each party are cumulative and are in addition to any other rights or remedies available at law or in equity.

The exercise of one remedy shall not preclude the exercise of any other available remedy.

**20.12 Further Assurances**

Each party agrees to execute and deliver such additional documents and take such further actions as may be reasonably necessary to carry out the intent and purposes of this Agreement.

**20.13 Electronic Signatures and Counterparts**

This Agreement may be executed in one or more counterparts, each of which shall be deemed an original and all of which together shall constitute one instrument.

Signatures transmitted electronically, including through electronic signature platforms, PDF, or other legally recognized electronic means, shall be deemed original signatures and shall have the same legal effect as manually executed signatures, to the fullest extent permitted by applicable law.

**20.14 Interpretation**

Unless the context clearly requires otherwise:

- Headings are for convenience only and do not affect interpretation.
- References to Articles, Sections, and Exhibits refer to this Agreement unless otherwise indicated.
- The words "including," "include," and similar terms mean "including without limitation."
- The singular includes the plural and vice versa.
- References to one gender include all genders.
- References to "days" mean calendar days unless expressly stated as Business Days.
- The rule of construction that ambiguities are construed against the drafter shall not apply to this Agreement.

**20.15 Survival**

Any provision that by its nature is intended to survive termination or expiration of this Agreement shall survive, including, without limitation:

- Payment obligations;
- Confidentiality;
- Data protection;
- Intellectual property;
- Warranty disclaimers;
- Limitation of liability;
- Indemnification;

- Dispute resolution; and
- Any accrued rights or obligations.

**20.16 Publicity**

Neither party shall issue a press release or public announcement regarding this Agreement without the prior written consent of the other party.

Notwithstanding the foregoing, unless Client objects in writing, DefendIT may identify Client by name and logo in customer lists and marketing materials solely to indicate that Client is or was a customer of DefendIT. DefendIT shall not disclose Confidential Information or imply Client's endorsement of DefendIT's services without Client's prior written consent.

**20.17 Export Compliance**

Each party shall comply with applicable export control, sanctions, and trade laws in connection with the Services.

Client shall not direct DefendIT to provide Services in violation of applicable export or sanctions laws.

**20.18 No Construction Against Drafter**

The parties acknowledge that this Agreement has been negotiated by sophisticated business entities and, to the extent applicable, shall be interpreted fairly and not strictly for or against either party based upon authorship.

**ARTICLE XXI**

**GOVERNING LAW, DISPUTE RESOLUTION, AND ARBITRATION**

**21.1 Governing Law**

This Agreement and any dispute, claim, or controversy arising out of or relating to this Agreement, the Services, or the relationship of the parties shall be governed by and construed in accordance with the laws of the **State of Texas**, without regard to its conflict of law principles.

**21.2 Good Faith Negotiation**

Before initiating arbitration or litigation, the parties shall first attempt in good faith to resolve any dispute through informal negotiations.

Either party may initiate this process by providing written notice describing the nature of the dispute.

Within fifteen (15) Business Days after receipt of such notice, representatives of both parties with authority to resolve the dispute shall confer, either in person or by videoconference, and make commercially reasonable efforts to resolve the matter.

Nothing in this Section prevents either party from seeking temporary injunctive or other emergency equitable relief where immediate action is reasonably necessary.

**21.3 Mediation**

If the dispute has not been resolved within thirty (30) days after the initial negotiation meeting, either party may request that the dispute be submitted to non-binding mediation before a mutually agreed mediator located in Texas.

Unless otherwise agreed:

- The parties shall share the mediator's fees equally.
- Each party shall bear its own attorneys' fees and costs incurred during mediation.
- Participation in mediation is a condition precedent to binding arbitration unless emergency equitable relief is sought.

**21.4 Binding Arbitration**

Except for matters expressly excluded in this Article, any dispute arising out of or relating to this Agreement that is not resolved through negotiation or mediation shall be resolved by **binding arbitration**.

The arbitration shall:

- Be administered by a nationally recognized arbitration organization mutually agreed upon by the parties, or, absent agreement, by the American Arbitration Association (AAA) under its Commercial Arbitration Rules;
- Be conducted before one arbitrator experienced in commercial technology disputes;
- Take place in **Bexar County, Texas**, unless the parties agree otherwise;
- Be conducted in the English language; and

- Result in a written decision setting forth the essential findings and conclusions.

Judgment upon the arbitration award may be entered in any court having jurisdiction.

**21.5 Exceptions to Arbitration**

Either party may seek relief in a court of competent jurisdiction for:

- Temporary restraining orders;
- Preliminary or permanent injunctions;
- Protection of Confidential Information;
- Protection or enforcement of intellectual property rights;
- Collection of undisputed amounts due under this Agreement; or
- Any matter that applicable law prohibits from being resolved through arbitration.

Seeking such relief shall not waive the right to arbitrate any remaining claims.

**21.6 Venue for Court Proceedings**

For matters properly brought before a court, including actions to enforce an arbitration award or obtain emergency equitable relief, the parties consent to the exclusive jurisdiction and venue of the state or federal courts located in **Bexar County, Texas**, unless applicable law requires otherwise.

Each party waives any objection based on improper venue or inconvenient forum.

**21.7 Attorneys' Fees and Costs**

In any arbitration or court proceeding arising from this Agreement, the prevailing party may recover its reasonable attorneys' fees, expert witness fees, court costs, arbitration costs, and other reasonable litigation expenses, to the extent permitted by applicable law and awarded by the arbitrator or court.

**21.8 Continued Performance**

During the pendency of any dispute, the parties shall continue to perform their respective obligations under this Agreement to the extent reasonably practicable.

Client shall continue to pay all undisputed amounts when due.

Neither party shall be required to continue performance if doing so would violate applicable law or materially compromise the safety or security of persons, systems, or information.

**21.9 Waiver of Jury Trial**

**TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EACH PARTY KNOWINGLY, VOLUNTARILY, AND IRREVOCABLY WAIVES ANY RIGHT TO A TRIAL BY JURY IN ANY LEGAL PROCEEDING ARISING OUT OF OR RELATING TO THIS AGREEMENT.**

This waiver applies whether the proceeding is brought in contract, tort, statute, or otherwise.

**21.10 Class Action Waiver**

To the fullest extent permitted by applicable law, each party agrees that any claim arising out of or relating to this Agreement shall be brought solely in that party's individual capacity.

Neither party shall participate in any class action, collective action, consolidated action, or representative proceeding relating to this Agreement, except where such waiver is prohibited by applicable law.

**21.11 Limitation Period**

Any dispute shall be subject to the limitation period established in **Article XVI (Limitation of Liability)** unless a different period is required by non-waivable law.

**21.12 Confidentiality of Proceedings**

Except as required by law or necessary to enforce an arbitration award or court order, the parties shall maintain the confidentiality of mediation, arbitration, settlement discussions, and related materials.

This provision does not restrict disclosures to legal counsel, insurers, accountants, auditors, regulators, or other professional advisors who have a legitimate need to know and are subject to appropriate confidentiality obligations.

**21.13 Survival**

The provisions of this Article shall survive the expiration or termination of this Agreement.

**ARTICLE XXII**

**EXECUTION AND SIGNATURES**

**22.1 Authority to Execute**

Each individual signing this Agreement represents and warrants that he or she is duly authorized to execute this Agreement on behalf of the respective party and to bind that party to its terms and conditions.

Each party further represents that it has obtained all necessary corporate, organizational, or governmental approvals required to enter into this Agreement.

**22.2 Effective Date**

This Agreement shall become effective on the **Effective Date** identified below or, if no Effective Date is specified, on the date the Agreement has been executed by both parties.

**22.3 Incorporation of Service Documents**

By executing this Agreement, the parties acknowledge that the following documents, as applicable, are incorporated by reference and together constitute the complete contractual relationship between the parties:

- Master Services Agreement (this Agreement)
- Managed Services Schedule(s)
- Statement(s) of Work
- Service Level Agreement(s)
- Cybersecurity Addendum(s)
- Shared Responsibility Matrix
- Microsoft Cloud Services Addendum(s)
- Business Associate Agreement(s), if applicable
- Data Processing Addendum(s), if applicable
- Technology Standards Manual, where incorporated by reference
- Any future amendments or addenda executed in accordance with this Agreement

Only those documents expressly executed or incorporated by reference shall be binding.

**22.4 Counterparts**

This Agreement may be executed in any number of counterparts, each of which shall be deemed an original, and all counterparts together shall constitute one and the same instrument.

**22.5 Electronic Signatures**

The parties agree that signatures transmitted electronically, including through electronic signature platforms, PDF, or other legally recognized electronic means, shall be deemed original signatures and shall have the same force and effect as manually executed signatures, to the fullest extent permitted by applicable law.

Each party agrees not to contest the validity or enforceability of this Agreement solely because it was executed electronically.

**22.6 Contract Administration**

Each party shall designate an authorized representative responsible for contractual communications under this Agreement.

Changes to billing contacts, technical contacts, or operational representatives do not require an amendment to this Agreement unless such change affects a contractual notice address required under Article XX.

**22.7 No Reliance**

Each party acknowledges that, in entering into this Agreement, it has not relied upon any statement, representation, promise, or warranty not expressly contained in this Agreement or the applicable Service Documents.

## EXHIBIT A

**SERVICE LEVEL AGREEMENT (SLA)**

*(Attached to and Incorporated into the Master Services Agreement)*

**1. Purpose**

This Service Level Agreement ("SLA") establishes the service objectives, response targets, communication standards, escalation procedures, and operational commitments applicable to the Managed Services provided by **DefendIT Services, LLC** ("DefendIT") under the Master Services Agreement ("MSA") and the applicable Managed Services Schedule ("MSS").

Unless expressly stated otherwise in a Statement of Work, this SLA applies to all recurring Managed Services.

This SLA establishes **service objectives** and **target performance levels**. It is not a guarantee of uninterrupted service or resolution within a specified period.

## 2. Definitions

For purposes of this SLA:

**Business Hours**
Monday through Friday, 8:00 AM to 5:00 PM, local time at the Client's primary business location, excluding recognized holidays unless otherwise stated in the MSS.

**Business Day**
Any day during Business Hours excluding weekends and recognized holidays.

**Response Time**
The elapsed time between receipt of a properly submitted support request and acknowledgement by a qualified technician who begins triage or work on the issue.

**Update Frequency**
The target interval at which DefendIT will provide status updates for active incidents.

**Restoration Target**
The objective to restore service or implement a commercially reasonable workaround. Restoration targets are goals and may be affected by factors outside DefendIT's reasonable control.

**Resolution**
Completion of all work necessary to permanently resolve an issue. Resolution times are not guaranteed due to dependencies on Client actions, third-party vendors, manufacturers, internet service providers, cloud providers, or other external factors.

## 3. Support Hours

**Standard Support**

Monday – Friday

8:00 AM – 5:00 PM

Local Time

**After-Hours Support**

After-hours support is available only for:

- Priority 1 incidents;
- Clients enrolled in after-hours support under the MSS; or
- Incidents specifically authorized by an authorized Client representative.

Work performed outside Standard Support Hours that is not covered by the MSS may be billed at the applicable after-hours rates.

**4. Incident Priority Levels**

**Priority 1 – Critical**

Examples include:

- Complete network outage
- Firewall failure
- Server outage affecting business operations
- Ransomware or active cybersecurity incident
- Microsoft 365 tenant inaccessible
- Internet outage affecting an entire location (excluding ISP-managed outages)
- Complete loss of line-of-business application affecting all users

Business Impact:

Business operations are substantially unavailable or a significant cybersecurity event is actively occurring.

**Priority 2 – High**

Examples include:

- Multiple users unable to work
- Core business application degraded
- VPN unavailable for multiple users
- Major printing outage
- Partial Microsoft 365 outage
- Significant performance degradation

Business Impact:

Business operations continue but with major impairment.

**Priority 3 – Medium**

Examples include:

- Single user unable to access email
- Individual workstation failure
- Software installation
- Printer affecting one department
- Peripheral device issues
- Routine application errors

Business Impact:

Limited impact affecting one user or a small group of users.

**Priority 4 – Low**

Examples include:

- Password reset
- User creation
- User termination
- Software request
- Device setup
- General questions
- Scheduled maintenance requests
- Cosmetic issues
- Non-urgent service requests

Business Impact:

Minimal operational impact.

**5. Service Objectives**

| Priority | Initial Response | Status Updates | Restoration Objective |
|---|---|---|---|
| **Priority 1** | **15 Minutes (24×7 for covered services)** | Every 60 minutes | Continuous effort until service is restored or a reasonable workaround is implemented |

| Priority | Initial Response | Status Updates | Restoration Objective |
|---|---|---|---|
| **Priority 2** | **1 Business Hour** | Every 4 Business Hours | Commercially reasonable efforts during applicable support hours |
| **Priority 3** | **4 Business Hours** | As appropriate | Commercially reasonable efforts |
| **Priority 4** | **1 Business Day** | Upon material status changes | Scheduled according to workload and Client priorities |

These objectives apply only after sufficient information has been received to open a support ticket.

**6. Ticket Submission**

Support requests may be submitted through:

- Client Portal
- Email
- Telephone
- Remote monitoring alerts
- Security monitoring systems
- Authorized integrations

Priority 1 incidents should be reported by telephone in addition to any electronic submission to ensure immediate attention.

**7. Ticket Prioritization**

DefendIT reserves the right to assign or adjust incident priority based on actual business impact.

If new information changes the severity of an incident, DefendIT may raise or lower the assigned priority after notifying the Client.

**8. Escalation Procedures**

Incidents may be escalated when:

- Restoration objectives are at risk;

- Specialized expertise is required;
- Vendor coordination becomes necessary;
- Executive communication is appropriate; or
- Business impact materially increases.

Escalation may include assignment to senior engineers, security personnel, management, or approved third-party vendors.

**9. Major Incident Management**

For Priority 1 incidents, DefendIT will:

- Assign an incident lead;
- Coordinate technical response efforts;
- Provide regular status updates;
- Engage necessary vendors or service providers;
- Maintain an incident timeline; and
- Conduct a post-incident review for significant events, upon request or where commercially appropriate.

**10. Scheduled Maintenance**

DefendIT may perform scheduled maintenance to maintain system security, reliability, and performance.

Where practical:

- Maintenance will be scheduled during off-hours;
- Advance notice will be provided for maintenance expected to cause service interruption; and
- Emergency maintenance may be performed without prior notice where necessary to address security risks or service stability.

**11. Client Responsibilities Affecting SLA**

SLA objectives are dependent upon the Client's cooperation. The Client shall:

- Designate authorized contacts;
- Provide timely access to systems, facilities, and personnel;
- Respond promptly to requests for information or approvals;
- Maintain supported hardware and software;
- Follow documented security requirements;
- Maintain internet connectivity and electrical power under the Client's control; and
- Notify DefendIT promptly of suspected security incidents or service disruptions.

Delays attributable to the Client may suspend applicable SLA objectives until the required cooperation is provided.

**12. SLA Exclusions**

Service objectives do not apply to delays resulting from:

- Force Majeure Events;
- Internet service provider failures;
- Public cloud provider outages;
- Third-party software defects;
- Manufacturer hardware failures;
- Client-requested delays;
- Unauthorized system modifications;
- Unsupported hardware or software;
- Cybersecurity incidents caused by the Client's failure to implement agreed security recommendations;
- Scheduled maintenance;
- Emergency maintenance;
- Delays awaiting vendor response, replacement hardware, software patches, or Client approval.

**13. Third-Party Vendors**

DefendIT will use commercially reasonable efforts to coordinate with internet service providers, cloud vendors, telecommunications carriers, software publishers, hardware manufacturers, and other third-party providers.

DefendIT is not responsible for the performance, response times, or service levels of third-party providers.

**14. Performance Reporting**

Where included in the MSS, DefendIT may provide periodic reports including:

- Ticket volumes;
- Response performance;
- System health;
- Patch compliance;
- Backup status;
- Security events;
- Endpoint status;
- Vulnerability trends;
- Microsoft 365 health;
- Strategic recommendations.

**15. Quarterly Business Reviews (QBRs)**

Where included in the MSS, DefendIT may conduct periodic service review meetings to discuss:

- Service performance;
- Open risks;
- Technology lifecycle planning;
- Security posture;
- Compliance initiatives;
- Capacity planning;
- Improvement opportunities.

**16. Service Credits**

Unless expressly stated in the applicable MSS, Statement of Work, or another written agreement signed by both parties, this SLA does **not** provide for monetary penalties, service credits, liquidated damages, fee reductions, or other financial remedies for failure to meet the service objectives described herein.

The service objectives in this SLA are operational targets intended to measure performance and support continuous improvement.

**17. Continuous Improvement**

DefendIT periodically reviews service performance and may update internal operational processes, staffing models, monitoring systems, and support procedures to improve service quality.

Operational improvements that do not materially reduce the Client's contractual rights do not require amendment of this SLA.

**18. Order of Precedence**

If a Statement of Work or Managed Services Schedule expressly establishes service levels that differ from this SLA, the terms of that document shall govern solely for the applicable Services.

**19. Acceptance**

This SLA is incorporated into the Master Services Agreement and becomes effective upon execution of the applicable Managed Services Schedule unless otherwise stated.

**EXHIBIT B**

**CYBERSECURITY SERVICES ADDENDUM**

*(Attached to and Incorporated into the Master Services Agreement)*

**1. Purpose**

This Cybersecurity Services Addendum ("CSA") defines the cybersecurity services, operational responsibilities, incident response procedures, security standards, and shared obligations applicable to the Managed Security Services provided by **DefendIT Services, LLC** ("DefendIT").

This Addendum supplements the Master Services Agreement ("MSA"), the Managed Services Schedule ("MSS"), and the Service Level Agreement ("SLA"). In the event of a conflict, the order of precedence established in the MSA shall apply.

**2. Scope of Cybersecurity Services**

Only those services expressly identified in the applicable MSS or Statement of Work are included.

Available services may include:

**Endpoint Protection**

- Managed Endpoint Detection & Response (EDR)
- Managed Extended Detection & Response (XDR)
- Managed Antivirus
- Device Isolation
- Behavioral Detection
- Threat Hunting
- Malware Remediation

**Email Security**

- Spam Filtering
- Anti-Phishing
- Safe Links
- Safe Attachments
- Email Encryption
- Business Email Compromise (BEC) Detection
- DMARC, DKIM, and SPF assistance

**Identity Security**

- Microsoft Entra ID administration
- Multi-Factor Authentication (MFA)
- Conditional Access policy management

- Identity monitoring
- Privileged account review
- Password policy enforcement

**Network Security**

- Firewall administration
- Secure VPN management
- DNS filtering
- Intrusion Detection / Prevention (IDS/IPS), where supported
- Secure remote access
- Firewall rule reviews

**Security Monitoring**

Where included in the MSS:

- 24×7 monitoring
- Security Information and Event Management (SIEM)
- Security Operations Center (SOC)
- Log aggregation
- Threat intelligence correlation
- Automated alerting
- Threat analysis

**Vulnerability Management**

- Internal vulnerability scanning
- External vulnerability scanning
- Risk scoring
- Patch recommendations
- Exposure reporting
- Remediation guidance

Unless otherwise stated, vulnerability remediation is performed through standard maintenance processes or separate project work.

**3. Security Baseline Requirements**

To receive Managed Security Services, Client agrees to maintain or permit DefendIT to implement the following minimum standards unless otherwise documented in a written risk acceptance:

- Supported operating systems
- Supported Microsoft 365 licensing
- Multi-Factor Authentication for administrative accounts
- Supported firewall platform
- Endpoint protection
- Disk encryption for portable devices
- Secure password policy
- Timely security patching
- Supported backup solution
- Administrative account separation
- DNS filtering where applicable

Failure to maintain minimum security standards may reduce the effectiveness of the Services and may affect incident response obligations.

**4. Security Monitoring**

DefendIT will use commercially reasonable efforts to monitor covered systems using the security tools included in the Client's subscribed services.

Monitoring is intended to identify known or suspected indicators of compromise, suspicious activity, or policy violations. No monitoring solution can detect every threat or guarantee prevention of unauthorized access.

**5. Security Incident Classification**

For operational purposes, Security Incidents are classified as follows:

**Severity 1 – Critical**

Examples:

- Active ransomware
- Confirmed domain compromise
- Confirmed Microsoft 365 compromise
- Active data exfiltration
- Widespread malware outbreak
- Active business email compromise
- Confirmed administrator account takeover

**Severity 2 – High**

Examples:

- Confirmed malware infection on one or more systems
- Privileged account compromise
- Firewall compromise
- Repeated unauthorized access attempts
- High-confidence SIEM alerts requiring immediate investigation

**Severity 3 – Medium**

Examples:

- Suspicious login activity
- Vulnerability requiring prompt remediation
- Endpoint security alerts with moderate confidence
- Policy violations

**Severity 4 – Low**

Examples:

- Informational alerts
- Routine vulnerability findings

- Policy recommendations
- Security awareness reporting

**6. Security Incident Response**

Upon confirmation of a covered Security Incident, DefendIT may:

- Validate the alert;
- Determine the scope of the incident;
- Initiate containment measures;
- Isolate affected devices where supported;
- Preserve relevant logs;
- Coordinate with authorized Client representatives;
- Engage approved third-party vendors where appropriate; and
- Recommend remediation actions.

Actions taken will be limited to the authority granted by the Client and the Services purchased.

**7. Incident Response Objectives**

| **Severity** | **Initial Response** | **Status Updates** |
|---|---|---|
| Critical | 15 Minutes (24×7 for covered services) | Hourly |
| High | 1 Business Hour | Every 4 Business Hours |
| Medium | 4 Business Hours | Daily as appropriate |
| Low | Next Business Day | As needed |

These are operational objectives and not guaranteed response times.

**8. Client Responsibilities**

The Client shall:

- Promptly report suspected security incidents.
- Maintain current emergency contacts.
- Provide timely authorization for containment actions.
- Preserve evidence where instructed.
- Notify DefendIT of employee terminations, role changes, or suspected insider threats.
- Cooperate with investigations and remediation efforts.

Delays in providing required information or approvals may affect response objectives.

**9. Excluded Services**

Unless expressly included in the MSS or a separate Statement of Work, the following are **not** included:

- Digital forensics
- eDiscovery
- Expert witness services
- Litigation support
- Cyber insurance claim management
- Legal advice
- Regulatory reporting
- Public relations services
- Ransom negotiations
- Cryptocurrency acquisition or payment
- Law enforcement coordination beyond reasonable operational assistance
- Data recovery from intentionally destroyed or encrypted systems
- Compliance certification audits
- Penetration testing
- Red team exercises
- Secure software development reviews

These services may be provided under a separate engagement if offered by DefendIT.

**10. Risk Acceptance**

If the Client elects not to implement a security recommendation that DefendIT reasonably determines is necessary to reduce a material cybersecurity risk, DefendIT may request written acknowledgment of the associated risk.

DefendIT reserves the right to document such decisions in the Client's service record. A Client's decision to decline recommended safeguards does not relieve DefendIT of its obligation to perform the contracted Services but may limit DefendIT's ability to prevent or mitigate resulting incidents.

**11. Backup and Recovery**

Unless expressly included in the MSS:

- DefendIT does not guarantee that backups exist, are complete, or are recoverable.
- Backup monitoring is distinct from backup validation and disaster recovery testing.
- Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs), if applicable, shall be defined in the MSS or a separate Statement of Work.
- The Client remains responsible for identifying critical systems and data requiring protection.

**12. Security Awareness**

Where included in the MSS, DefendIT may provide:

- Security awareness training
- Simulated phishing campaigns
- User risk reporting
- Educational content
- Administrative reporting

User participation and compliance remain the Client's responsibility.

**13. Compliance Assistance**

DefendIT may assist with cybersecurity frameworks such as:

- CIS Controls
- NIST Cybersecurity Framework (CSF)
- CMMC
- HIPAA Security Rule
- PCI DSS

Unless expressly stated in writing, DefendIT does **not** certify the Client's compliance, provide legal opinions, or guarantee that the Client satisfies any regulatory or contractual requirement.

**14. Limitation of Security Services**

The parties acknowledge that no cybersecurity program can eliminate all risk. DefendIT does not warrant or guarantee that:

- Every attack will be detected;
- Every vulnerability will be identified;
- Every malicious email will be blocked;
- Every compromise will be prevented;
- Every system will remain continuously secure; or
- The Client will avoid financial loss, operational disruption, regulatory action, or reputational harm.

The Services are designed to materially reduce cybersecurity risk through commercially reasonable administrative, technical, and operational safeguards.

**15. Confidentiality of Security Information**

Security assessments, vulnerability reports, penetration testing results, incident reports, threat intelligence, and security recommendations provided by DefendIT are Confidential Information under the MSA and shall not be disclosed to third parties except as required by law or with DefendIT's prior written consent.

**16. Acceptance**

This Cybersecurity Services Addendum is incorporated into and governed by the Master Services Agreement and becomes effective upon execution of the applicable Managed Services Schedule or other Service Document referencing this Addendum.

**EXHIBIT C**

**SHARED RESPONSIBILITY MATRIX**

*(Attached to and Incorporated into the Master Services Agreement)*

**1. Purpose**

This Shared Responsibility Matrix ("SRM") defines the respective operational and security responsibilities of **DefendIT Services, LLC** ("DefendIT") and the Client. It supplements the Master Services Agreement ("MSA"), Managed Services Schedule ("MSS"), Service Level Agreement ("SLA"), and Cybersecurity Services Addendum.

Unless expressly stated otherwise in a Statement of Work, responsibilities are allocated as set forth below.

For purposes of this Matrix:

- **DefendIT** = Primary responsibility for performing or managing the activity.
- **Client** = Primary responsibility for performing or authorizing the activity.
- **Shared** = Both parties have defined responsibilities that must be fulfilled for the control to be effective.

Failure by either party to perform its assigned responsibilities may affect service delivery, security posture, incident response, or compliance outcomes.

**2. Governance & Administration**

| **Responsibility** | **DefendIT** | **Client** | **Shared** |
|---|---|---|---|
| IT Strategy Recommendations | ✓ | | |
| Business Risk Decisions | | ✓ | |
| Technology Budget Approval | | ✓ | |
| Technology Roadmap | ✓ | | ✓ |
| Vendor Coordination | ✓ | | ✓ |
| Executive Business Decisions | | ✓ | |
| Policy Development Assistance | ✓ | | ✓ |

| Responsibility | DefendIT | Client | Shared |
|---|---|---|---|
| Policy Approval | | ✓ | |

---

### 3. Identity & Access Management

| Responsibility | DefendIT | Client | Shared |
|---|---|---|---|
| MFA Configuration | ✓ | | |
| MFA Enrollment | | | ✓ |
| Password Policy Configuration | ✓ | | |
| Password Creation & Protection | | ✓ | |
| User Account Provisioning | ✓ | | ✓ |
| User Termination Notification | | ✓ | |
| Disable Departed User Accounts | ✓ | | ✓ |
| Administrative Account Management | ✓ | | ✓ |
| Privileged Access Approval | | ✓ | |

### 4. Endpoint Security

| Responsibility | DefendIT | Client | Shared |
|---|---|---|---|
| Endpoint Protection Deployment | ✓ | | |
| EDR/MDR Monitoring | ✓ | | |
| Patch Management | ✓ | | |
| Operating System Updates | ✓ | | ✓ |
| Hardware Replacement Decisions | | ✓ | |

| Responsibility | DefendIT | Client | Shared |
|---|---|---|---|
| Physical Device Security | | ✓ | |
| Report Lost or Stolen Devices | | ✓ | |
| Disk Encryption Configuration | ✓ | | |
| Endpoint Compliance Monitoring | ✓ | | |

**5. Microsoft 365 & Cloud Services**

| Responsibility | DefendIT | Client | Shared |
|---|---|---|---|
| Tenant Administration | ✓ | | |
| Licensing Administration | ✓ | | ✓ |
| License Purchasing Approval | | ✓ | |
| Exchange Administration | ✓ | | |
| SharePoint Administration | ✓ | | |
| Teams Administration | ✓ | | |
| OneDrive Administration | ✓ | | |
| Retention Policy Configuration | ✓ | | ✓ |
| Business Data Classification | | ✓ | |

**6. Network Infrastructure**

| Responsibility | DefendIT | Client | Shared |
|---|---|---|---|
| Firewall Management | ✓ | | |
| Switch Management | ✓ | | |

| Responsibility | DefendIT | Client | Shared |
|---|---|---|---|
| Wireless Administration | ✓ | | |
| VPN Administration | ✓ | | |
| ISP Relationship | | ✓ | ✓ |
| Structured Cabling | | ✓ | |
| Electrical Power & Environmental Controls | | ✓ | |
| Physical Security of Network Equipment | | ✓ | |

**7. Backup & Disaster Recovery**

| Responsibility | DefendIT | Client | Shared |
|---|---|---|---|
| Backup Monitoring | ✓ | | |
| Backup Job Management | ✓ | | |
| Restore Testing (if included) | ✓ | | ✓ |
| Recovery Priorities | | ✓ | |
| Business Continuity Planning | | ✓ | ✓ |
| Disaster Recovery Plan Approval | | ✓ | |
| Critical Data Identification | | ✓ | |
| Recovery Validation | | | ✓ |

**8. Security Monitoring & Incident Response**

| Responsibility | DefendIT | Client | Shared |
|---|---|---|---|
| Security Monitoring | ✓ | | |

| Responsibility | DefendIT | Client | Shared |
|---|---|---|---|
| Alert Validation | ✓ | | |
| Threat Investigation | ✓ | | |
| Initial Containment | ✓ | | ✓ |
| Notify DefendIT of Suspected Incidents | | ✓ | |
| Executive Incident Decisions | | ✓ | |
| Regulatory Notification Decisions | | ✓ | |
| Law Enforcement Coordination | | ✓ | ✓ |
| Cyber Insurance Notification | | ✓ | |

**9. Compliance**

| Responsibility | DefendIT | Client | Shared |
|---|---|---|---|
| Technical Safeguards | ✓ | | |
| Compliance Guidance | ✓ | | |
| Legal Compliance | | ✓ | |
| Internal Audits | | ✓ | |
| External Audits | | ✓ | ✓ |
| Regulatory Reporting | | ✓ | |
| Policy Enforcement | | ✓ | |
| Risk Acceptance Decisions | | ✓ | |

**10. End Users**

| Responsibility | DefendIT | Client | Shared |
|---|---|---|---|
| Security Awareness Platform | ✓ | | |
| User Participation | | ✓ | |
| Phishing Campaign Administration | ✓ | | |
| Security Awareness Completion | | ✓ | |
| Acceptable Use Enforcement | | ✓ | |
| Report Suspicious Activity | | | ✓ |
| Protect Credentials | | ✓ | |

**11. Procurement & Asset Lifecycle**

| Responsibility | DefendIT | Client | Shared |
|---|---|---|---|
| Technology Recommendations | ✓ | | |
| Procurement Assistance | ✓ | | ✓ |
| Purchasing Approval | | ✓ | |
| Asset Inventory | ✓ | | ✓ |
| Equipment Disposal Guidance | ✓ | | |
| Secure Device Disposal | | | ✓ |
| Warranty Management | ✓ | | ✓ |

**12. Responsibilities Not Assumed by DefendIT**

Unless expressly included in the MSS or a separate Statement of Work, DefendIT does **not** assume responsibility for:

- Executive business decisions.

- Corporate governance.
- Legal or regulatory interpretation.
- Financial approvals.
- Human resources functions.
- Employee disciplinary actions.
- Cyber insurance procurement or claims management.
- Payment authorization controls.
- Accounting controls.
- Internal fraud investigations.
- Physical building security.
- Environmental controls.
- Business continuity ownership.
- Data classification.
- Records retention policy decisions.

**13. Client Acknowledgment**

The Client acknowledges that effective cybersecurity requires cooperation between the parties. DefendIT's ability to provide the Services depends upon the Client fulfilling its assigned responsibilities, including timely approvals, accurate information, user participation, and implementation of agreed security measures.

Failure to perform Client responsibilities may reduce the effectiveness of the Services and may affect DefendIT's ability to meet service objectives under the MSA, SLA, or Cybersecurity Services Addendum.

**14. Updates to the Matrix**

DefendIT may periodically update this Shared Responsibility Matrix to reflect changes in technology, security practices, supported platforms, regulatory requirements, or service offerings.

Material changes that reduce the Client's contractual rights or materially increase the Client's obligations will be communicated in advance and, where required by the MSA, implemented through an amendment or updated exhibit.

**15. Acceptance**

This Shared Responsibility Matrix is incorporated into and governed by the Master Services Agreement and becomes effective upon execution of the applicable Managed Services Schedule or other Service Document referencing this Matrix.

**EXHIBIT D**

**MICROSOFT CLOUD SERVICES ADDENDUM**

*(Attached to and Incorporated into the Master Services Agreement)*

**1. Purpose**

This Microsoft Cloud Services Addendum ("Addendum") governs the procurement, licensing, administration, and support of Microsoft cloud services provided by **DefendIT Services, LLC** ("DefendIT") under the Microsoft Cloud Solution Provider ("CSP") program or other authorized Microsoft licensing programs.

This Addendum supplements the Master Services Agreement ("MSA"), the applicable Managed Services Schedule ("MSS"), and any applicable Statement of Work ("SOW"). In the event of a conflict, the order of precedence established in the MSA shall apply.

**2. Scope of Services**

Where included in the MSS or SOW, DefendIT may provide services including:

- Microsoft 365 licensing
- Microsoft 365 administration
- Exchange Online administration
- SharePoint Online administration
- Microsoft Teams administration
- OneDrive administration
- Microsoft Entra ID administration
- Microsoft Intune administration
- Microsoft Defender administration
- Microsoft Azure subscription administration
- Microsoft licensing advisory services

- Tenant administration
- Microsoft support coordination

Only those services expressly identified in the MSS or SOW are included.

**3. Microsoft Relationship**

The Client acknowledges that:

- Microsoft cloud services are provided by Microsoft Corporation or its affiliates.
- DefendIT is an authorized reseller and service provider, not the publisher or owner of Microsoft's services.
- Microsoft's online service terms, product terms, privacy commitments, and licensing requirements continue to apply.
- Microsoft may modify its products, licensing models, service features, pricing, and availability at its discretion.

DefendIT is not responsible for changes made by Microsoft to its services or licensing programs.

**4. Tenant Ownership**

Unless otherwise agreed in writing:

- The Microsoft 365 tenant belongs to the Client.
- The Client retains ownership of its domain names, data, and Microsoft tenant.
- DefendIT may be delegated administrative privileges solely for the purpose of delivering contracted Services.
- Upon termination of the Services, DefendIT will cooperate in the orderly transition of administrative access, subject to payment of all outstanding amounts and any agreed transition services.

**5. Licensing**

The Client is responsible for maintaining sufficient licenses for all users, devices, and services utilizing Microsoft products.

DefendIT may recommend licensing changes based on Microsoft's requirements or the Client's operational needs. The Client is responsible for approving all licensing purchases and modifications.

**6. Microsoft New Commerce Experience (NCE)**

Where Microsoft subscriptions are purchased under the New Commerce Experience ("NCE") or any successor program:

- Subscription commitments are subject to Microsoft's applicable terms and commitment periods.
- Annual commitment subscriptions generally cannot be reduced or canceled during the commitment term except as permitted by Microsoft.
- Monthly commitment subscriptions may have different pricing and cancellation rights.
- DefendIT will administer subscriptions consistent with Microsoft's then-current CSP policies.

The Client acknowledges that Microsoft—not DefendIT—establishes these program rules.

**7. Seat Additions and Reductions**

Additional licenses requested by the Client may be added at any time, subject to Microsoft's licensing rules and current pricing.

License reductions or cancellations are governed by Microsoft's applicable licensing program and may not become effective until the end of the applicable commitment period.

DefendIT is not responsible for charges resulting from Microsoft-imposed commitment periods.

**8. Pricing**

Microsoft licensing prices are subject to change.

DefendIT may adjust recurring charges to reflect:

- Microsoft price increases or decreases;
- Currency or regional pricing changes imposed by Microsoft;
- Changes in subscription quantity;
- Changes in Microsoft's licensing programs; or
- Changes requested by the Client.

Where commercially practicable, DefendIT will provide advance notice of pricing changes received from Microsoft.

**9. Billing**

Unless otherwise stated in the MSS:

- Microsoft subscriptions are billed monthly in advance.
- Azure consumption services may be billed monthly in arrears based on actual usage.
- Taxes, governmental fees, and regulatory charges are additional unless expressly stated otherwise.
- Failure to timely pay invoices may result in suspension of Microsoft services in accordance with the MSA.

**10. Azure Consumption Services**

Where Azure services are provided:

- Charges are based upon actual Microsoft-reported consumption.
- Monthly usage may fluctuate.
- DefendIT cannot guarantee monthly Azure costs.
- The Client remains responsible for all authorized Azure resource consumption.

Upon request, DefendIT may assist with budgeting, cost optimization, and monitoring.

**11. Administrative Access**

To provide the Services, the Client authorizes DefendIT to receive delegated administrative privileges appropriate for the subscribed services.

DefendIT will use such access solely to deliver the contracted Services and in accordance with the confidentiality and security obligations of the MSA.

**12. Security Responsibilities**

Where included in the subscribed Services, DefendIT may:

- Configure Multi-Factor Authentication (MFA)
- Configure Conditional Access
- Configure Microsoft Defender policies
- Configure Intune device management

- Configure Exchange Online Protection
- Configure Microsoft Secure Score recommendations
- Configure security baselines

The Client remains responsible for approving security policies that materially affect business operations.

**13. Data Ownership**

The Client retains all ownership rights in its Microsoft 365 data, email, SharePoint content, Teams data, OneDrive content, and Azure-hosted information.

Nothing in this Addendum transfers ownership of Client data to DefendIT.

**14. Backup**

The Client acknowledges that Microsoft provides service availability features but does **not** provide comprehensive backup of customer data for all recovery scenarios.

Unless expressly included in the MSS or SOW, DefendIT does not provide Microsoft 365 backup or long-term retention services.

Where Microsoft 365 backup services are purchased, those services are governed by the applicable MSS, SOW, and backup documentation.

**15. Microsoft Service Availability**

DefendIT does not warrant or guarantee the availability, uptime, or performance of Microsoft's cloud services.

Any Microsoft service outage, degradation, maintenance event, or regional disruption is outside DefendIT's reasonable control.

DefendIT will use commercially reasonable efforts to assist the Client in monitoring Microsoft service health, opening support requests with Microsoft where appropriate, and implementing available workarounds.

**16. End of Life and Service Changes**

Microsoft may discontinue, replace, rename, or materially modify products or features.

DefendIT may recommend migration to successor services where necessary to maintain supportability or security.

Migration work beyond ordinary administration may constitute billable Professional Services unless otherwise included in the MSS or SOW.

**17. Third-Party Integrations**

The Client is responsible for evaluating and approving third-party applications integrated with Microsoft services.

DefendIT may assist with integration and administration but does not warrant the security, availability, or functionality of third-party products.

**18. Transition Assistance**

Upon expiration or termination of the Services, DefendIT will provide commercially reasonable transition assistance to transfer administrative access and relevant documentation to the Client or its designated successor provider.

Transition services beyond routine administrative access transfer may be performed as billable Professional Services under a separate SOW or the applicable hourly rates in the MSS.

**19. Compliance**

DefendIT may assist the Client with Microsoft security and compliance capabilities, including Microsoft Purview, retention policies, sensitivity labels, audit logging, and related features where included in the subscribed services.

Unless expressly agreed in writing, DefendIT does not warrant that the Client's Microsoft environment satisfies any legal, regulatory, contractual, or industry-specific compliance requirement.

**20. Acceptance**

This Microsoft Cloud Services Addendum is incorporated into and governed by the Master Services Agreement and becomes effective upon execution of the applicable Managed Services Schedule or other Service Document referencing this Addendum.