MASTER SERVICES AGREEMENT (2026 EDITION)

Gyver Networks LLC d/b/a Gyver Technologies

1. INTRODUCTION

This Master Services Agreement ("Agreement") is between Gyver Networks LLC d/b/a Gyver Technologies ("Gyver") and the client identified in the applicable Service Order ("Client"). This Agreement governs all managed services, cybersecurity services, support, monitoring, and professional services provided by Gyver.

2. DEFINITIONS

2.1 Services – All managed IT services, monitoring, support, cybersecurity services, tools, patching, updates, and professional services delivered under any Service Order.

2.2 Service Order – A written document executed by both parties specifying services purchased, the applicable service model, pricing, and term.

2.3 Attachments and Addendums

Attachments apply to all Clients and are automatically incorporated into this Agreement. The following Attachments form part of this Agreement:

- Attachment A – Cybersecurity Incident Response
- Attachment B – Security Standards
- Attachment C – OEM / End-of-Life Policy

Addendums apply only when referenced in a Client's Service Order. Addendums may vary based on the selected service tier or nature of services provided and may include:

- Managed Services SLA Addendum
- GyverShield SMB SLA Addendum
- T&M Limited SLA Addendum
- Data Retention & Backup Addendum
- Cabling & Professional Services Addendum
- Any additional mutually executed SOWs or service-specific addendums

For each Client, the SLA Addendum corresponding to their selected service tier (Managed Services, GyverShield SMB, or Time & Materials) automatically becomes part of this Agreement upon execution of the Service Order.

2.4 Incident – An unplanned interruption, reduction, or malfunction of a supported system.

2.5 Service Request – A non-urgent request such as onboarding, access changes, software installation, or administrative tasks.

2.6 Change – Any modification to systems, access, security, network, or configurations requiring engineering or elevated privileges.

2.7 Client Systems – All systems, networks, hardware, software, cloud accounts, platforms, and related infrastructure owned, leased, operated, or controlled by Client.

3. SCOPE OF SERVICES

3.1 Gyver will provide the Services listed in the Client's Service Order.

3.2 Services may include managed IT services, cybersecurity services, end-user support, security tools, monitoring, cloud and Microsoft 365 administration, network support, patch management, professional services, and project services.

3.3 Any service not explicitly stated in the Service Order is out of scope and may be billed separately.

4. SERVICE LEVEL MODELS

Gyver delivers services through three service-level models. The Client's Service Order specifies which model applies.

4.1 Managed Services

Includes covered device troubleshooting, monitoring, patching, remediation, endpoint security tools, vendor coordination, and response commitments as defined in the Managed SLA Addendum.

4.2 GyverShield SMB

Includes proactive maintenance, monitoring, patching, endpoint security tools, and updates. Troubleshooting is not included and is billed at the reduced SMB hourly rate as defined in the SMB SLA Addendum.

4.3 Time & Materials (T&M)

Includes endpoint security tools, monitoring, updates, and patching. All troubleshooting is billable at T&M rates. Any response commitments (if applicable) are listed in the T&M Limited SLA Addendum.

5. CLIENT RESPONSIBILITIES

5.1 Provide Gyver with reasonable access to systems, personnel, and resources required to deliver services.

5.2 Maintain valid licensing and third-party support agreements.

5.3 Follow Gyver's Security Standards (Attachment B), including MFA, supported devices, antivirus/EDR, patching, and basic security controls.

5.4 Ensure users follow acceptable security practices and do not bypass or remove security controls.

5.5 Maintain backups unless backup services are purchased under a Service Order.

5.6 Notify Gyver promptly of suspected security incidents or compromised accounts.

5.7 BYOD (Bring Your Own Device)

(a) Personal devices ("BYOD Devices") are not covered, supported, monitored, patched, secured, or eligible for included support unless explicitly listed as Covered in the Service Order.

(b) If Client allows employees to access company resources using personal devices, Client must:

- maintain and enforce a written BYOD policy;
- require screen lock, password/PIN, encryption (where supported), and up-to-date OS and security patches;
- ensure employees promptly report lost or stolen devices.

(c) Gyver may remove access, revoke profiles, or wipe corporate data (not personal data) from a BYOD Device when necessary to protect Client Systems. Client is responsible for obtaining user consent.

(d) Gyver is not liable for loss of personal data, configurations, or applications on BYOD Devices resulting from support or security actions.

(e) Gyver cannot guarantee the security of any system, network, or cloud environment accessed via unmanaged or non-compliant BYOD Devices.

6. FEES & PAYMENT TERMS

6.1 Recurring services are billed monthly in advance.

6.2 Hourly labor, project services, and other non-recurring fees are billed in arrears per the rates defined in the Service Order.

6.3 Invoices are due upon receipt.

6.4 Late payments may incur a 1.5% monthly finance charge.

6.5 Gyver may suspend services for non-payment after providing notice.

6.6 Prices may adjust annually with 30 days' notice.

6.7 Client is responsible for any applicable taxes except taxes based on Gyver's net income.

7. DATA SECURITY, PRIVACY & RETENTION

7.1 Gyver uses commercially reasonable efforts to secure systems but cannot guarantee prevention of all cybersecurity incidents.

7.2 Backup and retention handling are defined only in the Data Retention & Backup Addendum.

7.3 Gyver is not responsible for outages, failures, or security issues arising from third-party vendors, cloud providers, unsupported systems, or systems outside Gyver's control.

8. CYBER INSURANCE REQUIREMENT

8.1 Client must maintain adequate cyber-liability insurance.

8.2 Gyver is not an insurer. Cybersecurity incident response is governed exclusively by Attachment A – Cybersecurity Incident Response.

9. LIMITATION OF LIABILITY

9.1 Gyver's total liability is limited to the fees paid by Client in the preceding twelve (12) months.

9.2 Neither party is liable for indirect, incidental, special, or consequential damages.

9.3 Gyver is not responsible for losses arising from misconfiguration by Client, third-party failures, unsupported systems, or Client non-compliance.

9.4 These limitations do not apply to gross negligence or intentional misconduct.

10. TERM & TERMINATION

10.1 This Agreement begins upon execution of the first Service Order.

10.2 Either party may terminate with 30 days' written notice unless the Service Order specifies otherwise.

10.3 Payment obligations survive termination.

11. CONFIDENTIALITY

11.1 Each party shall maintain the confidentiality of the other's confidential information.

11.2 Confidentiality obligations survive termination.

12. INCLUDED VS BILLABLE SUPPORT

12.1 Included Support (where applicable)

Included support may consist of:

- troubleshooting Covered Devices (Managed only)
- monitoring and automated remediation
- security tool management
- patching and updates
- standard user support (Managed only)
- coordination with third-party vendors
- security alerts that do not rise to the level of a cybersecurity incident

12.2 Billable Support

Support becomes billable when it falls outside the services included under the selected service model.

12.2.1 Change Requests

Includes firewall, network, routing, VPN adjustments, cloud or server configuration changes, DNS or certificate adjustments, and architectural modifications.

12.2.2 Non-Standard User Requests

Includes unauthorized software removal, reversing user-caused misconfigurations, corrupted profiles, or any BYOD-related fixes.

12.2.3 Unsupported or Out-of-Compliance Systems

Includes devices that are out-of-lifecycle, unsupported, failing, misconfigured, or not meeting Gyver's Security Standards.

12.2.4 Project-Level Work

Includes migrations, deployments, redesigns, bulk changes, or troubleshooting requiring more than three hours.

12.2.5 After-Hours Work

Support outside normal business hours unless included in the service model.

12.2.6 Cybersecurity Incidents

Cybersecurity incident response is governed by Attachment A. Gyver will attempt to notify Client before taking action; however, Gyver may take immediate containment steps to stop an active threat. Containment efforts may require up to four (4) hours, and all containment, investigation, remediation, and recovery work is fully billable.

12.3 Determination Rule

Gyver determines whether a ticket is classified as an Incident, Service Request, or Change.

12.4 Extended Troubleshooting Rule

Troubleshooting exceeding three (3) hours or work performed on devices older than three (3) years may be reclassified as billable.

12.5 Authorization Rule

Billable work requires Client approval unless immediate action is required to prevent data loss or security exposure.

12.6 Covered Device Eligibility

A device is eligible for included support only if it:

a. is in good working order at service start;
b. meets Gyver's security and hardware standards;
c. is within supported lifecycle;
d. is listed as Covered in the Service Order;
e. is not a BYOD Device unless explicitly listed as Covered.

12.7 Dormant / Inactive Device Billing

A device temporarily removed from active use ("Dormant Device") may be billed at a reduced rate if all of the following conditions are met:

(a) Client provides written notice at least five (5) business days prior to the billing month;
(b) The device remains enrolled in Gyver's monitoring, security, and management tools and must remain capable of receiving updates;
(c) The device is not assigned to an active user and is not used in production;
(d) Dormant Devices are billed at 40% of the standard device rate unless otherwise stated in the Service Order;
(e) Reactivation may require a one-time reactivation or onboarding fee at Gyver's then-current rate;
(f) Devices that fall out of compliance with Security Standards may be returned to full billing;
(g) Retroactive billing adjustments are not permitted.

12.8 Pre-Existing Issues

Issues existing prior to Gyver's service start require billable remediation.

12.9 Device Age Limitations

Devices older than 3 years may require billable troubleshooting.

Devices older than 5 years are excluded unless explicitly approved and listed.

Devices in degraded condition may require billable remediation.

12.10 Onboarding of New Hardware, Users & Devices

12.10.1 New Hardware Purchased Through Gyver

All hardware purchased through Gyver includes a one-time setup, configuration, and deployment fee included in the hardware quote.

12.10.2 Reassigning or Repurposing Existing Gyver-Managed Devices

Managed Services: Standard user onboarding included.

GyverShield SMB: Onboarding billed at SMB hourly rate.

T&M: Onboarding billed at T&M hourly rates.

Non-Standard Work for all tiers (billable):

- profile cleanup or recovery
- malware removal
- major OS updates
- reversing user-caused configuration changes
- file migrations
- local account conflicts

12.10.3 Client-Provided or Non-Managed Hardware

Any device not purchased through Gyver and not already under full management is fully billable for onboarding.

12.10.4 Device Health Requirement

Devices must be healthy, supported, patched, malware-free, and able to join Gyver's baseline.

If remediation is needed before onboarding, it is billable under Section 12.2.

13. GENERAL PROVISIONS

13.1 Massachusetts law governs this Agreement.

13.2 Neither party may assign this Agreement without consent, except Gyver may assign to affiliates or in corporate restructuring.

13.3 Force Majeure applies.

13.4 This Agreement, together with its Attachments and Addendums, constitutes the entire agreement.

13.5 Modifications must be in writing and executed by both parties.

ATTACHMENTS & ADDENDUMS (PROVIDED SEPARATELY)

Attachments (apply to all Clients):

A. Attachment A – Cybersecurity Incident Response

B. Attachment B – Security Standards

C. Attachment C – OEM / End-of-Life Policy

Addendums (apply only when referenced in the Service Order):

D. Managed Services SLA Addendum

E. GyverShield SMB SLA Addendum

F. T&M Limited SLA Addendum

G. Data Retention & Backup Addendum

H. Cabling & Professional Services Addendum

END OF MASTER SERVICES AGREEMENT (2026 EDITION)

ATTACHMENT A – CYBERSECURITY INCIDENT RESPONSE

Gyver 2026 Contract Package – V2026.1

1. PURPOSE

This Attachment defines Gyver's process and responsibilities for responding to cybersecurity incidents and establishes the escalation, coordination, and authorization procedures applicable to all Clients.

2. DEFINITION OF A CYBERSECURITY INCIDENT

A Cybersecurity Incident is any event that compromises or threatens the confidentiality, integrity, or availability of systems, data, or credentials. Examples include:

- Ransomware or malware infection
- Unauthorized access or privilege escalation
- Credential theft or account compromise
- Phishing or social-engineering attacks
- Data exfiltration, tampering, encryption, or deletion

Devices or systems not meeting the Security Standards defined in Attachment B may require remediation before incident response can proceed.

3. TIER-3 RESPONSE AND BILLING

Cybersecurity incidents may require senior-level (Tier 3) personnel trained in containment and remediation.

All incident-response services are billed at the Tier-3 or Project rate in the Client's Offer.

Incident response is always out-of-scope from all service tiers (Managed, SMB, T&M).

4. INITIAL CONTAINMENT EFFORT

Gyver will attempt to notify Client before taking action; however, if an active threat is present, Gyver may take immediate containment steps to protect Client systems and prevent further damage. Containment efforts may require up to four (4) hours depending on the nature of the incident. All containment, investigation, remediation, and recovery work performed by Gyver is fully billable. Once immediate risk is mitigated or the four-hour threshold is reached, Gyver will pause and request authorization before proceeding with additional work.

- Isolate compromised systems
- Reset credentials and tokens
- Review SOC alerts and logs
- Implement temporary safeguards
- Communicate initial findings

Gyver may take limited initial containment actions necessary to protect Client systems. These actions may require up to four (4) hours, depending on severity. Once immediate risk is mitigated or the four-hour threshold is reached, Gyver will request authorization before proceeding with any further investigation, remediation, or recovery.

Minor security events that can be resolved by Tier 1 (e.g., password resets, MFA resets, removing malicious inbox rules, or clearing isolated alerts) may be handled without triggering the full incident-response process at Gyver's discretion.

5. AUTHORIZATION FOR CONTINUED WORK

If additional time, advanced remediation, or forensics is required:

- Gyver will pause work once containment is achieved
- Gyver will seek explicit written authorization from Client
- Work will resume only after approval is received

6. THIRD-PARTY AND INSURANCE COORDINATION

If the incident requires external forensic resources:

- Gyver may recommend third-party specialists
- Client may engage them directly or through cyber-insurance
- Gyver may coordinate with the insurer or assigned vendor

Third-party costs are the Client's responsibility.

7. COMMUNICATION DURING EVENTS

During an active incident, Client's designated contact may verbally authorize work.

Gyver will confirm authorization in writing once stable.

Gyver will provide updates and a post-incident summary when available.

8. LIMITATIONS

Gyver's responsibilities under this Attachment are limited to initial containment and remediation support.

Full forensic investigation, legal/regulatory notifications, and extended recovery services require separate written agreements.

9. GOVERNING TERMS

This Attachment forms part of the MSA and supersedes any conflicting terms.

Clients will be notified of material updates.

END OF ATTACHMENT A – CYBERSECURITY INCIDENT RESPONSE

ATTACHMENT B – SECURITY STANDARDS

Gyver 2026 Contract Package – V2026.1

This Attachment defines the minimum technical and security requirements for any system or device to qualify as a **Covered Device** under the MSA and applicable SLA Addendums.

Gyver may refuse support or limit functionality for any device or system that does not meet these standards.

1. ENDPOINT REQUIREMENTS

1.1 Supported Operating Systems

Endpoints must run an operating system currently supported by the vendor, including:

- Windows 10/11
- macOS versions within Apple's support lifecycle
- Any other OS explicitly documented as supported in the Service Order

1.2 Unsupported or Ineligible Systems

The following endpoints are not eligible as Covered Devices:

- Out-of-support Windows versions
- End-of-life macOS versions
- Unsupported or unpatched Linux distributions (unless explicitly approved)
- Devices older than five (5) years unless explicitly listed as Covered
- Systems failing hardware baselines (TPM2, Secure Boot, SSD, etc.)

Devices out of lifecycle or failing hardware baselines are further governed by Attachment C – OEM / End-of-Life Policy.

1.3 Required Security Tools

All endpoints must run Gyver-approved:

- EDR/AV
- RMM monitoring and management agent
- Patch management tooling
- Disk encryption (BitLocker, FileVault, or equivalent)

Removal, tampering, or disabling of any required agent may result in billing or device exclusion.

1.4 Local Administrator Rights

Local administrator access must be restricted.

Gyver may revoke local admin rights on any endpoint that poses a security risk.

2. SERVER & NETWORK REQUIREMENTS

Servers must:

- Be within OEM support lifecycle
- Be enrolled in monitoring and patching
- Use supported file systems, storage, and backup mechanisms

Network equipment must:

- Be business-grade and supported by the manufacturer
- Maintain updated firmware
- Support MFA-secured VPN or Zero Trust access

Public RDP, unrestricted port forwarding, or insecure remote access methods are prohibited.

3. EMAIL & IDENTITY SECURITY

3.1 MFA Requirements

MFA is required for:

- Microsoft 365 users
- Administrative, privileged, and service accounts
- Remote access (VPN, firewalls, cloud admin portals)

3.2 Authentication Standards

Legacy authentication (basic auth, IMAP/POP) must be disabled unless explicitly needed and documented.

3.3 Email Security

Mailboxes must use Gyver-approved:

- Mail filtering
- Anti-phishing controls
- Conditional access policies (when applicable)

4. BACKUP & DATA PROTECTION

Backup scope and responsibilities are defined in the Data Retention & Backup Addendum.

Client retains full responsibility for:

- Any data not included in the backup scope
- Local-only file storage
- Systems not enrolled in the agreed backup plan

5. APPLICATION REQUIREMENTS

Clients must:

- Maintain licensing for all software and LOB applications
- Use supported versions
- Remove unauthorized, high-risk, or pirated software upon request

Gyver may remove or block applications that present security risk.

6. PASSWORD & ACCOUNT STANDARDS

- Minimum password length: 8 characters or a passphrase
- Password reuse and shared accounts discouraged
- Shared accounts require explicit approval
- Client must notify Gyver immediately when employees separate from the organization

Failure to notify Gyver of staff changes may lead to security exposure and billable corrective action.

7. PHYSICAL SECURITY

Covered Devices must:

- Support modern security hardware (TPM, Secure Boot, etc.)
- Be physically secured (locks, access control, secured rooms)
- Not be left unattended in insecure environments

Network equipment must be installed in secure areas only.

8. COMPLIANCE WITH STANDARDS

Non-compliant devices or systems:

- May be excluded from support
- May require billable remediation
- May have reduced service levels
- May result in refusal of service

Gyver will notify Client if systems fall out of compliance and may recommend remediation or replacement options.

9. BYOD (BRING YOUR OWN DEVICE)

BYOD devices:

- Are **not** Covered Devices
- Are **not** eligible for included support
- Must not be used to access corporate resources without MFA, encryption, and mobile security controls
- May require billable remediation if they create a security issue

- May be blocked from network or application access at Gyver's discretion

BYOD access used in violation of these standards may result in incident classification under Attachment A.

10. DORMANT / INACTIVE DEVICES

Dormant Devices are governed primarily by the MSA.

To remain eligible for dormant pricing:

- Device must stay enrolled in security/monitoring tools
- Device must receive patches/updates
- Device must not be used for production work
- Client must declare dormant status before the billing cycle
- Non-compliance voids dormant pricing and may require billable remediation to reactivate

11. CHANGES TO STANDARDS

Gyver may update these standards as threats evolve.

Clients will be notified of material changes.

12. CLIENT OBLIGATIONS & RISK ACCEPTANCE

Client agrees to follow:

- These security standards
- Gyver's security recommendations and advisories
- Required remediations to maintain compliance

If Client refuses required security measures after notification:

- Client assumes all associated risks
- Gyver may decline support or limit services
- Client indemnifies Gyver for losses arising from the refusal

Gyver may notify executive or ownership contacts after repeated refusals.

END OF ATTACHMENT B – SECURITY STANDARDS

ATTACHMENT C – OEM / END-OF-LIFE (EOL) POLICY

Gyver 2026 Contract Package – V2026.1

This Attachment defines Gyver's policies and support limitations for hardware, software, operating systems, and firmware that are **End-of-Life (EOL)**, **End-of-Support (EOS)**, or otherwise outside of vendor support lifecycle.

This Attachment applies to **all Clients and all service tiers** (Managed, SMB, T&M).

1. DEFINITIONS

1.1 OEM

Original Equipment Manufacturer or vendor of hardware, software, or firmware.

1.2 End-of-Life (EOL)

The date the OEM stops selling a product.

1.3 End-of-Support (EOS)

The date the OEM ends security updates, patches, and technical support.

1.4 Unsupported Equipment

Any device, OS, application, or hardware no longer receiving security patches or vendor support.

1.5 Out-of-Compliance System

Any system that fails Attachment B (Security Standards) due to age, unsupported OS/firmware, or inability to run required tools.

2. GYVER SUPPORT LIMITATIONS FOR EOL & UNSUPPORTED SYSTEMS

2.1 Not Eligible for Included Support

EOL, EOS, or unsupported systems are **not eligible** for included support under any SLA.

2.2 Best-Effort Only

If Gyver provides support for such systems, it is strictly **best-effort** with **no guarantees of resolution, stability, or performance.**

2.3 All Work Is Billable

All work on EOL/EOS/unsupported systems is billable at the project or hourly rate defined in the Client's Service Order.

2.4 Monitoring Limitations

Gyver may remove or exclude unsupported systems from:

- RMM tools
- EDR/AV platforms
- Patch management
- Compliance reporting

2.5 Incident-Response Limitations

Unsupported systems may escalate incidents and are governed by **Attachment A – Cybersecurity Incident Response.**

These systems significantly increase risk and may be classified as contributing factors during containment.

3. CLIENT RESPONSIBILITIES

Client must:

3.1 Maintain Supported Hardware & Software

Ensure systems remain within their OEM support lifecycle.

3.2 Approve Recommended Replacements

Follow Gyver's recommendations for upgrades or replacements when hardware, OS, or firmware becomes EOL/EOS.

3.3 Notify Gyver of Unapproved Changes

Unapproved modifications may require billable remediation or re-enrollment.

3.4 Maintain Licensing

Client must maintain valid software licensing to ensure vendor support eligibility.

4. RISK ACCEPTANCE & INDEMNIFICATION

If Client declines recommended upgrades or chooses to operate EOL/EOS systems:

- Client **accepts all associated security and operational risks**
- Client **indemnifies Gyver** for damages, outages, delays, breaches, or losses related to these systems
- Gyver may limit or decline support
- Gyver may notify executive or ownership contacts of risk exposure

This risk acceptance also applies to any **security incidents** involving these systems under Attachment A.

5. REMEDIATION REQUIREMENTS

Gyver may require remediation before providing support when a system:

- Poses a security risk
- Prevents GyverShield tools from functioning properly
- Violates Security Standards (Attachment B)
- Is unstable, misconfigured, or repeatedly failing
- Causes recurring tickets or service degradation
- Creates barriers to providing Managed Services

All remediation is billable.

6. RIGHT TO DECLINE SUPPORT

Gyver may decline or discontinue support for:

- EOL/EOS hardware
- Unsupported OS or firmware
- Systems older than five (5) years
- Devices causing instability or repeated service failures
- Shadow IT or equipment installed without Gyver's involvement
- Any system that cannot meet Attachment B (Security Standards)

Billing does **not** decrease until the device is removed from management and the Service Order is updated.

7. REPLACEMENT TIMELINES

Gyver will notify Client of upcoming EOL/EOS milestones.

Client must either:

- Approve replacement prior to the EOL/EOS date, **or**
- Accept risk in writing (email is sufficient)

For security-critical items, Gyver may impose deadlines to maintain compliance with Attachment B.

Failure to replace critical systems may result in:

- Loss of included support
- Additional billable remediation
- Removal from monitoring platforms
- Declination of further support

8. APPLICABILITY

This Attachment applies to all Clients and all service tiers:

- Managed Services

- GyverShield SMB
- Time & Materials

These policies take precedence over any conflicting expectations or verbal statements.

END OF ATTACHMENT C – OEM / END-OF-LIFE POLICY