

SERVICES CATALOG

This Terms and Conditions is part of an aggregate series of agreements which, combined by reference, create one integrated contract (the "Agreement") between Uprite ("we," or "us," including "our," and "Uprite") and Client ("you," including "your," or "Client"). Each of Uprite and Client may also be referred to as a Party and collectively as the Parties.

For any Quotes, Quotations, Proposals, Statements of Work, Sales Orders or Service Order ("Service Order") agreements executed by you (individually and collectively, "Engagements"), this document and all the applicable documents listed in the tables immediately below ("Included Agreements") are legally integrated as if fully set forth as one Agreement.

Upon each Engagement renewal, this Agreement, but not the terms of any ongoing Engagement, will be superseded by the terms and conditions set forth in the then currently published version of the Agreement available online as of the date on which your services are renewed (the "Renewal Terms"). If you do not agree to the Renewal Terms, you may decline to renew your services.

The Aggregate Set of Agreements between Client and Uprite, the Included Agreements

Applicable Agreements Integrated into All Engagements	Available Online at
Master Services Agreement	https://www.uprite.com/MSA
Service Level Agreement ("SLA")	https://www.uprite.com/SLA
Services Catalog	https://www.uprite.com/SC
Terms and Conditions	https://www.uprite.com/TC
Standard Rates	https://www.uprite.com/rates
Security Standard	https://www.uprite.com/SS

Included Agreements Integrated into Specific Engagements, as Applicable	Available Online at

General

Uprite delivers and prices its technology expertise in the form of Services. It specifies responsibilities for that delivery of expertise, for the delivery of work products from that expertise, or for the delivery of expertise in conjunction with the delivery of technology products or functional services Uprite sells.

Service Unit Pricing

Uprite offers and prices most of its Managed IT Services per Unit, on a variable basis by Unit usage. What comprises a "Unit" is defined by each available Service but is typically (a) a single piece of equipment, (b) an individual user, (c) a configured service instance or user account, or (d) a quantity of provisioned or utilized capacity. Each month, Uprite monitors and determines the number of applicable units billable for each service. This Services Catalog describes the actions that are considered in the scope of the specific service offering that Uprite will take related to each Unit as set forth on a Service Order. Any Managed IT Service that is not billed by the Unit is noted in that service's Special Provisions section.

Service Responsibilities

Because of the all-inclusive nature of information technology in a business, all services provided by Uprite have shared responsibility between Client and Uprite. "Responsibility" means to address/handle and be accountable for the designated item or service. By signing a service agreement with Uprite, you accept all Client Responsibilities as designated for each contracted service. If you do not perform your Responsibilities, Uprite will be unable to provide the services as described.

Normal Service Hours

Unless otherwise stated, Uprite services are offered during our Normal Service Hours, Monday through Friday, excluding observed holidays:

- 8 AM to 5 PM Central

Uprite observes the following holidays:

- New Year's Day
- Good Friday
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving Day
- The Friday immediately following Thanksgiving
- Christmas Eve
- Christmas Day

Managed IT & Support

Included Services

Managed IT & Support includes all services listed in this section for the monthly fee listed herein, limited to the quantity of Supported Users.

- A. Helpdesk support (end-user support)
 - i. Issue triage and ticketing
 - ii. Operating system support and maintenance
 - iii. Support for the operation of Microsoft Office tools
 - iv. Support for third-party applications, subject to limitations specified in Engineering Services, item A.
 - v. Support of company-issued hardware and peripherals
 - a. Keyboard, mouse
 - b. Monitor
 - c. Printer / scanner
 - d. External memory device
 - vi. Maintenance of mainstream browser plug-ins such as Adobe Flash, Adobe Reader, and Java
- B. Server Administration
 - i. Active Directory Administration
 - a. User Access and Security Administration
 - b. User Adds / Changes / Deletes
 - c. DHCP
 - d. DNS
 - ii. Email Administration
 - a. User Mailbox add/change/remove
 - b. Support for shared resources (calendar sharing, etc.)
 - iii. Network file and print services including security permissions on file/folder access and existing network printing functions.
 - iv. Offline Microsoft Exchange database defragmentation services, when required.
 - v. Domain Controller replication configuration and issue resolution
- C. Monitoring

- i. Proactive Network Monitoring & Alerting
 - a. Servers
 - b. Firewalls
 - c. Routers
 - d. Active Directory
 - e. Microsoft Exchange services
 - ii. Trending
 - a. Servers
 - b. Computer workstations
 - c. Networked devices
- D. Patches & Updates
 - i. Managing and maintaining Microsoft Windows Updates and apply critical updates and patches to supported servers and workstations.
 - ii. Weekly server and workstation Maintenance and Patch management
 - iii. Third Party Patching
- E. Basic Cybersecurity Protection - Also see Required Licensing.
 - i. Multi-factor Authentication (MFA) - Prevent credentials compromise and breach of email security. Centrally managed and secured multi-factor authentication for access to the following company resources:
 - a. Servers
 - b. Microsoft 365 Email
 - c. Azure-based authentication (SSO)
 - ii. Email Security - Advanced virus and spam filtering for Hosted Exchange, with message continuity, attachment sandbox evaluation, and URL inspection. Includes email encryption and policy-driven email digital leak protection (DLP).
 - iii. Endpoint Protection - Cloud-native Next-Generation Antivirus with behavioral AI prevention for servers and workstations. Protects against ransomware, known and unknown malware, hacking tools, memory exploits, script misuse, bad macros, and living off the land attacks.
 - iv. Services required to remediate virus or malware related issues. See Cybersecurity Incident Response section for applicable coverage, hours, and conditions.
- F. Mobile device support
 - i. Support for company-issued devices including Active Sync Enabled smartphones. Note: does not include implementation of and upgrades to mobility infrastructure, which would be performed as a Change Order or deliverables-based project at additional cost to Client
 - ii. Services required to configure, troubleshoot, and resolve related to mobile devices and services.
- G. Diagnostics, repair, and issue resolution, limited to Supported Devices
 - i. Desktop / laptop and server hardware diagnostics
 - ii. Desktop / laptop and server hardware repair (excluding cost for any parts). Note: supported device must be covered under warranty.
 - iii. Networking devices
 - iv. Server operating systems and roles, workstation operating systems and productivity tools
 - v. Third-party applications, with limitations specified in Engineering Services, item A
- H. Maintaining and updating Client technology (server / network) documentation
- I. Reviews of standard monitoring reports, technology risks, and technology recommendations with a Client Success Manager (CSM)
- J. Management and administration of Microsoft 365 licenses and IAM services
- K. Data backup administration
 - i. Daily monitoring of backup job status

- ii. End user file restoration operations from backup. Note: does not include configuring backup services, data recovery, forensics, or rebuilding server data stores as part of a drive or server replacement, which would be performed as a Change Order or deliverables-based project at additional cost to Client.
 - iii. Services required to configure, troubleshoot, and resolve issues related to data backup services
- L. Scheduled monthly desktop disk maintenance including:
 - i. Deleting temp files and temporary internet files
 - ii. Disk defragmentation
- M. Provisioning
 - i. Laptop/Desktop Computers - When new computers provisioned for Client, Uprite will charge Client a computer provisioning fee for labor to install and configure applications and migrate data and files. When new computers are purchased from Uprite, Client will be charged \$350 per provisioned computer. When new computers are purchased through other sources, Client will be charged \$500 per provisioned computer. If Client sources computers from vendors other than Uprite, Client will supply vendor quotes to Uprite prior to purchase in order for Uprite to review and ensure that proper equipment is purchased. All computers must conform with Uprite technology standards.
 - ii. Mobile devices
- N. Audio / Video and Conference Equipment: maintenance, support, administration, and issue resolution
- O. Vendor Management: issue ticketing, triage, resolution path determination, vendor communication, system admin support, and escalation for third-party vendors. Note: install, upgrade, repair and issue resolution with third-party vendor software and services subject to limitations in Engineering Services, item A.
- P. Virtual CIO (vCIO): services to assist with technology infrastructure roadmaps, risk analysis, planning, and prioritization, up to the number of hours included in the Service Order, after which vCIO services will be charged on a T&M basis at the rates specified herein.

For included services, after-hours support will be provided at no additional charge to Client.

Uprite may add or change required licensing when deemed necessary. Required licensing and Microsoft licensing prices are subject to change.

Note: Any services not listed in this section will be considered out of scope and billed as Engineering Services (See Engineering Services), as a Change Order, or as deliverables-based project at additional cost to Client.

Technology Roadmap, Documentation, and Onboarding

Setup and provisioning includes the following services and activities and are paid for by the Client as described herein.

- A. Infrastructure Assessment, Initial Roadmap, and Documentation
 - a. Uprite will perform an initial assessment of the existing configurations and overall health of the network and server infrastructure. Uprite will provide an initial proactive roadmap with recommendations on how to improve the stability, reliability, availability, and security of the technology environment.
 - b. Based on assessment findings, Uprite may propose remediation and/or solutions to improve technology stability, reliability, availability, and security to bring Client's environment in-line with Uprite standards. Uprite proposals include defined deliverables and a project budget. Client understands that remediation may be required to be an Uprite managed client.

- c. Uprite will produce documentation of the existing network and server configurations. Network documentation becomes a “living” document that is updated any time there is a change made to the network/server infrastructure. Network documentation is the property of Client and will be available to Client at any time upon written request to the Uprite Client Success Manager (CSM).
 - d. Uprite will establish a hardware refresh plan based on industry best practices to ensure business continuity and technology stability.
 - e. Uprite will identify critical devices and applications, and document Client-specific escalation and after-hours procedures for server administration, issue resolution, and end user assistance requests.
 - f. Uprite will define standard desktop builds, if appropriate, to minimize provisioning time for desktop adds and replacements.
- B. Provisioning Client in Uprite ticketing system
 - C. Provisioning Client in Uprite monitoring system
 - D. Provisioning Spam and Virus filtering
 - E. Provisioning Endpoint Virus / Malware Protection
 - F. Placing Uprite Support Tags with help desk contact information and equipment identifiers on all Supported Devices
 - G. Deploying monitoring agents to servers and customizing service monitors
 - H. Deploying monitoring agents to workstations
 - I. Configuring Microsoft VPN access from Uprite to Client
 - J. Installing remote control tools on servers and workstations
 - K. Providing group and/or one-on-one end user training of the Helpdesk portal and issue submittal procedures

Cybersecurity Incident Response

Uprite structures its incident response services in accordance with the NIST Cybersecurity Framework (CSF) 2.0. Incident response activities correspond to the Respond and Recover functions of the NIST CSF. The scope and pricing of incident response services is determined by the security capabilities active on the Client’s Service Order and confirmed as deployed and managed by Uprite at the time of the incident. Coverage and rates are based on actual deployment status, not Service Order enrollment alone.

Uprite Recommended Security Standard

The Uprite Recommended Security Standard defines the minimum set of security capabilities required for full incident response coverage. The current approved technologies fulfilling each capability are published at <https://www.uprite.com/SS>. Uprite may update approved technologies within each category over time; Clients will be notified of material changes. Required capability categories are:

1. Managed Detection & Response (MDR) — 24/7 SOC-based threat monitoring and response
2. Identity Threat Detection & Response (ITDR) — monitoring and response for identity-based attacks
3. Endpoint Protection — next-generation, behavior-based protection for all supported devices
4. Multi-Factor Authentication (MFA) — enforced on all accounts and systems managed by Uprite
5. Offsite and Immutable Data Backup — managed backup solution stored offsite and protected against modification or deletion

A. Full Standard Deployed

This section applies to Clients for whom all Uprite Recommended Security Standard capabilities are active on the Service Order and confirmed as deployed and managed by Uprite at the time of the incident.

- i. **Included Services — No Additional Charge.** The following incident response activities are included, up to four (4) hours per incident:
 - a. 24/7 alert triage, incident validation, and scope assessment via Uprite's SOC partners
 - b. Endpoint isolation, account lockout, credential resets, and firewall blocks
 - c. Malware removal, closing of initial access vector, and removal of persistence mechanisms
 - d. Client notification and incident communication

- ii. **Billed Services — Standard Rates.** The following services are available and billed at Uprite's then-current published labor rates, beginning after four (4) included hours are consumed per incident:
 - a. Extended investigation beyond initial scope
 - b. System rebuilds, reimaging, or operating system restoration
 - c. Data recovery and restoration from backup
 - d. Confirmed data exfiltration response, including collection of available system logs and event data to the extent retained and accessible within the client environment
 - e. Reintegration of affected systems with extended monitoring
 - f. Post-incident documentation and lessons learned reporting
 - g. Vendor coordination with third-party security resources

For incidents involving confirmed data exfiltration or system restoration affecting multiple devices, Uprite will provide a written scope and estimate prior to proceeding, allowing the Client to make an informed decision before additional charges are incurred.

B. Partial Deployment

This section applies to Clients for whom one or more Uprite Recommended Security Standard capabilities are not deployed at the time of the incident, whether due to Service Order configuration or Client declination of deployment.

- i. **Included Services — No Additional Charge.** Clients with partial deployment receive virus and malware remediation only, up to two (2) hours per incident, at no additional charge. This coverage is limited to: (a) devices on which Uprite's standard endpoint protection has been deployed and is actively managed by Uprite; and (b) incidents confirmed by Uprite as virus or malware in nature. Incidents of any other type — including but not limited to credential compromise, identity-based attacks, data exfiltration, or network intrusion — are not covered under the included hours and will be billed at the rates described below. Incidents on devices where Uprite's endpoint protection is not deployed are not covered and will be billed at the rates described below.

- ii. **Billed Services — Premium Rates.** All incident response work for Clients with partial deployment — including virus and malware remediation beyond the two (2) included hours — is billed at 1.25x Uprite's then-current published labor rates. Work performed outside Normal Service Hours as defined in the Service Level Agreement is billed at 1.5x published labor rates. The full Respond and Recover catalog described in Section A.ii above is available to partial deployment Clients at these premium rates. For incidents involving confirmed data exfiltration or system restoration affecting multiple devices, Uprite will provide a written scope and estimate prior to proceeding.

Uprite recommends that all Clients maintain a cyber liability insurance policy that includes incident response coverage.

Engineering Services are to be used to support Client-specific network functionality, for issue resolution beyond the included services, and for other activities that might be required to properly support the technology environment.

Services that may be provided under this service order and will be charged as Engineering Services include:

- A. Issue resolution, maintenance, installation, updates, and upgrades of software application packages, including but not limited to financial applications (e.g., QuickBooks) and other package applications, beyond the first two hours per incident, issue, installation, or upgrade, and should be performed under a Change Order or as deliverables-based project at additional cost to Client, or will be billed as Engineering Services.
- B. Services required to remediate virus or malware related issues beyond the included hours. See Cybersecurity Incident Response section for applicable hours, rates, and conditions.
- C. Cybersecurity incident response and services to remediate cybersecurity breaches and/or incidents. See Cybersecurity Incident Response section for applicable scope, coverage, and rates.
- D. Installation and upgrades of operating systems (server and workstation).
- E. Creation of new virtual machines.
- F. Installation and provisioning of new servers, storage appliances, and network devices.
- G. Support of migrations from one internet service provider to another, including firewall configuration changes, changing MX records, and testing and troubleshooting the migration.
- H. Services to migrate server data, such as when replacing servers or when re-architecting file share structures.
- I. House-calls: service visits to employee homes and locations other than Client's offices.
- J. Maintenance, support, administration, and issue resolution for any user not identified as a Supported User, or device not identified as a supported device.
- K. Maintenance, support, administration, and issue resolution related to telecommunication systems and equipment when not provided by Uprite.
- L. Maintenance, support, administration, and issue resolution related to physical security systems and equipment, including video cameras, DVRs, access control systems, etc.
- M. It is Client's responsibility to develop and enforce procedures governing Client's employees, vendors, and contractors contacting the Uprite help desk for technical assistance.
- N. Engineering Services cannot be used to perform Project Management Services, Senior Network Architecture and Engineering, and Application Development. These services will be provided via a separate service order as a deliverables-based project at standard bill rates.

Excluded Services

Services rendered under this Service Order do not include the following ("Excluded Services") and if applicable would be performed under a separate service order as a deliverables-based project:

- A. The cost of servicing parts, equipment or software not covered by vendor/manufacture warranty or support or not meeting the minimum standards (See Minimum Standards Required for Services)

- B. The cost of any parts, equipment, or shipping charges of any kind
- C. The cost of any software licensing, software renewal, software maintenance, or software upgrade fees of any kind
- D. The cost of any vendor or manufacturer support or incident fees of any kind
- E. Remediation of cybersecurity risks and implementing of cybersecurity safeguards that are not included in a Service Order
- F. Licensed forensic investigation. In Texas, the analysis of computer-based data for purposes of identifying the conduct or activities of a person, or the preparation of reports intended to secure evidence for use in court or legal proceedings, constitutes a regulated investigative service under Texas Occupations Code §1702.104 (the Texas Private Security Act). Uprite does not hold a license under this Act and does not provide regulated forensic investigation services. Uprite will assist clients with operational recovery activities, including data restoration, system recovery, collection of available system logs and event data to the extent retained and accessible, and answering questions regarding the nature, timing, and scope of an incident based on evidence available within the client environment. Uprite does not represent that system logs will be complete, intact, or sufficient to reconstruct all incident activity. This assistance does not constitute licensed forensic investigation, does not include the preparation of forensic reports attributing conduct to specific individuals, and is not intended or represented as suitable for use in criminal proceedings or civil litigation. Clients requiring licensed forensic investigation services should engage a qualified, licensed forensic firm.
- G. Services required to bring Client's environment up to minimum standards required for services.
- H. Services required due to Acts of God, heating / cooling / humidity issues, building modifications, fire, lightning, power surge, other electrical failures and disruptions, or other circumstances beyond the control of Uprite.
- I. Installation of third-party applications not listed in the included services.
- J. Programming (modification of software code) and program (software) maintenance
- K. Development of and updates to end user reports.
- L. Training services of any kind.
- M. Special Requests – special requests involving technologies or software will be discussed and approved with Client and would result in additional cost to Client (e.g., hardware refresh, software upgrades for multiple machines in short time frame).
- N. Other services not listed in the included services (See Included Services) or provided as engineering services (See Engineering Services).

Uprite provides a wide range of information technology services including Azure migration services, email and file server migrations to Microsoft 365, Microsoft SharePoint implementation, VoIP services, business continuity planning and assessment, and HIPAA assessments, but not under this Service Order. Uprite can provide deliverables-based proposals for information technology services such as these Excluded Services.