SURETY TECHNOLOGIES INCORPORATED
4617 S 139th St, Omaha, NE 68137 | (402) 896-4261 | info@suretytek.com | suretytek.com

Services Guide

Companion document to the Surety Master Services Agreement • Last Updated: August 10, 2026

1. ABOUT THIS SERVICES GUIDE

This Services Guide contains provisions that define, clarify, and govern the scope of the services described in the quote that has been provided to you (the "Quote"), as well as the policies and procedures that we follow (and to which you agree) when we provide a service to you or facilitate a service for you. If you do not agree with the terms of this Services Guide, you should not sign the Quote and you must contact us for more information.

This Services Guide is our "owner's manual" that generally describes all managed services provided or facilitated by Surety Technologies Incorporated ("Surety," "we," "us," or "our"); however, only those services specifically described in the Quote will be facilitated and/or provided to you (collectively, the "Services").

This Services Guide is governed under our Master Services Agreement ("MSA"). You may locate our MSA through the link in your Quote or, if you want, we will send you a copy of the MSA by email upon request. Capitalized terms in this Services Guide will have the same meaning as the capitalized terms in the MSA, unless otherwise indicated below.

Activities or items that are not specifically described in the Quote will be out of scope and will not be included unless otherwise agreed to by us in writing.

This Services Guide contains important provisions pertaining to the auto-renewal of the Services in the Quote, as well as fee increases that may occur from time to time. Please read this Services Guide carefully and keep a copy for your records.

2. INITIAL AUDIT / DIAGNOSTIC SERVICES

In the Initial Audit/Diagnostic phase of our services, we audit your managed information technology environment (the "Environment") to determine the readiness for, and compatibility with, ongoing managed services. Our auditing services may be comprised of some or all of the following:

- Audit to determine general Environment readiness and functional capability
- Review of hardware and software configurations
- Review of current vendor service / warranty agreements for Environment hardware and software
- Basic security vulnerability check
- Basic backup and file recovery solution audit
- Speed test and ISP audit
- Print output audit
- Office telephone vendor service audit
- Asset inventory

- Email and website hosting audit
- IT support process audit

If deficiencies are discovered during the auditing process (such as outdated equipment or unlicensed software), we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of the Services and provide you with options to correct the deficiencies. Please note, unless otherwise expressly agreed by us in writing, auditing services do not include the remediation of any issues, errors, or deficiencies ("Issues"), and we cannot guarantee that all Issues will be detected during the auditing process. Issues that are discovered in the Environment after the auditing process is completed may be addressed in one or more subsequent quotes.

3. ONBOARDING SERVICES

In the Onboarding phase of our services, we will prepare your IT environment for the monthly managed services described in the Quote. During this phase, we will work with your Authorized Contact(s) to review the information we need to prepare the targeted environment, and we may also:

- Uninstall any monitoring tools or other software installed by previous IT service providers.
- Compile a full inventory of all protected servers, workstations, and laptops.
- Uninstall any previous endpoint protection and install our managed security solutions (as indicated in the Quote).
- Install remote support and management agents (i.e., software agents) on each managed device to enable remote support.
- Configure Windows® and application patch management agent(s) and check for missing security updates.
- Secure administrative access to Client's Microsoft 365 tenant, apply our baseline security standards, and enroll users in multi-factor authentication.
- Deploy email threat protection and update email authentication records (SPF, DKIM, and DMARC) for Client's domains.
- Collect, rotate, and securely document administrative credentials for the Environment.
- Document the Environment, including network configuration, assets, and vendor and internet service provider account information.
- Uninstall unsafe applications or applications that are no longer necessary.
- Optimize device performance including disk cleanup and endpoint protection scans.
- Review firewall configuration and other network infrastructure devices, and back up network device configurations.
- Review status of battery backup protection on all mission critical devices.
- Review and document current server configuration and status.
- Deploy the backup services indicated in the Quote and verify completion of an initial successful backup.
- Determine existing business continuity strategy and status; prepare backup and recovery options for consideration (see Backup & Recovery Planning above).
- Review password policies and update user and device passwords.

- Introduce end users to our support process, including how to submit support requests.
- As applicable, make recommendations for changes that should be considered to the managed environment.

This list is subject to change if we determine, at our discretion, that different or additional onboarding activities are required.

If deficiencies are discovered during the onboarding process, we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of our monthly managed services. Please note, unless otherwise expressly stated in the Quote, onboarding-related services do not include the remediation of any issues, errors, or deficiencies ("Issues"), and we cannot guarantee that all Issues will be detected during the onboarding process.

The duration of the onboarding process depends on many factors, many of which may be outside of our control, such as product availability/shortages, required third party vendor input, etc. As such, we can estimate, but cannot guarantee, the timing and duration of the onboarding process. We will keep you updated as the onboarding process progresses.

4. ONGOING / RECURRING SERVICES

Ongoing/recurring services are services that are provided to you or facilitated for you on an ongoing basis and, unless otherwise indicated in a Quote, are billed to you monthly. Some ongoing/recurring services will begin with the commencement of onboarding services; others will begin when the onboarding process is completed. Please direct any questions about start or "go live" dates to your technician.

5. MANAGED SERVICES

Bundled Services. If the Quote indicates that Services are billed on a "per user" or "per device" basis as a single combined fee, the services included in that fee (the "Bundle") are those components described in this Services Guide that are designated as included in the Bundle. The Bundle is a single, indivisible service offering and is not a sum of individually priced components. Surety may, in its reasonable discretion, add to, remove, or replace individual components of the Bundle, provided that the overall scope of the Bundle is not materially diminished. Client acknowledges that the Bundle price is a single, integrated fee; no partial refunds, credits, or price adjustments will be made for unused or discontinued components.

Each service described in this Services Guide is designated as `INCLUDED` (a component of the SureIT Managed User bundle), `ADD-ON` (available for an additional recurring fee as indicated in the Quote), or `SEPARATE QUOTE` (provided under a separate quote or on a time and materials basis). The current designations are summarized below:

INCLUDED IN SUREIT MANAGED USER	AVAILABLE AS AN ADD-ON	SEPARATE QUOTE
• Remote Helpdesk • Basic Network Monitoring & Maintenance	• Backup and File Recovery • Server Monitoring & Maintenance • Email Archiving	• Prepaid Block Hours • Project Labor

- Remote Monitoring and Management Agent
- Workstation Monitoring & Maintenance
- Updates & Patching
- Endpoint Antivirus & Malware Protection
- Email Threat Protection
- DNS Threat Protection
- Microsoft 365 Management & Security
- Microsoft 365 Backup
- Backup & Recovery Planning
- Privileged Access Management
- Expert Solution Planning

- Security Information & Event Management (SIEM)
- Extended Detection & Response (XDR)
- End User Security Awareness Training
- Vulnerability Management
- Password Manager
- Two Factor Authentication
- Mobile Device Management
- Managed VPN
- Cloud Server & Cloud Desktop Hosting
- Printer Management
- Network as a Service (NaaS)
- Network Operations Center (NOC)
- Front of Line Response
- Recurring On-Site Technician
- Email-Only User
- Extra Workstations
- PDF Editing Software
- HIPAA Compliance Program Facilitation
- VoIP Services Facilitation

- Penetration (Pen) Testing
- Vulnerability Scanning
- IT Consulting

Backup and File Recovery ADD-ON

Implementation and facilitation of a top-tier, image-based backup and file recovery solution from our designated Third Party Provider. Features include:

- Image-based backups of covered servers and workstations, capturing the full system (operating system, applications, settings, and data).
- Two deployment options, as indicated in the Quote: (i) an onsite backup appliance ("Backup Appliance") with replication to secure cloud storage, or (ii) direct-to-cloud backup with no onsite appliance.
- Immutable copies of backed up data retained in the cloud to protect against ransomware and accidental or malicious deletion.
- Automated, recurring backup integrity checks.
- Recovery options ranging from individual files and folders to full system images, including virtualization of protected systems locally or in the cloud for business continuity purposes.
- Offsite backup of supported network-attached storage (NAS) devices to secure cloud storage, where indicated in the Quote.
- Monitoring of the backup system, including monitoring of backup successes and failures, and troubleshooting and remediation of failed backups.
- Firmware and software updates of the Backup Appliance (if deployed).

Backup Data Security: All backed up data is encrypted in transit and at rest using 256-bit AES encryption. Cloud copies of backed up data are stored in secure datacenters that implement physical security controls and redundant internet connectivity.

Backup Retention: Backed up data will be retained on a rolling thirty (30) day basis unless a different time period is expressly stated in the Quote. This applies to both local and cloud backups.

Recovery of Data: If you need to recover any of your backed up data, then the following procedures will apply:

- **Service Hours:** Backed up data can be requested during our normal business hours, which are currently 8:00 AM to 5:00 PM Central, Monday through Friday.
- **Request Method.** Requests to restore backed up data should be made through one of the following methods:
  - Email: help AT suretytek.com
  - Telephone: 402-896-4261
- **Restoration Time:** We will endeavor to restore backed up data as quickly as possible following our receipt of a request to do so; however, in all cases data restoration services are subject to (i) technician availability and (ii) confirmation that the restoration point(s) is/are available to receive the backed up data.

Backup & Recovery Planning INCLUDED

Development and maintenance of a backup and recovery strategy for Client's critical data and systems. Features include:

- Identification of Client's critical data, systems, and resources.
- Definition of Client's tolerances for recovery time and data loss.
- Development of a backup and recovery strategy using the backup solutions described in this Services Guide, with recommended backup services reflected in the Quote.
- Annual review of the backup and recovery strategy, with updated recommendations as Client's environment and needs change.

Note: Backup & Recovery Planning is a planning and advisory service. The backup services themselves (such as Backup and File Recovery and Microsoft 365 Backup) are provided as described in their respective sections and as indicated in the Quote.

Basic Network Monitoring & Maintenance INCLUDED

- Basic 24x7x365 automated monitoring of covered network devices' online status.
- Management of covered network devices, including configuration changes as reasonably needed.
- Patch management for covered network devices, including deployment of firmware and software updates as deemed necessary by Surety.
- Backup of covered network device configurations to support recovery and device replacement.

Prepaid Block Hours SEPARATE PURCHASE

If you purchase one or more blocks of prepaid technical support or consulting hours from Surety, then we will provide our professional information technology consulting services to you from time to time on an ongoing, “on demand” basis (“Block Hour Services”). Block Hour Services are a subset of the Services, and this section governs only Block Hour Services.

Client may purchase Prepaid Block Hours through a Quote or invoice identifying the number of hours, price, and any applicable scope, timing, term, or limitations (a “Block Order”). A Block Order becomes binding when Client signs or electronically accepts it, confirms acceptance by email, or pays the invoice. When payment is electronic, the associated payment record constitutes an electronic record of Client’s acceptance. A Block Order supplements, but does not amend or override, an existing Quote, the MSA, or this Services Guide unless the Block Order is a Surety-initiated amendment that satisfies the “Amendment” provision of the MSA. Surety’s performance or delivery alone does not constitute Client’s acceptance of a Block Order.

The specific scope, timing, term, and pricing of the Services (collectively, “Specifications”) will be determined between you and us at the time that you request the Services from us.

You and we may finalize the Specifications (i) by exchanging emails confirming the relevant terms, or (ii) by you agreeing to an invoice, purchase order, or similar document we send to you that describes the Specifications (an “Invoice”), or in some cases, (iii) by us performing the Services or delivering the applicable deliverables in conformity with the Specifications.

An email or Invoice may confirm Specifications for a particular request within an accepted Block Order, but does not amend or override the Block Order, a Quote, the MSA, or this Services Guide. If requested Specifications would differ from an existing Block Order or Quote, Surety will issue a replacement Quote for Client’s acceptance or a written amendment that satisfies the “Amendment” provision of the MSA.

A Service will be deemed completed upon our final delivery of the applicable portions of Specifications unless a different completion milestone is expressly agreed upon in the Specifications (“Service Completion”). (For example, sales of hardware will be deemed completed when the hardware is delivered to you; licensing will be completed when the licenses are provided to you, etc.) Acceptance of, and the reporting of any defects or deviations from the Specifications in, a completed Service is governed by the “Services Warranty; Acceptance” provisions of the MSA. Issues or remedial activities that fall outside of those provisions will be billed to you at our then-current hourly rates.

Unless we agree otherwise in writing, Services will be provided only during our normal business hours, which are currently 8:00 AM to 5:00 PM Central, Monday through Friday. Services provided outside of our normal business hours are subject to increased fees and technician availability and require your and our mutual consent to implement.

The priority given to implementing the Services will be determined in our reasonable discretion, considering any milestones or deadlines expressly agreed upon in an invoice or email from Surety. If no specific milestone or deadline is agreed upon, then the Services will be performed in accordance with your needs, the specific requirements of the job(s), and technician availability.

Cloud Server & Cloud Desktop Hosting ADD-ON

Implementation, configuration, and ongoing management of cloud-hosted servers and/or cloud-hosted desktops on an industry-leading cloud platform from our designated Third Party Provider.

- Hosted resources may be provisioned in Client's own cloud tenant and subscription, or in a cloud environment provisioned and managed by Surety, as indicated in the Quote. Where resources are provisioned in Client's own tenant, Client owns and controls the subscription, and Surety manages the hosted resources on Client's behalf.
- Provisioning and configuration of cloud servers and/or cloud desktops, including operating system deployment, network configuration, and secure access setup.
- Ongoing monitoring, patching, and maintenance of managed cloud resources in accordance with the Service Levels described below.

Please note: Cloud platform consumption fees are usage-based, are billed under the cloud provider's terms, and may fluctuate from month to month based on Client's actual usage. Consumption fees may begin to accrue before the "go-live" date of other Services (see "Reconciliation" in the Fees section below). Availability and uptime of the cloud platform are governed by the cloud provider's own terms and service level commitments, and are not warranted or guaranteed by Surety. Cloud-hosted services require a reliable, always-connected internet solution.

DNS Threat Protection INCLUDED

Implementation and facilitation of an industry-recognized DNS filtering and web protection solution from our designated Third Party Provider. Features include:

- Blocking of known malicious websites, including phishing, malware, and command-and-control domains.
- Category-based content filtering of unwanted or inappropriate web content, configured in consultation with Client.
- Protection for managed devices both on and off the managed network.
- Web activity and threat reporting available on request.

Please see the Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details. No filtering solution will block all malicious or unwanted content.

Email Archiving ADD-ON

Implementation and facilitation of an industry-recognized email archiving solution from our designated Third Party Provider. Features include:

- Automatic capture and preservation of inbound, outbound, and internal email messages for archived mailboxes.
- Archived messages are retained in secure, tamper-evident storage and encrypted in transit and at rest.
- Search and export capabilities to assist with Client's legal, regulatory, or internal record-keeping needs.
- Archived data will be retained for the period indicated in the Quote.

Note: Email archiving is a message retention service only and is not a backup and file recovery solution. Please see the Microsoft 365 Backup section for mailbox backup services.

Email-Only User ADD-ON

An “Email-Only User” is a user identified in the Quote who does not use a managed workstation. For each Email-Only User, the following Services are provided for that user’s account and mailbox:

- Email threat protection (as described in the Email Threat Protection section).
- Identity threat detection and response monitoring of the user’s account (as described in the Microsoft 365 Management & Security section).
- Cloud-to-cloud backup of the user’s mailbox and associated cloud data (as described in the Microsoft 365 Backup section).

Please note: Support for Email-Only Users is limited to email and account-related issues. Email-Only Users are not entitled to the Business Device included in standard “per user” billing (see Covered Environment below), and device-related support for Email-Only Users is out of scope unless otherwise agreed in writing.

Email Threat Protection INCLUDED

Implementation and facilitation of a trusted email threat protection solution from our designated Third Party Provider. Features include:

- Managed email protection from phishing, business email compromise (BEC), SPAM, and email-based malware.
- Artificial intelligence and machine learning analysis of inbound, outbound, and internal email to detect phishing and social engineering attacks such as whaling, CEO fraud, and invoice fraud.
- Scanning and emulation of attachments and links to detect malware and malicious websites before delivery.
- Protection against impersonation attacks, including display name spoofing and “look-alike” domain names.
- Management of email authentication records (SPF, DKIM, and DMARC) for Client’s domains, including ongoing monitoring of authentication reporting to detect spoofing of Client’s domains and unauthorized senders.
- Quarantine management and end-user notification of blocked or held messages.

Please see the Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details. All hosted email is subject to the terms of our Hosted Email Policy and our Acceptable Use Policy.

Endpoint Antivirus & Malware Protection INCLUDED

Implementation and facilitation of a top-tier, cloud-native endpoint protection platform from our designated Third Party Provider. This service covers managed workstations and managed servers expressly identified as covered in the applicable Quote. Features include:

- Next-generation antivirus using artificial intelligence, machine learning, and behavioral analysis to block malware, ransomware, and fileless attacks, including malicious scripts and macros.
- Software agents deployed to managed laptops and desktops and, when expressly covered in the applicable Quote, managed servers across supported operating systems.
- Endpoint detection and response (EDR): continuous recording of endpoint activity to support threat detection, investigation, and root cause analysis.
- Remote response capabilities, including network containment (isolation) of a compromised endpoint to prevent the spread of a threat.
- Cloud-delivered threat intelligence, with endpoint telemetry retained in the platform to support investigations.

Please see the Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.

Extended Detection & Response (XDR) ADD-ON

Implementation and facilitation of an industry-recognized extended detection and response platform from our designated Third Party Provider. Features include:

- Collection and correlation of security telemetry from across the managed environment, which may include endpoints, network devices, servers, and cloud services.
- Threat detections developed and maintained by the Third Party Provider, updated as new threats emerge.
- Automated response capabilities, which may include isolation of a compromised endpoint in response to critical threats and automated blocking of traffic from known malicious sources.
- Prioritized findings with recommended response steps.
- Deception (honeypot) sensors that provide early detection of unauthorized activity inside the managed network, where deployed.
- Escalation support from the Third Party Provider for urgent, priority findings.

Remediation of detected threats beyond the automated response actions described above may be provided on a time and materials basis. Please see the Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.

End User Security Awareness Training ADD-ON

Implementation and facilitation of a security awareness training solution from our designated Third Party Provider. Features include:

- Online, on-demand training modules covering phishing, social engineering, and other common security threats (multi-lingual).
- Simulated phishing email campaigns, which may be automatically generated and personalized based on real-world attack patterns, or configured from administrator-defined templates.
- Tracking and reporting of training completion and simulation results.

Please see the Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.

Expert Solution Planning INCLUDED

Assistance identifying technology problems and opportunities within Client's business and mapping out practical solutions. Features include:

- Consultation to help identify and define the underlying problem or business need.
- Research and recommendation of appropriate solutions, including hardware, software, and service options.
- Scoping and planning of the recommended solution.

Note: Implementation of a recommended solution is performed as a separately quoted project (see the Fees section below and the Procurement policy toward the end of this Services Guide). Solution planning is advisory in nature, and we do not warrant or guarantee any particular business outcome.

Extra Workstations ADD-ON

Standard "per user" billing includes one (1) Business Device per licensed user (see Covered Environment below). If a user requires more than one managed workstation, each additional workstation may be added as an "Extra Workstation" for an additional per-device fee as indicated in the Quote. Each Extra Workstation includes:

- Remote monitoring and management agent.
- Next-generation antivirus and endpoint protection (as described in the Endpoint Antivirus & Malware Protection section above).
- DNS threat protection / malicious website blocking (as described in the DNS Threat Protection section below).
- Privileged access management (as described in the Privileged Access Management section below).

Extra Workstations are Covered Hardware. Each Extra Workstation receives the services listed above together with Updates & Patching, Workstation Monitoring & Maintenance, and Remote Helpdesk support, on the same terms as other covered workstations.

Front of Line Response ADD-ON

If the Quote includes Front of Line Response, support requests submitted by Client will be placed at the front of our support queue, ahead of standard-priority requests from other clients.

- Applies to support requests received through our designated support channels during our normal business hours.
- Requests remain subject to severity-based triage; a higher-severity issue affecting another client may still be addressed first where reasonably necessary.
- Front of Line Response prioritizes the order in which requests are addressed; it does not modify the response time targets in the Service Levels section below and does not constitute a guarantee of resolution within any specific time period.

HIPAA Compliance Program Facilitation ADD-ON

For Clients subject to the Health Insurance Portability and Accountability Act ("HIPAA"), we can facilitate Client's enrollment in a HIPAA compliance program offered by an independent Third Party Provider. Compliance program features (such as risk assessments, policy templates, workforce training, and compliance documentation) are provided solely by the Third Party Provider under its own agreement with Client.

Please note: Surety does not provide HIPAA compliance services, and we are not a compliance auditor, compliance consultant, or law firm. Enrollment in a compliance program, and/or the implementation of technical safeguards by Surety as described in a Quote, does not by itself make Client HIPAA compliant, and we do not warrant or guarantee that Client will achieve or maintain compliance with HIPAA or any other law or regulation. Client is and remains solely responsible for its own regulatory compliance, and we strongly recommend that Client consult with competent legal counsel regarding its compliance obligations.

Managed VPN ADD-ON

Implementation and facilitation of an industry-recognized secure remote network access (VPN) solution from our designated Third Party Provider. Features include:

- Encrypted, point-to-point connectivity between enrolled devices, networks, and designated resources.
- Zero trust access policies that limit connectivity based on user, device, and resource.
- Central management of device enrollment, encryption keys, and access policies.
- Integration with Client's identity provider for single sign-on and multi-factor authentication, where applicable.

Note: VPN services require a reliable internet connection at each participating location and device. Connection speed and quality depend on the underlying internet connections, and we do not warrant or guarantee uninterrupted or error-free VPN connectivity.

Microsoft 365 Backup INCLUDED

Implementation and facilitation of an industry-recognized cloud-to-cloud backup solution from our designated Third Party Provider. Features include:

- Automated daily backup of covered Microsoft 365 data, which may include mailboxes, calendars, contacts, cloud file storage, and collaboration site data (as indicated in the Quote).
- Backed up data is stored in secure cloud storage, separate from Client's Microsoft 365 tenant, and encrypted in transit and at rest.
- Granular restore capabilities at the item, folder, mailbox, or account level.
- Backed up data will be retained for the period indicated in the Quote.
- Monitoring of backup successes and failures.

Note: Native Microsoft 365 retention features are not a backup solution. Requests to restore backed up Microsoft 365 data follow the "Recovery of Data" procedures described in the Backup and File Recovery section above.

Microsoft 365 Management & Security INCLUDED

Administration, hardening, and security monitoring of Client's Microsoft 365 tenant. Features include:

- **Tenant Administration:** Management of users, licenses, mailboxes, groups, and tenant-level settings; user onboarding and offboarding support.
- **Consolidated Billing:** Microsoft 365 licenses may be purchased and billed through Surety (see "Access Licensing" in the Fees section below for important license terms).
- **Tenant Hardening:** Application of security baseline standards to the managed tenant using an industry-recognized tenant management platform, with ongoing monitoring for configuration drift and remediation of deviations from the established baseline.
- **Identity Threat Detection & Response:** Continuous monitoring of sign-in activity and identity-related events in the managed tenant using an industry-recognized identity threat detection solution from our designated Third Party Provider; detection of suspicious activity such as anomalous sign-ins, unauthorized mailbox rules, and indicators of account compromise; alerting and response actions, which may include disabling affected accounts and terminating active sessions.
- **Encrypted Email:** Configuration and support of encrypted email capabilities included with Client's Microsoft 365 licensing.

Blumira's identity-threat-detection telemetry consists of security event logs, user metadata, and access-attempt information. Blumira does not store electronic protected health information (ePHI). If a Service will create, receive, maintain, or transmit ePHI on Client's behalf, the MSA's Business Associate Agreement requirement applies before that Service begins.

Please see the Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details. No security solution is 100% effective, and we do not warrant or guarantee that all threats to the managed tenant will be detected or prevented.

Mobile Device Management (MDM) ADD-ON

Implementation and facilitation of an industry-recognized mobile device management solution. Features include:

- Enrollment of Client-owned devices (and, where expressly agreed, personal devices) into the managed platform.
- Deployment of configuration profiles, compliance policies, and device access requirements to enrolled devices.
- Deployment and updating of approved applications on enrolled devices.
- Remote lock and selective removal of managed Client data, where supported.

Please note: Support for personal (BYOD) devices is limited to these management functions; hardware, carrier, and personal application issues are out of scope. Surety does not factory-reset personal devices or remove personal data. Remote actions require a responsive, powered-on, internet-connected device, and removal of all managed Client data is not guaranteed.

Network as a Service (NaaS) ADD-ON

If indicated in the Quote, Surety will supply, install, and manage network hardware at Client's premises on a subscription basis ("NaaS Equipment"). NaaS Equipment may include gateway/firewall appliances, network switches, and wireless access points from our designated hardware provider. Features include:

- NaaS Equipment is centrally managed through a cloud-based management platform, enabling remote configuration, monitoring, and alerting.
- Managed gateway/firewall appliances help to prevent unauthorized access to internal network(s) from outside the network(s), and include stateful firewalling, intrusion detection and prevention (IDS/IPS), website/content filtering, and secure and encrypted remote access and site-to-site VPN capabilities, as supported by the deployed hardware. Please note: gateway appliances do not perform antivirus scanning of network traffic; malware protection is provided at the endpoint level (see Endpoint Antivirus & Malware Protection above).
- Wireless access points are installed to provide wireless coverage in areas agreed upon by Surety and Client. Wireless connectivity support is provided on a "best efforts" basis, and Client understands that some end-user devices may not connect to, or perform well on, the wireless network.
- Firmware updates applied as deemed necessary by Surety.
- Replacement of failed NaaS Equipment (normal wear and tear) at no additional charge, subject to hardware availability.

The following terms apply to all NaaS Equipment:

- NaaS Equipment is and remains the sole property of Surety. Client acquires no ownership interest in NaaS Equipment.
- Client must not move, modify, reconfigure, or affix or install any accessory, addition, or upgrade to NaaS Equipment without our prior written consent.
- Upon termination of the applicable Services, all NaaS Equipment must be returned in accordance with the Term; Termination section of this Services Guide. Client will be responsible for the replacement value of missing or damaged (normal wear and tear excepted) NaaS Equipment.

Network Operations Center (NOC) ADD-ON

NOC services are focused exclusively on network devices, such as gateway/firewall appliances, switches, wireless access points, and other supported network hardware identified in the Quote, and may be purchased as an add-on to other managed services or as a standalone service under its own Quote. Features include:

- 24x7x365 automated monitoring of covered network devices, including online status, performance, and device health, with alerting to our network operations team.
- Management of covered network devices, including configuration changes as reasonably needed.
- Patch management for covered network devices, including deployment of firmware and software updates as deemed necessary by Surety.
- Backup of covered network device configurations to support recovery and device replacement.
- Coordination with Client's designated onsite contacts and with Client's internet service provider(s) during alert response, as reasonably needed to facilitate remediation.
- Response to alerts during our normal business hours in accordance with the Service Levels described below.
- For critical alerts received outside of normal business hours, we will endeavor to respond on a "best efforts" basis, subject to technician availability. After-hours response is not guaranteed, and after-hours remediation work is billed as Non-Business Hour Support (see the Service Levels section below).

Please note: NOC services cover only the network devices identified in the Quote. Support for workstations, servers, applications, end users, and other portions of the Environment is not included and, if requested, will be provided under a separate service or billed on a time and materials basis. Where NOC services are provided on a standalone basis, references in this Services Guide to Covered Hardware and the Environment apply only to the covered network devices.

Password Manager ADD-ON

Implementation and facilitation of industry-leading password management protection solution from our designated Third Party Provider. Features include:

- **Secure Vaults:** Encrypted vaults for storing passwords and other sensitive items, such as payment cards, identities, and secure notes.
- **Password Generation:** Generate strong, unique passwords with editable options to meet specific criteria.
- **Shared Vaults:** Team-based shared vaults with permission controls, allowing credentials to be shared securely within Client's organization.
- **Browser Extension:** Browser extension with automatic form filling for easy, secure sign-ins.
- **Mobile App:** Mobile apps provide access to vaults and stored items on smartphones and tablets.
- **Credential Health Monitoring:** Built-in monitoring that flags weak, reused, or compromised passwords that appear in known data breaches.

PDF Editing Software ADD-ON

Licensing of a business-grade PDF editing application from our designated Third Party Provider, resold on a per-user or per-device basis as indicated in the Quote. Features include:

- Creation, editing, conversion, and annotation of PDF documents.
- Installation and deployment of the application on managed devices.
- License management through Surety (see the Software Licensing section below).

The application is licensed, not sold, and is subject to the vendor's end user license agreement. Support beyond installation and basic configuration is facilitated with the software vendor on a best-effort basis.

Penetration (Pen) Testing SEPARATE QUOTE

Penetration testing (or "pen" testing) simulates a cyberattack against your IT infrastructure to identify exploitable vulnerabilities. Unlike ongoing vulnerability scanning services that provide a constant, static level of network scanning, pen testing may involve several stages of reconnaissance and actual attack methodologies (such as brute force attacks and/or SQL injection attacks) and may include unconventional and targeted attacks that occur during business and non-business hours. Pen testing may consist of any of the following:

- **External Pen Testing:** Exposes vulnerabilities in your internet-facing systems, networks, firewalls, devices, and/or web applications that could lead to unauthorized access.
- **Internal Pen Testing:** Validates the effort required for an attacker to overcome and exploit your internal security infrastructure after access is gained.
- **PCI Pen Testing:** Using the goals set by the PCI Security Standards Council, this test involves both external and internal pen testing methodologies.
- **Web App Pen Testing:** Application security testing using attempted infiltration through a website or web application utilizing PTES and the OWASP standard testing checklist.

Please see additional terms for Penetration Testing below.

Printer Management ADD-ON

Implementation and facilitation of an industry-recognized cloud print management solution from our designated Third Party Provider. Features include:

- Centralized deployment of print queues and printer drivers to managed devices.
- Monitoring of managed print infrastructure and print-related alerting.
- User self-service printer installation on managed devices.
- Secure print release functionality, where supported by Client's printer hardware.

Please note: Printer management covers print software and queue management only. Printer hardware repair, physical maintenance, and consumables (such as toner and drums) are not included; if requested, we will facilitate hardware service with the applicable printer vendor on a time and materials basis.

Privileged Access Management (PAM) INCLUDED

Implementation and facilitation of an industry-recognized endpoint privilege management solution from our designated Third Party Provider. Features include:

- Removal of standing local administrator rights from end users on managed endpoints.
- Just-in-time elevation requests, with approval workflows handled by our technicians in accordance with the Service Levels described below.
- Application-level privilege rules that permit approved applications to run with elevated rights without exposing administrator credentials to end users.
- Audit logging of elevation requests and privileged activity on managed endpoints.

Note: Because standing administrator rights are removed, some software installations and system changes on managed endpoints will require an elevation request and our approval. This is by design and is an important part of the security value of this service.

Project Labor SEPARATE QUOTE

Project-based professional services performed under a separate quote. The specific scope of work for each project (the "Project Scope") will be described in the applicable Quote. Projects may include, by way of example and not limitation:

- Deployment of new or replacement workstations, including setup, agent and security software installation, domain or tenant join, application installation, and transfer of user data and profiles.
- Server deployments, migrations, and upgrades.
- Network design, infrastructure refresh, and new office buildouts.
- Cloud and email platform migrations.
- Office moves and equipment relocations.
- Other technology projects described in a Quote.

Fees; Fixed Fee; Hidden Conditions. Unless otherwise stated in the Quote, the quoted project fee is fixed for the Project Scope. If Surety identifies a pre-existing, hidden, or undisclosed condition in the Environment (for example, deficient cabling, a corrupted directory service, unsupported or failing hardware, or undocumented configurations) that requires work beyond the Project Scope, Surety will notify Client in writing. Where the additional work is reasonably expected to cost the lesser of ten percent (10%) of the quoted project fee or five hundred dollars ($500), Surety may proceed and invoice that work at our then-current hourly rates following notice to Client. For additional work above that threshold, Surety will provide a written change order describing the condition, the additional work, the pricing, and any anticipated schedule impact, and will not perform or bill that work unless Client accepts the change order in accordance with the Change Orders section below. If Client does not accept the change order, Surety may suspend the affected portion of the project and the project schedule may be adjusted accordingly.

Payment Terms. Fifty percent (50%) of the quoted project fee is due in advance before work begins. For projects with a quoted fee of more than $5,000, the remaining balance will be invoiced against completion milestones if milestones are identified in the Quote, and otherwise upon completion. For all other projects, the remaining balance is invoiced upon completion.

Scheduling; Rates. Project work is scheduled in advance and is subject to technician availability and, where applicable, hardware and licensing availability. Unless otherwise stated in the Quote, project work is performed during our normal business hours; work performed outside of normal business hours is subject to the increased rates described in the Service Levels section below. Onsite project work is subject to the two (2) hour minimum charge described in the Service Levels section below. Project labor does not draw from prepaid remote support time; however, project labor may be applied against Prepaid Block Hours purchased by Client.

Scope Changes; Acceptance. Changes to the Project Scope are governed by the Change Orders section below. Acceptance of completed project work, and the reporting of any defects or non-conformance, are governed by the "Services Warranty; Acceptance" provisions of the MSA.

Exclusions. Unless expressly included in the Quote, project fees do not include: data or voice cabling and wiring; electrical work; furniture, millwork, or physical mounting; customization or programming of third party applications; data entry or data cleanup; end user training; battery backup replacement; the cost of hardware, software, licenses, parts, shipping, or third party

services; repairs to hardware; support for operating systems, applications, or hardware no longer supported by the manufacturer; and remediation of pre-existing issues or deficiencies not identified in the Project Scope. Where Surety is providing hardware or licensing as part of a project, that will be stated in the Quote and is subject to the Procurement policy below.

Client Responsibilities. To allow us to complete projects on schedule, Client agrees to: (i) provide timely physical and remote access to the premises and the Environment; (ii) make an authorized decision maker reasonably available for questions and approvals; (iii) agree to and honor scheduled downtime and maintenance windows; (iv) provide all required software licenses, installation media, and key codes; (v) disclose known issues, deficiencies, and undocumented configurations in the Environment before work begins; (vi) refrain from making changes to the affected portions of the Environment during the project without our knowledge; and (vii) unless Client subscribes to our backup services, maintain current backups of all data and systems affected by the project.

Note: Appointment cancellation and rescheduling of project work is subject to the Appointment Cancellations provisions in the Fees section below. We recommend business-grade computers and equipment from major manufacturers; used, remanufactured, or consumer-grade hardware may limit supportability (see Minimum Requirements / Exclusions below).

Recurring On-Site Technician ADD-ON

If the Quote includes Recurring On-Site Technician services, a Surety technician will visit Client's designated location(s) on a pre-determined, recurring schedule (e.g., weekly or monthly) as indicated in the Quote.

- During scheduled visits, the technician will address open support requests, perform proactive maintenance, and assist end users on site.
- Visit frequency and duration are as indicated in the Quote. Time required beyond the scheduled visit duration is subject to technician availability and will be billed at our then-current hourly rates.
- Scheduled visits may be rescheduled by either party with reasonable advance notice. The Appointment Cancellations provisions in the Fees section below apply to missed or untimely canceled visits.

Remote Helpdesk INCLUDED

- Remote support provided during normal business hours for managed devices and covered software.
- **Prepaid Remote Support Time:** Each covered user accumulates fifteen (15) minutes of prepaid remote support time each month. Prepaid remote support time is pooled among all covered users in Client's organization and may be used by any covered user. Unless otherwise stated in the Quote, unused prepaid remote support time does not roll over to subsequent months and has no cash value.
- Remote support time in excess of the monthly pooled allotment will be billed at our then-current hourly rates, less any eligible discounts.
- Prepaid remote support time applies to remote support only. Onsite visits do not consume prepaid remote support time and are billed at our then-current applicable rates, less any eligible discounts, with a two (2) hour minimum charge per visit (see the Fees section below).
- Tiered-level support provides a smooth escalation process and helps to ensure effective solutions.
- **Remote Employee Onboarding:** Assistance establishing computer and email accounts for new employees, including initial sign-in and access support.
- **Vendor Coordination:** Coordination with Client's line of business software and service vendors to help bridge the gap between those vendors and Client's managed technology.

Remote Monitoring and Management Agent INCLUDED

Software agents installed in Covered Equipment (defined below) report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below.

- Includes capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD partitions, not external devices such as USB or mapped drives).
- Includes routine operating system inspection and cleansing to help ensure that disk space is increased before space-related issues occur.
- Review and installation of updates and patches for supported software.

In addition to the above, our remote monitoring and management service will monitor and alert on the following:

- Hardware Failures
- Device Offline
- Failed/Missing Backup
- Failed/Missing Updates
- Low Disk Space
- Excessive Uptime

Security Information & Event Management (SIEM) ADD-ON

Implementation and facilitation of an industry leading, cloud-delivered SIEM solution from our designated Third Party Provider.

The SIEM service collects and analyzes log data from across the managed environment to detect threats against the managed network.

- **Log Collection.** Collection of log and event data from covered network devices, servers, cloud services, and applications through sensors and platform integrations deployed in the managed environment.
- **Detection.** Prebuilt threat detection rules developed and maintained by the Third Party Provider's security operations team, updated automatically as new threats emerge. Detections cover external attacks as well as potential insider threats occurring inside the monitored network.
- **Alerts & Analysis.** Detections are prioritized by severity and accompanied by guided response playbooks. For urgent, priority findings, the Third Party Provider's security operations team is available for additional analysis and assistance.
- **Retention.** Collected log data will be retained for the period indicated in the Quote or, if no period is indicated, for the platform's standard retention period.

During the initial period following deployment, detection rules are tuned to the Client's environment and user behavior. During this tuning period, Client may experience some "false positives" or, alternatively, not all anomalous activities may be detected.

Note: The SIEM service is a monitoring and alert-based system only; remediation of detected or actual threats is not within the scope of this service and may require Client to retain Surety's services on a time and materials basis.

Server Monitoring & Maintenance ADD-ON

As part of our RMM service, we will monitor and maintain managed servers as follows:

- Software agents installed in covered servers report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below.
- Online status monitoring, alerting us to potential failures or outages.
- Capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD and SSD partitions, not external devices such as USB or mapped network drives).
- Performance monitoring, alerting us to unusual processor or memory usage.
- Server essential service monitoring, alerting us to server role-based service failures.
- Endpoint protection agent monitoring, alerting us to potential security vulnerabilities.
- Routine operating system inspection and cleansing.
- Secure remote connectivity to the server and collaborative screen sharing.
- Review and installation of updates and patches for Windows and supported software.
- Asset inventory and server information collection.

Two Factor Authentication ADD-ON

Implementation and facilitation of a two factor authentication solution from our designated Third Party Provider. Features include:

- App-based authentication on user smartphones, including push-notification approvals and one-time passcodes.
- Protection for cloud applications and supported on-premises applications and logins.
- Access policies based on user, group, location, and/or device state, where supported by the platform and Client's licensing.
- Enrollment support and ongoing administration of the two factor authentication platform.

Software Licensing

(applies to all software licensed by or through Surety)

All software provided to you by or through Surety is licensed, not sold, to you ("Software"). In addition to any Software-related requirements described in Surety's Master Services Agreement, Software may also be subject to end user license agreements (EULAs), acceptable use policies (AUPs), and other restrictions all of which must be strictly followed by you and any of your authorized users.

When installing or implementing Software licenses in the managed Environment or as part of the Services, acceptance and applicability of any EULA, AUP, or other Provider Term will follow the MSA's "Provider Terms; Third-Party Terms Schedule" provision. If a provider requires direct acceptance by Client or an Authorized User, Surety will not accept for Client or activate the affected Software until that required direct acceptance is completed. If a provider expressly permits Surety, its reseller, or a service provider to complete acceptance for the customer, Surety may complete that permitted acceptance step. Otherwise, Client accepts the identified customer- and user-facing obligations in the Provider Terms by accepting the Quote and MSA as stated in the MSA. The applicable provider document, published version or effective date, and acceptance method will be identified in the Third-Party Terms Schedule or applicable Quote. You should assume that all Software has an applicable EULA and/or AUP to which your authorized users and you must adhere. If you have any questions or require a copy of the EULA or AUP, please contact us.

Updates & Patching INCLUDED

- Remotely deploy updates (e.g., x.1 to x.2), as well as bug fixes, minor enhancements, and security updates as deemed necessary on all managed hardware.
- Perform minor hardware and software installations and upgrades of managed hardware.
- Perform minor installations (i.e., tasks that can be performed remotely and typically take less than thirty (30) minutes to complete).
- Deploy, manage, and monitor the installation of approved service packs, security updates and firmware updates as deemed necessary on all applicable managed hardware.

Please note: We will keep all managed hardware and managed software current with critical patches and updates ("Patches") as those Patches are released generally by the applicable manufacturers. Patches are developed by third party vendors and, on rare occasions, may make the Environment, or portions of the Environment, unstable or cause the managed equipment or software to fail to function properly even when the Patches are installed correctly. We will not be responsible for any downtime or losses arising from or related to the installation or use of any Patch. We reserve the right, but not the obligation, to refrain from installing a Patch if we are aware of technical problems caused by a Patch, or we believe that a Patch may render the Environment, or any portion of the Environment, unstable.

IT Consulting SEPARATE QUOTE

Professional IT consulting services provided under a separate quote or engagement. Consulting services may include:

- Technology strategy, roadmaps, and assessments.
- Assistance in the creation of information/data-related plans and budgets.
- Strategic guidance and consultation across different technologies.
- Creation of company-specific best standards and practices.
- Education and recommendations for business technologies.
- Participation in scheduled meetings to maintain goals.
- Maintenance of technology documentation.
- Assessment and recommendations for improving technology usage and services.

Voice Over IP (VoIP) Services Facilitation ADD-ON

We can facilitate Client's enrollment with an industry-recognized VoIP telephone service offered by an independent Third Party Provider. The VoIP service, including call routing, voicemail, caller ID, conference calling, desktop and mobile applications, and related telephone features, is hosted and provided solely by the Third Party Provider under its own agreement with Client.

Our facilitation services may include:

- Assisting with provider selection and initial account setup.
- Deployment and configuration of telephone hardware and applications on the managed network.
- Coordinating with the Third Party Provider on service and support issues.

Please note: Surety does not host, operate, or provide telephone or VoIP services. Service availability, call quality, uptime commitments, and E911 functionality are governed by the Third Party Provider's own terms of service, including any E911 address registration requirements and consent forms required by the Third Party Provider. Client is responsible for reviewing and complying with the Third Party Provider's E911 requirements and for understanding the limitations of 911 dialing over VoIP services.

Vulnerability Management ADD-ON

Implementation and facilitation of an industry-recognized, agent-based vulnerability management solution from our designated Third Party Provider. Features include:

- Continuous monitoring of covered devices for known vulnerabilities in operating systems and supported applications.
- Periodic vulnerability reporting, including severity ratings and remediation recommendations.
- Development of a custom patch deployment plan with Client that aligns remediation activities with Client's business requirements, maintenance windows, and application compatibility considerations.
- Deployment of patches and remediations in accordance with the agreed patch deployment plan.
- For covered servers, confirmation of usability after updates are applied, based on a verification plan outlined by Client.

Please note: Patches and updates are developed by third party vendors and, on rare occasions, may cause instability or failures even when installed correctly (see the Updates & Patching section above). Unless Client subscribes to our backup services (see the Backup and File Recovery section above), Client is solely responsible for maintaining backups, snapshots, or other rollback protection for covered devices prior to patch deployment. Server usability confirmation is limited to the checks identified in Client's verification plan; Client is responsible for defining and maintaining that plan, and we do not warrant or guarantee that all post-update issues will be detected.

Vulnerability Scanning SEPARATE QUOTE

Implementation and facilitation of an industry-recognized vulnerability scanning solution from our designated Third Party Provider.

Vulnerability scanning identifies holes in the managed network that could be exploited. External vulnerability scans (which pertain to the IP address assigned to each customer location through the Client's ISP) are run monthly. Internal vulnerability scans (which pertain to all systems inside the managed network) are run at least annually.

Vulnerability results will be discussed during business review meetings with Client. Vulnerability reports will be made available on request.

Please see additional terms for vulnerability scanning below.

Workstation Monitoring & Maintenance INCLUDED

Software agents installed in covered workstations report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below.

- Online status monitoring, alerting us to potential failures or outages.
- Capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD and SSD partitions, not external devices such as USB or mapped network drives).
- Performance monitoring, alerting us to unusual processor or memory usage.
- Endpoint protection agent monitoring, alerting us to potential security vulnerabilities.
- Routine operating system inspection and cleansing.
- Secure remote connectivity to the workstation and collaborative screen sharing.
- Review and installation of updates and patches for Windows and supported software.
- Asset inventory and workstation information collection.

6. COVERED ENVIRONMENT

Managed Services will be applied to the number of devices indicated in the Quote ("Covered Hardware"). The list of Covered Hardware may be modified by mutual consent (email is sufficient for this purpose); however, we reserve the right to modify the list of Covered Hardware at any time if we discover devices that were not previously included in the list of Covered Hardware and which are receiving Services, or as necessary to accommodate changes to the quantity of Covered Hardware.

Unless otherwise stated in the Quote, Covered Devices will only include technology assets (such as computers, servers, and networking equipment) owned by the Client's organization. As an accommodation, Surety may provide guidance in connecting a personal device to the Client's organization's technology, but support of personal devices is generally not included in the Scope of Services.

If the Quote indicates that the Services are billed on a "per user" basis, then the Services will be provided for one (1) Business Device per licensed user indicated in the Quote. Additional workstations may be covered for an additional per-device fee (see the Extra Workstations section above). A "Business Device" is a workstation, laptop, or tablet that (i) is owned or leased by Client and used primarily for business, (ii) is regularly connected to Client's managed network, and (iii)

has installed on it a software agent through which we (or our designated Third Party Providers) can monitor the device. Servers are not Business Devices and are covered only where a server service is expressly purchased in the Quote.

We will provide support for any software applications that are licensed through us. Such software ("Supported Software") will be supported on a "best effort" basis only and any support required beyond Level 2-type support will be facilitated with the applicable software vendor/producer. Coverage for non-Supported Software is outside of the scope of the Quote and will be provided to you on a "best-effort" basis and a time and materials basis with no guarantee of remediation. Should our technicians provide you with advice concerning non-Supported Software, the provision of that advice should be viewed as an accommodation, not an obligation, to you.

If we are unable to remediate an issue with non-Supported Software, then you will be required to contact the manufacturer/distributor of the software for further support. Please note: Manufacturers/distributors of such software may charge fees, some of which may be significant, for technical support; therefore, we strongly recommend that you maintain service or support contracts for all non-Supported Software ("Service Contract"). If you request that we facilitate technical support for non-Supported Software, then if you have a Service Contract in place, our facilitation services will be provided at no additional cost to you.

In this Services Guide, Covered Hardware and Supported Software will be referred to as the "Environment" or "Covered Equipment."

7. PHYSICAL LOCATIONS COVERED BY SERVICES

Services will be provided remotely unless, in our discretion, we determine that an onsite visit is required. Surety visits will be scheduled in accordance with the priority assigned to the issue (below) and are subject to technician availability. Unless we agree otherwise, all onsite Services will be provided at Client's primary business location. Additional fees may apply for onsite visits: Please review the Service Level section below for more details.

8. MINIMUM REQUIREMENTS / EXCLUSIONS

The scheduling, fees and provision of the Services are based upon the following assumptions and minimum requirements, all of which must be provided/maintained by Client at all times:

- Server hardware must be under current warranty coverage.
- All equipment with Microsoft Windows® operating systems must be running then-currently supported versions of such software and have all the latest Microsoft service packs and critical updates installed.
- All software must be genuine, licensed, and vendor- or OEM-supported.
- Server file systems and email systems (if applicable) must be protected by licensed and up-to-date virus protection software.
- The managed environment must have a currently licensed, vendor-supported server-based backup solution that can be monitored.
- All wireless data traffic in the managed environment must be securely encrypted.
- All servers must be connected to working UPS devices.

- Recovery coverage assumes data integrity of the backups or the data stored on the backup devices. We do not guarantee the integrity of the backups or the data stored on the backup devices. Server restoration will be to the point of the last successful backup.
- Client must provide all software installation media and key codes in the event of a failure.
- Any costs required to bring the Environment up to these minimum standards are not included in this Services Guide.
- Client must provide Surety with the administrative privileges reasonably necessary to provide the Services. No third party may have overlapping administrative access to a portion of the Environment managed by Surety unless that party is identified as a Co-Managed Provider in the applicable Quote or Surety otherwise permits the access in writing.
- Client must not affix or install any accessory, addition, upgrade, equipment, or device on to the firewall, server, or NAS appliances (other than electronic data) unless expressly approved in writing by us.

Exclusions. Services that are not expressly described in the Quote will be out of scope and will not be provided to Client unless otherwise agreed, in writing, by Surety. Without limiting the foregoing, the following services are expressly excluded, and if required to be performed, must be agreed upon by Surety in writing:

- Customization of third party applications, or programming of any kind.
- Support for operating systems, applications, or hardware no longer supported by the manufacturer.
- Data/voice wiring or cabling services of any kind.
- Battery backup replacement.
- Equipment relocation.
- The cost to bring the managed environment up to these minimum requirements (unless otherwise noted in the Quote).
- The cost of repairs to hardware or any supported equipment or software, or the costs to acquire parts or equipment, or shipping charges of any kind.

9. SERVICE LEVELS

Automated monitoring is provided on an ongoing (i.e., 24x7x365) basis. Response, repair, and/or remediation services (as applicable) will be provided only during our business hours (currently Monday through Friday, 8:00 AM to 5:00 PM Central, excluding legal holidays and Surety-observed holidays as listed below), unless otherwise specifically stated in the Quote or as otherwise described below.

We will endeavor to respond to problems, errors, or interruptions in the provision of the Services during business hours within the target timeframes described below (each, a “Response Time Objective”). Response Time Objectives are performance targets that we strive to meet or exceed; they are objectives only and are not guarantees of response or resolution within any specific time period. Severity levels will be determined by Surety in our discretion after consulting with the Client. All remediation services will initially be attempted remotely; Surety will provide onsite service only if remote remediation is ineffective and, under all circumstances, only if covered under the Service plan selected by Client.

TROUBLE / SEVERITY	RESPONSE TIME OBJECTIVE*
Critical / Service Not Available (e.g., all users and functions unavailable)	Target response within fifteen (15) minutes after notification.
Significant Degradation (e.g., large number of users or business critical functions affected)	Target response within one (1) hour after notification.
Standard (e.g., limited number of users or functions affected, business process can continue)	Target response within two (2) hours after notification.
Long Term Project, Preventative Maintenance	Target response within two (2) business days after notification.

* All Response Time Objectives are measured from the time that we are notified of the applicable issue / problem by Client through our designated support channels (email or telephone as listed in the Quote). Notifications received in any manner other than described herein may result in a delay in the provision of remediation efforts.

Priority Response: As a managed services client, Client's support requests are prioritized ahead of support requests from customers who do not receive ongoing managed services from Surety. For prioritization ahead of other managed services clients' standard requests, please see the Front of Line Response section above.

Support During Off-Hours/Non-Business Hours: Technical support provided outside of our normal business hours is offered on a case-by-case basis and is subject to technician availability. If Surety agrees to provide off-hours/non-business hours support ("Non-Business Hour Support"), then that support will be provided on a time and materials basis (which is not covered under any Service plan), and will be billed to Client at the following increased hourly rates:

- Project Professional: 1.5x normal rate
- Support Technician: 1.5x normal rate

All hourly services are billed in 15 minute increments, and partial increments are rounded to the next highest increment. A one (1) hour minimum applies to all Non-Business Hour Support, and a two (2) hour minimum applies to all onsite visits, whether during or outside of normal business hours.

Surety-Observed Holidays: Surety observes the following holidays:

- New Year's Day
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving Day
- The day following Thanksgiving Day

- Christmas Eve
- Christmas Day
- New Year's Eve

Service Credits: Service credits are not provided under our standard Service plans, and the Response Time Objectives described above do not entitle Client to any credit, refund, or fee reduction. If a Quote expressly includes a service credit commitment, then (i) credits will be calculated and applied as set forth in that Quote, (ii) the receipt of those service credits will be Client's sole and exclusive remedy for any failure to meet the applicable service level commitment, and (iii) credits will not exceed the percentage of monthly recurring fees stated in the Quote.

10. FEES

The fees for the Services will be as indicated in the Quote.

Reconciliation. Fees for certain Third Party Services that we facilitate or resell to you may begin to accrue prior to the "go-live" date of other applicable Services. (For example, Microsoft Azure or AWS-related fees begin to accrue on the first date on which we start creating and/or configuring certain hosted portions of the Environment; however, the Services that rely on Microsoft Azure or AWS may not be available to you until a future date). You understand and agree that you will be responsible for the payment of all fees for Third Party Services that are required to begin prior to the "go-live" date of Services, and we reserve the right to reconcile amounts owed for those fees by including those fees on your monthly invoices.

Changes to Environment. The fees stated in the Quote are based on the Covered Environment stated in the Quote. If the number of users, devices, or other covered items changes, the fees will be adjusted prospectively to reflect the change, effective on the first invoice issued after the change is identified, using the per-unit rates stated in the Quote. Surety will identify the adjustment on the applicable invoice. Additions made at Client's request, and additions Surety identifies through its monitoring tools, may be invoiced without a separate signed amendment. Any other change to the Covered Environment requires the mutual consent of the parties, and email is sufficient for this purpose. An adjustment under this paragraph reflects a change in quantity at previously agreed per-unit rates and is not an increase in fees for purposes of the "Increases" provision of the MSA. Reductions in quantity remain subject to the "Minimum Monthly Fees" provision of the MSA.

No Unbundling. The Bundle is offered and sold as a single, integrated service package. Client may not require Surety to remove, substitute, or separately purchase individual components of the Bundle. If Client wishes to discontinue a specific component, the only option is termination of the applicable Services in accordance with the Agreement, and Client will remain obligated for all fees through the end of the then-current term, including fees for any non-cancelable Access Licenses procured on Client's behalf. Surety may itemize or separately state the price of components of the Bundle on invoices, rate cards, or price lists for invoicing, tax, or administrative purposes, and no such itemization entitles Client to purchase components separately, to discontinue components, or to any price adjustment.

Managed Client Labor Discount. Clients receiving ongoing managed services under a Quote receive a ten percent (10%) discount off our standard hourly rates for onsite labor and project labor billed on a time and materials basis. The discount applies for as long as the applicable

managed services Quote remains in effect, and does not apply to hard costs, licenses, travel-related expenses, or Third Party Services.

Travel Time. If onsite services are provided, we will travel up to 30 minutes from our office to your location at no charge. Time spent traveling beyond 30 minutes (e.g., locations that are beyond 30 minutes from our office, occasions on which traffic conditions extend our drive time, etc.) will be billed to you at our then current hourly rates. In addition, you will be billed for all tolls, parking fees, and related expenses that we incur if we provide onsite services to you.

Appointment Cancellations. You may cancel or reschedule any appointment with us at no charge by providing us with notice of cancellation at least one business day in advance. If we do not receive timely a notice of cancellation/re-scheduling, or if you are not present at the scheduled time or if we are otherwise denied access to your premises at a pre-scheduled appointment time, then you agree to pay us a cancellation fee equal to two (2) hours of our normal consulting time (or non-business hours consulting time, whichever is appropriate), calculated at our then-current hourly rates.

Access Licensing. One or more of the Services may require us to purchase certain "per seat" or "per device" licenses (often called "Access Licenses") from one or more Third Party Providers. (Microsoft "New Commerce Experience" licenses as well as Cisco Meraki "per device" licenses are examples of Access Licenses.) Access Licenses cannot be canceled once they are purchased and often cannot be transferred to any other customer. For that reason, you understand and agree that regardless of the reason for termination of the Services, fees for Access Licenses are non-mitigatable and you are required to pay for all applicable Access Licenses in full for the entire term of those licenses. Provided that you have paid for the Access Licenses in full, you will be permitted to use those licenses until they expire.

11. CHANGE ORDERS

Any material change to the scope of the Services described in a Quote must be documented in a written change order accepted by both parties (email or electronic acceptance is sufficient for this purpose). Surety has no obligation to perform services that fall outside the scope of the Quote unless and until a change order is accepted. Unless otherwise stated in the change order, pricing for change order work will be determined by Surety based on our then-current rates, and change order work may affect project timelines and delivery dates.

12. TERM; TERMINATION

The Services will commence, and billing will begin, on the date indicated in the Quote ("Commencement Date"). If the Quote states "Month-to-month" or does not state a number of committed months, no minimum term applies and either party may terminate the Services on thirty (30) days prior written notice under the MSA. If the Quote states a number of committed months, that period is the "Minimum Term" for purposes of the MSA. Unless the Quote states otherwise, each renewal is equal in length to the initial Minimum Term and is itself a Minimum Term for all purposes of the MSA.

We reserve the right to delay the Commencement Date until all onboarding or transition services (if any) are completed and all deficiencies or revisions identified during onboarding (if any) are addressed or remediated to Surety's reasonable satisfaction.

Per Seat/Per Device Licensing: Regardless of the reason for the termination of the Services, you will be required to pay for all per seat or per device licenses that we acquire on your behalf. Please see "Access Licensing" in the Fees section above for more details.

Removal of Software Agents; Return of Surety-Provided Equipment: Unless we expressly direct you to do so, you will not remove or disable, or attempt to remove or disable, any software agents that we installed in the managed environment or any of the devices on which we installed software agents. Doing so without our guidance may make it difficult or impracticable to remove the software agents, which could result in network vulnerabilities and/or the continuation of license fees for the software agents for which you will be responsible, and/or the requirement that we remediate the situation at our then-current hourly rates, for which you will also be responsible. Depending on the particular software agent and the costs of removal, we may elect to keep the software agent in the managed environment but in a dormant and/or unused state.

Within ten (10) days after being directed to do so, you must remove, package and ship, at your expense and in a commercially reasonable manner, all hardware, equipment, and accessories leased, loaned, rented, or otherwise provided to you by Surety "as a service." If you fail to timely return all such equipment to us, or if the equipment is returned to us damaged (normal wear and tear excepted), then we will have the right to charge you, and you hereby agree to pay, the replacement value of all such unreturned or damaged equipment.

13. OFFBOARDING

Subject to the requirements in the MSA, Surety will off-board Client from Surety's services by performing one or more of the following:

- Removal / disabling of monitoring and remote management agents from the Environment.
- Removal / disabling of endpoint security software from the Environment, including antivirus/ EDR, DNS protection, and privilege management agents.
- Removal / disabling of backup software from the Environment. Post-termination availability, export, and deletion of backup data are governed by the "Backup Data" provision of the MSA. Client should request any desired export before the Backup Availability Period expires.
- Completion of any Access Licensing terms already in place under the MSA for Microsoft 365 licenses provided through Surety or, where applicable, transfer of those licenses to an eligible incoming provider, together with removal of Surety's administrative access to Client's Microsoft 365 tenant.
- Termination of any other Access Licensing being provided by or through Surety, subject to the Access Licensing provisions in the Fees section above and the MSA.
- Removal of Surety's administrative access to the Environment, including network management platforms and cloud consoles.
- Provision of administrative credentials and reasonable environment documentation to Client or Client's designated incoming provider.
- Return of Surety-provided equipment, as governed by the Term; Termination section above.

Additional offboarding or transition assistance requested by Client (such as knowledge transfer with an incoming provider) will be provided on a time and materials basis at our then-current rates.

14. ADDITIONAL POLICIES

The following additional policies ("Policies") apply to Services that we provide or facilitate under a Quote. By accepting a Service for which one or more of the Policies apply, you agree to always abide by the applicable Policy.

AUTHENTICITY

Everything in the managed environment must be genuine and licensed, including all hardware, software, etc. If we ask for proof of authenticity and/or licensing, you must provide us with such proof. All minimum hardware or software requirements as indicated in a Quote or this Services Guide ("Minimum Requirements") must be implemented and maintained as an ongoing requirement of us providing the Services to you.

MONITORING SERVICES; ALERT SERVICES

Unless otherwise indicated in the Quote, all monitoring and alert-type services are limited to detection and notification functionalities only. Monitoring levels will be set by Surety, and Client shall not modify these levels without our prior written consent.

CONFIGURATION OF THIRD PARTY SERVICES

Certain third party services provided to you under an Order may provide you with administrative access through which you could modify the configurations, features, and/or functions ("Configurations") of those services. However, any modifications of Configurations made by you without authorization could disrupt the Services and/or cause a significant increase in the fees charged for those third party services. For that reason, we strongly advise you to refrain from changing the Configurations unless we authorize those changes. You will be responsible for paying any increased fees or costs arising from or related to changes to the Configurations.

MODIFICATION OF ENVIRONMENT

Changes made to the Environment without our prior authorization or knowledge may have a substantial, negative impact on the provision and effectiveness of the Services and may impact the fees charged under the Quote. You agree to refrain from moving, modifying, or otherwise altering any portion of the Environment without our prior knowledge or consent. For example, you agree to refrain from adding or removing hardware from the Environment, installing applications on the Environment, or modifying the configuration or log files of the Environment without our prior knowledge or consent.

ANTI-VIRUS; ANTI-MALWARE

Our anti-virus / anti-malware solution will generally protect the Environment from becoming infected with new viruses and malware ("Malware"); however, Malware that exists in the Environment at the time that the security solution is implemented may not be capable of being removed without additional services, for which a charge may be incurred. We do not warrant or guarantee that all Malware will be detected, avoided, or removed, or that any data erased, corrupted, or encrypted by Malware will be recoverable. The applicable anti-virus, anti-malware, and endpoint-security products may collect and transmit to Surety and/or the applicable Third Party Provider security and endpoint data, including file and process information, executed scripts and commands, login and device data, URLs, network data, security events, threat indicators, and suspicious or unknown files submitted or retrieved for analysis. Depending on Client's systems, configurations, and content, that information may include personal information or Client's

Confidential Information. The collection, use, transfer, retention, and deletion of that information will be governed by this Agreement, applicable law, and the applicable Provider Terms. Client authorizes those activities for the purposes described in the Provider Terms, including providing, supporting, securing, and improving the applicable security services. The applicable documents and acceptance methods are identified in the Third-Party Terms Schedule below and may be requested as described in the Provider Terms provision of the MSA.

BREACH/CYBER SECURITY INCIDENT RECOVERY

Unless otherwise expressly stated in the Quote, the scope of the Services does not include the remediation and/or recovery from a Security Incident (defined below). Such services, if requested by you, will be provided on a time and materials basis under our then-current hourly labor rates. Given the varied number of possible Security Incidents, we cannot and do not warrant or guarantee (i) the amount of time required to remediate the effects of a Security Incident (or that recovery will be possible under all circumstances), or (ii) that all data or systems impacted by the incident will be recoverable or remediated. For the purposes of this paragraph, a Security Incident means any unauthorized or impermissible access to or use of the Environment, or any unauthorized or impermissible disclosure of Client's confidential information (such as user names, passwords, etc.), that (i) compromises the security or privacy of the information or applications in, or the structure or integrity of, the managed environment, or (ii) prevents normal access to the managed environment, or impedes or disrupts the normal functions of the managed environment.

ENVIRONMENTAL FACTORS

Exposure to environmental factors, such as water, heat, cold, or varying lighting conditions, may cause installed equipment to malfunction. Unless expressly stated in the Quote, we do not warrant or guarantee that installed equipment will operate error-free or in an uninterrupted manner, or that any video or audio equipment will clearly capture and/or record the details of events occurring at or near such equipment under all circumstances.

FAIR USAGE POLICY

Our Fair Usage Policy ("FUP") applies to all services that are described or designated as "unlimited" or which are not expressly capped in the number of available usage hours per month. An "unlimited" service designation means that, subject to the terms of this FUP, you may use the applicable service as reasonably necessary for you to enjoy the use and benefit of the service without incurring additional time-based or usage-based costs. However, unless expressly stated otherwise in the Quote, all unlimited services are provided during our normal business hours only and are subject to our technicians' availabilities, which cannot always be guaranteed. In addition, we reserve the right to assign our technicians as we deem necessary to handle issues that are more urgent, critical, or pressing than the request(s) or issue(s) reported by you. Consistent with this FUP, you agree to refrain from (i) creating urgent support tickets for non-urgent or non-critical issues, (ii) requesting excessive support services that are inconsistent with normal usage patterns in the industry (e.g., requesting support in lieu of training), (iii) requesting support or services that are intended to interfere, or may likely interfere, with our ability to provide our services to our other customers.

HOSTED EMAIL

You are solely responsible for the proper use of any hosted email service provided to you ("Hosted Email").

Hosted Email solutions are subject to acceptable use policies ("AUPs"), and your use of Hosted Email must comply with those AUPs, including ours. In all cases, you agree to refrain from uploading, posting, transmitting or distributing (or permitting any of your authorized users of the Hosted Email to upload, post, transmit or distribute) any prohibited content, which is generally content that (i) is obscene, illegal, or intended to advocate or induce the violation of any law, rule or regulation, or (ii) violates the intellectual property rights or privacy rights of any third party, or (iii) mischaracterizes you, and/or is intended to create a false identity or to otherwise attempt to mislead any person as to the identity or origin of any communication, or (iv) interferes or disrupts the services provided by Surety or the services of any third party, or (v) contains Viruses, trojan horses or any other malicious code or programs. In addition, you must not use the Hosted Email for the purpose of sending unsolicited commercial electronic messages ("SPAM") in violation of any federal or state law. Surety reserves the right, but not the obligation, to suspend Client's access to the Hosted Email and/or all transactions occurring under Client's Hosted Email account(s) if Surety believes, in its discretion, that Client's email account(s) is/are being used in an improper or illegal manner.

BACKUP (BDR) SERVICES

All data transmitted over the Internet may be subject to malware and computer contaminants such as viruses, worms and trojan horses, as well as attempts by unauthorized users, such as hackers, to access or damage Client's data. Neither Surety nor its designated affiliates will be responsible for the outcome or results of such activities.

BDR services require a reliable, always-connected internet solution. Data backup and recovery time will depend on the speed and reliability of your internet connection. Internet and telecommunications outages will prevent the BDR services from operating correctly. In addition, all computer hardware is prone to failure due to equipment malfunction, telecommunication-related issues, etc., for which we will be held harmless. Due to technology limitations, all computer hardware, including communications equipment, network servers and related equipment, has an error transaction rate that can be minimized, but not eliminated. Surety cannot and does not warrant that data corruption or loss will be avoided, and Client agrees that Surety shall be held harmless if such data corruption or loss occurs. Client is strongly advised to keep a local backup of all stored data to mitigate against the unintentional loss of data.

PROCUREMENT

Equipment and software procured by Surety on Client's behalf ("Procured Equipment") may be covered by one or more manufacturer warranties, which will be passed through to Client to the greatest extent possible. By procuring equipment or software for Client, Surety does not make any warranties or representations regarding the quality, integrity, or usefulness of the Procured Equipment. Certain equipment or software, once purchased, may not be returnable or, in certain cases, may be subject to third party return policies and/or re-stocking fees, all of which shall be Client's responsibility in the event that a return of the Procured Equipment is requested. Surety is not a warranty service or repair center. Surety will facilitate the return or warranty repair of Procured Equipment; however, Client understands and agrees that (i) the return or warranty repair of Procured Equipment is governed by the terms of the warranties (if any) governing the applicable Procured Equipment, for which Surety will be held harmless, and (ii) Surety is not responsible for the quantity, condition, or timely delivery of the Procured Equipment once the equipment has been tendered to the designated shipping or delivery courier.

BUSINESS REVIEW / IT STRATEGIC PLANNING MEETINGS

We strongly suggest that you participate in business review/strategic planning meetings as may be requested by us from time to time. These meetings are intended to educate you about recommended (and potentially crucial) modifications to your IT environment, as well as to discuss your company's present and future IT-related needs. These reviews can provide you with important insights and strategies to make your managed IT environment more efficient and secure. You understand that by suggesting a particular service or solution, we are not endorsing any specific manufacturer or service provider.

IT CONSULTING / ADVISORY SERVICES

The advice and suggestions provided by us in connection with our IT consulting or advisory services will be for your informational and/or educational purposes only. Surety will not hold an actual director or officer position in Client's company, and we will neither hold nor maintain any fiduciary relationship with Client. Under no circumstances shall Client list or place Surety on Client's corporate records or accounts.

SAMPLE POLICIES, PROCEDURES

From time to time, we may provide you with sample (i.e., template) policies and procedures for use in connection with Client's business ("Sample Policies"). The Sample Policies are for your informational use only, and do not constitute or comprise legal or professional advice, and the policies are not intended to be a substitute for the advice of competent counsel. You should seek the advice of competent legal counsel prior to using or distributing the Sample Policies, in part or in whole, in any transaction. We do not warrant or guarantee that the Sample Policies are complete, accurate, or suitable for your (or your customers') specific needs, or that you will reduce or avoid liability by utilizing the Sample Policies in your (or your customers') business operations.

PENETRATION TESTING; VULNERABILITY SCANNING

You understand and agree that security devices, alarms, or other security measures, both physical and virtual, may be tripped or activated during the penetration testing and/or vulnerability scanning processes, despite our efforts to avoid such occurrences. You will be solely responsible for notifying any monitoring company and all law enforcement authorities of the potential for "false alarms" due to the provision of the penetration testing or vulnerability scanning services, and you agree to take all steps necessary to ensure that false alarms are not reported or treated as "real alarms" or credible threats against any person, place, or property. Some alarms and advanced security measures, when activated, may cause the partial or complete shutdown of the Environment, causing substantial downtime and/or delay to your business activities. We will not be responsible for any claims, costs, fees, or expenses arising or resulting from (i) any response to the penetration testing or vulnerability scanning services by any monitoring company or law enforcement authorities, or (ii) the partial or complete shutdown of the Environment by any alarm or security monitoring device.

NO THIRD PARTY SCANNING

Unless we authorize such activity in writing, you will not conduct any test, nor request or allow any third party to conduct any test (diagnostic or otherwise), of the security system, protocols, processes, or solutions that we implement in the managed environment ("Testing Activity"). Any services required to diagnose or remediate errors, issues, or problems arising from unauthorized Testing Activity are not covered under the Quote, and if you request us (and we elect) to perform

those services, those services will be billed to you at our then-current hourly rates. Note: We are unable to perform penetration testing, scanning, or any other form of Testing Activity on upstream providers such as Microsoft without their written, express authorization.

OBSOLESCENCE

If at any time any portion of the managed environment becomes outdated, obsolete, reaches the end of its useful life, or acquires “end of support” status from the applicable device’s or software’s manufacturer (“Obsolete Element”), then we may designate the device or software as “unsupported” or “non-standard” and require you to update the Obsolete Element within a reasonable time period. If you do not replace the Obsolete Element reasonably promptly, then in our discretion we may (i) continue to provide the Services to the Obsolete Element using our “best efforts” only with no warranty or requirement of remediation whatsoever regarding the operability or functionality of the Obsolete Element, or (ii) eliminate the Obsolete Element from the scope of the Services by providing written notice to you (email is sufficient for this purpose). In any event, we make no representation or warranty whatsoever regarding any Obsolete Element or the deployment, service level guarantees, or remediation activities for any Obsolete Element.

LICENSES

If we are required to re-install or replicate any software provided by you as part of the Services, then it is your responsibility to verify that all such software is properly licensed. We reserve the right, but not the obligation, to require proof of licensing before installing, re-installing, or replicating software into the managed environment. The cost of acquiring licenses is not included in the scope of the Quote unless otherwise expressly stated therein.

15. ACCEPTABLE USE POLICY

The following policy applies to all hosted services provided to you, including but not limited to (and as applicable) hosted applications, hosted websites, hosted email services, and hosted infrastructure services (“Hosted Services”).

Surety does not routinely monitor the activity of hosted accounts except to measure service utilization and/or service uptime, security-related purposes and billing-related purposes, and as necessary for us to provide or facilitate our managed services to you; however, we reserve the right to monitor Hosted Services at any time to ensure your compliance with the terms of this Acceptable Use Policy (this “AUP”) and our master services agreement, and to help monitor and ensure the safety, integrity, reliability, or security of the Hosted Services.

Similarly, we do not exercise editorial control over the content of any information or data created on or accessible over or through the Hosted Services. Instead, we prefer to advise our customers of inappropriate behavior and any necessary corrective action. If, however, Hosted Services are used in violation of this AUP, then we reserve the right to suspend your access to part or all of the Hosted Services without prior notice.

Violations of this AUP: The following constitute violations of this AUP:

- **Harmful or illegal uses:** Use of a Hosted Service for illegal purposes or in support of illegal activities, to cause harm to minors or attempt to contact minors for illicit purposes, to transmit any material that threatens or encourages bodily harm or destruction of property or to transmit any material that harasses another is prohibited.

- **Fraudulent activity:** Use of a Hosted Service to conduct any fraudulent activity or to engage in any unfair or deceptive practices, including but not limited to fraudulent offers to sell or buy products, items, or services, or to advance any type of financial scam such as “pyramid schemes,” “Ponzi schemes,” and “chain letters” is prohibited.
- **Forgery or impersonation:** Adding, removing, or modifying identifying network header information to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or other identifying information is prohibited. The use of anonymous remailers or nicknames does not constitute impersonation.
- **SPAM:** Surety has a zero tolerance policy for the sending of unsolicited commercial email (“SPAM”). Use of a Hosted Service to transmit any unsolicited commercial or unsolicited bulk e-mail is prohibited. You are not permitted to host, or permit the hosting of, sites or information that is advertised by SPAM from other networks. To prevent unnecessary blacklisting due to SPAM, we reserve the right to drop the section of IP space identified by SPAM or denial-of-service complaints if it is clear that the offending activity is causing harm to parties on the Internet, if open relays are on the hosted network, or if denial of service attacks are originated from the hosted network.
- **Internet Relay Chat (IRC):** The use of IRC on a hosted server is prohibited.
- **Open or “anonymous” proxy:** Use of open or anonymous proxy servers is prohibited.
- **Cryptomining:** Using any portion of the Hosted Services for mining cryptocurrency or using any bandwidth or processing power made available by or through a Hosted Services for mining cryptocurrency, is prohibited.
- **Hosting spammers:** The hosting of websites or services using a hosted server that supports spammers, or which causes (or is likely to cause) our IP space or any IP space allocated to us or our customers to be listed in any of the various SPAM databases, is prohibited. Customers violating this policy will have their server immediately removed from our network and the server will not be reconnected until such time that the customer agrees to remove all traces of the offending material immediately upon reconnection and agrees to allow Surety to access the server to confirm that all material has been completely removed. Any subscriber guilty of a second violation may be immediately and permanently removed from the hosted network for cause and without prior notice.
- **Email/message forging:** Forging any email message header, in part or whole, is prohibited.
- **Unauthorized access:** Use of the Hosted Services to access, or to attempt to access, the accounts of others or to penetrate, or attempt to penetrate, Surety’s security measures or the security measures of another entity's network or electronic communications system, whether or not the intrusion results in the corruption or loss of data, is prohibited. This includes but is not limited to accessing data not intended for you, logging into or making use of a server or account you are not expressly authorized to access, or probing the security of other networks, as well as the use or distribution of tools designed for compromising security such as password guessing programs, cracking tools, or network probing tools.
- **IP infringement:** Use of a Hosted Service to transmit any materials that infringe any copyright, trademark, patent, trade secret or other proprietary rights of any third party, is prohibited.
- **Collection of personal data:** Use of a Hosted Service to collect, or attempt to collect, personal information about third parties without their knowledge or consent is prohibited.

- **Network disruptions and sundry activity:** Use of the Hosted Services for any activity which affects the ability of other people or systems to use the Hosted Services or the internet is prohibited. This includes “denial of service” (DOS) attacks against another network host or individual, “flooding” of networks, deliberate attempts to overload a service, and attempts to “crash” a host.
- **Distribution of malware:** Intentional distribution of software or code that attempts to and/or causes damage, harassment, or annoyance to persons, data, and/or computer systems is prohibited.
- **Excessive use or abuse of shared resources:** The Hosted Services depend on shared resources. Excessive use or abuse of these shared network resources by one customer may have a negative impact on all other customers. Misuse of network resources in a manner which impairs network performance is prohibited. You are prohibited from excessive consumption of resources, including CPU time, memory, and session time. You may not use resource-intensive programs which negatively impact other customers or the performances of our systems or networks.
- **Allowing the misuse of your account:** You are responsible for any misuse of your account, even if the inappropriate activity was committed by an employee or independent contractor. You shall not permit your hosted network, through action or inaction, to be configured in such a way that gives a third party the capability to use your hosted network in an illegal or inappropriate manner. You must take adequate security measures to prevent or minimize unauthorized use of your account. It is your responsibility to keep your account credentials secure.

To maintain the security and integrity of the hosted environment, we reserve the right, but not the obligation, to filter content, requests, or website access for any web requests made from within the hosted environment.

Revisions to this AUP: We reserve the right to revise or modify this AUP from time to time. Revisions to this AUP are subject to the notice and objection provisions of the “Changes to Services Guide” provision of the MSA.

16. THIRD-PARTY TERMS SCHEDULE

This schedule is part of this Services Guide and is incorporated into the MSA. A listed document applies only when the affected Services Guide service is included in an accepted Quote, whether as an expressly named Quote line item, as an Included component of a purchased bundle, or through another quoted bundle or add-on that this Guide expressly states includes that service. Client's acceptance of a Quote constitutes acceptance of the listed terms when the stated acceptance method is "accepted through Quote." If the provider requires separate direct, click-through, registration, installation, access, or use acceptance, Client must also complete that step.

Only customer, beneficiary, end-user, user, and data-related obligations that apply to Client or Client's use of the affected Third Party Service are incorporated. Terms governing solely the relationship between Surety and a provider are excluded. The listed provider terms govern Client's rights and obligations concerning the provider and the Third Party Service; they do not change the price, scope, payment terms, or other obligations between Client and Surety, or expand Surety's obligations, except where the MSA or Quote expressly says otherwise.

Any customer-specific, product-specific, order-specific, or successor terms required by a provider will be delivered or identified with the applicable Quote before acceptance and retained with the accepted contract record. A separately executed data processing addendum or business associate agreement is not incorporated unless it is listed below, identified in the Quote, or supplied with the Quote. For a document without a published version date, "current online version" means the version available at the linked official source when the Quote is accepted. Surety will retain a static copy of each applicable version as evidence of the terms disclosed at acceptance. Later provider changes are handled under the Provider Terms provision of the MSA.

Axcient

Services Guide services: Backup and File Recovery (x360Recover); Backup & Recovery Planning (x360Recover).

- Master Terms of Service and the policies it expressly incorporates, collected on the Axcient Legal Host `CUSTOMER TERMS`
- Axcient Data Privacy Addendum for Customers `VENDOR DATA TERMS`

Version: Master Terms of Service, January 6, 2020; Data Privacy Addendum, 2018; incorporated policies as identified on the Legal Host for the applicable product and order.

Acceptance: Accepted through Quote. Registration, login, or use also constitutes acceptance where stated in Axcient's terms. Surety retains the accepted Quote and the applicable archived versions.

Microsoft (including Azure)

Services Guide services: Cloud Server & Cloud Desktop Hosting; Mobile Device Management (MDM) using Microsoft Intune; Voice Over IP (VoIP) Services Facilitation.

- Microsoft Customer Agreement `CUSTOMER AGREEMENT`
- Microsoft Product Terms `LICENSE TERMS`
- Microsoft Products and Services Data Protection Addendum `VENDOR DATA TERMS`

Version: Microsoft Customer Agreement, March 1, 2023; Product Terms publication in effect for the applicable order; Data Protection Addendum, May 22, 2026.

Acceptance: Client completes the Microsoft-required acceptance through Microsoft's digital workflow or another Microsoft-permitted acceptance method. Surety verifies and retains the available Microsoft acceptance record before placing the applicable order.

DefensX

Services Guide service: DNS Threat Protection.

- Terms & Conditions `PUBLISHED TERMS`

Version: June 10, 2020.

Acceptance: Accepted through Quote and by access or use to the extent stated in the published terms. DefensX's public page does not identify a separate DNS-product license; any additional product-specific customer terms supplied by DefensX will be delivered with and identified in the applicable Quote before acceptance.

Check Point Software Technologies

Services Guide services: Email Archiving; Email Threat Protection; End User Security Awareness Training (Check Point Harmony Email & Collaboration).

- Terms of Service – Cloud Services; Infinity Portal / Cloud End-user License Agreement `CUSTOMER TERMS`
- Customers Data Protection Addendum `VENDOR DATA TERMS`

Version: Cloud terms v.1.20; Data Protection Addendum current online version accessed August 3, 2026.

Acceptance: Accepted through Quote. Surety retains evidence of Client's consent, as Check Point requires for managed-service customers. Click-through or use acceptance also applies if presented by the provider.

CrowdStrike

Services Guide services: Endpoint Antivirus & Malware Protection (MSSP Advanced Defend); Vulnerability Management; Vulnerability Scanning.

- CrowdStrike Terms and Conditions, including the Data Security and Privacy Schedule `BENEFICIARY TERMS`
- CrowdStrike Global Data Protection Agreement, if and to the extent its stated applicability conditions are met `VENDOR DATA TERMS`
- CrowdStrike Open-Source Notices `REQUIRED NOTICE`

Version: Current online versions accessed August 1, 2026, plus any customer-specific terms identified on the applicable CrowdStrike quote.

Acceptance: The accepted Quote, MSA, and this schedule constitute the beneficiary agreement for the affected CrowdStrike service. Surety retains the acceptance record and the archived terms. Any customer-specific CrowdStrike quote terms will be supplied and identified before Quote acceptance.

Blumira

Services Guide services: Microsoft 365 Management & Security (Identity Threat Detection & Response); Extended Detection & Response (XDR); Security Information & Event Management (SIEM).

- Pass-Through Terms and Conditions and the linked Blumira Terms of Use `PASS-THROUGH TERMS`

Version: Blumira Terms of Use dated April 5, 2022.

Acceptance: Accepted through Quote. Client or an authorized user must also affirmatively consent before first use if Blumira presents a separate acceptance step.

Abyde

Services Guide service: HIPAA Compliance Program Facilitation.

- Terms and Conditions `DIRECT CUSTOMER TERMS`

Version: Current online version accessed August 1, 2026.

Acceptance: Client contracts directly with Abyde and completes Abyde's subscription, online-signup, and terms-acceptance process. Surety does not activate or facilitate the affected service until Client supplies confirmation of direct acceptance.

NetBird

Services Guide service: Managed VPN.

- NetBird Terms of Service, including the NetBird data processing agreement referenced in Section 13 when applicable `CUSTOMER & DATA TERMS`

Version: Current online version accessed August 1, 2026; provider-supplied data processing agreement version applicable to the account.

Acceptance: Accepted through Quote. Client or its authorized user must also complete registration or click-through acceptance if presented by NetBird; Surety retains available evidence of that acceptance.

OpenText (CloudAlly)

Services Guide service: Microsoft 365 Backup.

- OpenText Cybersecurity Cloud Terms and Conditions `CUSTOMER TERMS`
- Service Specific Terms Addendum, Section 7, OpenText Core Cloud-to-Cloud Backup / CloudAlly SaaS Data Protection Platform `PRODUCT TERMS`
- OpenText Data Processing Addendum, when its stated applicability conditions are met `VENDOR DATA TERMS`

Version: Cloud Terms current online version accessed August 1, 2026; Service Specific Terms Addendum last updated April 23, 2026; Data Processing Addendum version incorporated by the Cloud Terms for the applicable processing.

Acceptance: Accepted through Quote and, where applicable, by order, access, or use. The accepted Quote identifies Client as the beneficiary of the affected service, and Surety retains the applicable archived versions.

Ubiquiti

Services Guide service: Network as a Service (NaaS).

- Ubiquiti Terms of Service `CUSTOMER TERMS`
- Ubiquiti Services General Terms and Conditions `SERVICE TERMS`

Version: Terms of Service updated May 31, 2024; Services General Terms last modified August 9, 2021.

Acceptance: Accepted through Quote and by Client’s or its authorized users’ registration, access, or use where stated in Ubiquiti’s terms.

Auvik

Services Guide service: Network Operations Center (NOC).

- Auvik Subscription Services Agreement CUSTOMER TERMS
- Auvik Service Specific Terms, to the extent applicable to the purchased features PRODUCT TERMS
- Auvik Data Processing Addendum, if and to the extent its stated applicability conditions are met VENDOR DATA TERMS
- Auvik Terms of Service (User), if Auvik requires acceptance by a Client user who is given account or portal access USER TERMS

Version: Subscription Services Agreement and Terms of Service (User) effective August 1, 2023; Service Specific Terms applicable to the purchased features; Data Processing Addendum current online version accessed August 3, 2026 and applicable to the Auvik agreement.

Acceptance: Accepted through Quote as a form of assent and by access or use to the extent stated in Auvik's terms. If Auvik presents a separate account-level or user-level acceptance step, Client or its authorized user must complete that step before access. Surety retains the accepted Quote and the applicable archived versions.

1Password

Services Guide service: Password Manager.

- Subscription Terms for Business Customers CUSTOMER TERMS
- 1Password Data Processing Agreement VENDOR DATA TERMS

Version: Subscription Terms last updated September 12, 2024; Data Processing Agreement current online version applicable to the order.

Acceptance: Accepted through Quote and by access or use. Surety provides access to the listed terms at the point of sale and retains the accepted Quote and archived versions.

Foxit Software

Services Guide service: PDF Editing Software.

- Foxit Software Inc. License Agreement for Software Applications END USER LICENSE

Version: June 27, 2025.

Acceptance: Accepted through Quote and by installing, copying, downloading, accessing, or using the product as stated in the license agreement.

Tungsten Automation (Printix)

Services Guide service: Printer Management.

- Subscription Terms of Service CUSTOMER TERMS

Version: January 2024.

Acceptance: Accepted through Quote and by use of the subscription service as stated in the terms.

CyberFOX (AutoElevate)

Services Guide service: Privileged Access Management (PAM).

- CyberFOX Master Terms and Conditions `CUSTOMER TERMS`

Version: Last updated April 25, 2024.

Acceptance: Accepted through Quote and by click, order, access, use, or continued use to the extent stated in CyberFOX's terms.

SuperOps

Services Guide services: Remote Helpdesk; Remote Monitoring and Management Agent; Server Monitoring & Maintenance; Updates & Patching; Workstation Monitoring & Maintenance.

- SuperOps Terms of Use `CUSTOMER TERMS`
- SuperOps Data Processing Agreement `VENDOR DATA TERMS`

Version: Terms of Use effective December 27, 2025; Data Processing Agreement effective March 29, 2024.

Acceptance: Accepted through Quote and by access or use where stated in SuperOps's terms. Because Surety holds the provider account, only provisions expressly applying to Client, Client's users or end users, Client data, or Client's use of the affected service are incorporated.

Cisco Duo

Services Guide service: Two Factor Authentication.

- Duo Service Terms and Conditions page, which identifies the governing terms by subscription start date `ROUTING PAGE`
- For subscriptions beginning on or after November 20, 2019: Cisco General Terms and Duo Offer Description `CUSTOMER TERMS`
- For subscriptions beginning before November 20, 2019, where still applicable: Duo Service Terms and Conditions for End-Customers of a Reseller `PASS-THROUGH TERMS`
- Cisco Data Protection Agreement, when applicable under the governing Cisco terms `VENDOR DATA TERMS`

Version: Cisco General Terms v.6.0, last modified September 10, 2025; Duo Offer Description v.9.1, last modified December 4, 2025; legacy pass-through terms last updated May 25, 2018.

Acceptance: Accepted through Quote for the terms applicable to the subscription start date. Client or its authorized users must also complete any provider-presented click-through or access acceptance. Surety retains the accepted Quote and applicable archived versions.