Verticomm

Managed IT Services Guide

Last updated: November 19, 2025

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 Verticomm ("Verticomm," "we," "us," or "our"); **however, only those services specifically described in the Quote will be facilitated and/or provided to you (collectively, the "Services").**

Throughout this Services Guide, references to "Client," "you," or "your" mean the entity who has accepted a quote, proposal, service order, or similar document (electronic or otherwise) from Verticomm.

By accepting the Quote, you agree to the terms of all agreements included in the Quote, the terms of all Scope of Works included in the Quote, the terms of the Master Services Agreement ("MSA") (https://www.verticomm.com/verticomm-master-service-agreement), and the terms of the Services Guide (https://www.verticomm.com/verticomm-services-guide). If you do not agree to any of the terms set forth in the Quote, the terms of any Scope of Work included in the Quote, the terms of the Master Services Agreement, or the terms of the Services Guide, then you should not accept or sign the Quote. From this point forward, this Quote, the Agreements included, the Scope of Works included, the Master Services Agreement, and the Services Guide will be collectively referred to as "Agreement." 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.

Please read this Services Guide carefully and keep a copy for your records.

Core Managed Services

Our Core Services are the 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 account manager.

Managed Services Base Fee:

To consistently provide Managed IT services, while also providing clear and transparent billing on our invoices, there will be a base fee associated with all managed services contracts. This base fee goes towards core systems and tools that we leverage across the client base and allows us to broadly manage and improve service without modifying the specific "Core Managed Services" listed below.

IT Systems Monitoring

Description

With the help of our tools, we track key performance indicators, events, and alerts from covered devices, while working to identify potential issues and alert the appropriate teams. We provide 24/7 monitoring and alert triage so that actions can be taken in an effort to keep your business running smoothly, enabling you to concentrate on your core operations.

Sales Prerequisites

1. Minimum 10 Devices ($250/month)
2. Must be paired with IT Service Desk and IT Systems Management Services.
3. Supported systems include Physical and Virtual Servers, Firewalls, Routers, Managed Switches, etc.

Deliverables

1. **Remote Monitoring and Management (RMM) Agent Installation:** This agent runs on Covered Devices and collects system information, logs key events, and monitors various metrics for alert conditions. It also provides us with secure remote access to the environment.
2. **Network Monitor Installation:** We install and configure our agent for network monitoring.
3. **Event, System, and Service Monitoring**: Our tools monitor services, metrics, events, and other system information for alert conditions to raise tickets for investigation and triage.
4. **Ticket/Alert Triage**: We manage the real-time triage of tickets generated by our monitoring systems to notify you or our internal teams of issues that may impact your IT services.
5. **Reporting**: Monitoring and ticket reports to provide clear visibility into your IT environment.

Constraints

1. Under this service, we do not collect ALL metrics, events, alerts, or other system messages. Only information required (by our pre-determined conditions) is utilized. Collected monitoring information is not stored for a specific amount of time, outside of what is required for our monitoring.
2. Monitoring can only be performed on systems that are compatible with our tools. While our tools are compatible with most systems there are certain scenarios where monitoring is unavailable.
3. Our Network monitoring relies on a locally installed agent. This agent must run on a compatible system within your business network, and that device must be able to communicate over the network with all other Covered Devices. If a compatible device is not available, one must be provided or purchased for use.
4. Monitoring and alerting will vary based on the device type. For example, servers will have different monitors and alerts than network devices. We do not perform monitoring on workstations (outside of passive monitoring performed by our IT Systems Management tools).
5. All Covered Devices must be able to communicate securely outbound over the network to our cloud-hosted monitoring providers.
6. All Covered Devices must comply with constraints detailed by the Terms and Conditions outlined in this document and the Master Services Agreement (MSA).
7. 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.

Hours of Support

Business support is provided 7:00 AM and 6:00 PM MST. Monitoring and triage of events is provided 24x7x365. Alert response SLOs are covered under our IT Service Desk Offering.

Pricing

Pricing will be determined during Presales/Quoting process.

Additional setup and onboarding fees will be required.

IT Systems Management

Description

Our IT Systems Management service provides your company with proactive maintenance (as described below) across your Covered Devices in an effort to help keep things running smooth. We validate system configurations against our baselines and report the configuration status on a recurring basis to keep you informed.

Sales Prerequisites

1. It must be purchased with IT Systems Monitoring and IT Service Desk services.
2. IT Systems Management provided only for Microsoft Windows environments.
3. Minimum $700 cumulative IT Systems Management Agreement.
4. All Critical environment systems are expected to be managed under the IT Systems Management Agreement.

Deliverables

1. **Documentation**: Using our suite of tools and professional experience we create documentation about the environment and its configuration. Documentation includes a systems asset list, device configuration, network diagram, and secure storage of provided credentials.

2. **OS Patching and Firmware Updates**: Automated OS patching will be provided through our automation agents. Patching includes patch installation, compliance monitoring, and correction of failed patch installations (for servers). Firmware updates for Covered Network Devices will occur at least once every 6-months, or upon notification of a critical severity release (CVE 9.0 or higher).

3. **Backup Management**: Management of existing backup systems, which includes monitoring that backups are completed successfully and appropriately in an effort to meet your Recovery Point and Recovery Time Objectives.

4. **Configuration Management**: Management of system baseline configuration in an effort to maintain the functional state of the Covered Device.

5. **Configuration Validation**: Monthly validation of the configuration of the Covered Environment and included systems to ensure alignment with our standards.

6. **Reporting**: Through this service, we provide recurring reports on OS patch compliance and backup status.

Please note that our deliverables vary depending on the type of Covered Device. Please refer to the chart below for an accurate description of what deliverables are provided:

Deliverable	**Servers**	**Network Equipment**	**Workstations**
Documentation	✓	✓	Asset List Only
OS Patching and Firmware updates	✓	✓ (* see constraint 7)	✓ (*** see constraint 9)
Backup Management	✓	✓ (** see constraint 8)	
Configuration Management	✓	✓	
Reporting	✓	✓	Patch compliance

Constraints

1. All Covered Devices must be able to communicate outbound over the network to our cloud-hosted monitoring providers.
2. All Covered Devices must meet or exceed our Minimum Requirements.
3. All Covered Devices must comply with constraints detailed by the Terms and Conditions outlined in this document and the Master Services Agreement (MSA).
4. Management provided only for Microsoft Windows Server environments.
5. IT System Management for Workstations requires a minimum quantity of 100 units. This is to account for the core system management and tool costs. Additional devices over 100 units will be billed at the per-unit price specified on the quote.
6. Configuration changes are not covered under this service. Certain configurational changes can be handled under our IT Service Desk service, while other changes will need to be managed through our Projects team. Depending on the scope of the required changes additional charges may apply.
7. * On covered network equipment OS Patching and Firmware updates are only managed on devices sold by us. Firmware and OS patches for other Covered Devices may be performed upon request through our IT Service Desk offering.
8. ** Automated backups of covered network devices will only be performed if the device is compatible with our tools. Devices that are not compatible with our tools will be backed up manually in accordance with our internal change management policy, per-device, through our IT Service Desk service or project based at our discretion.
9. *** Workstations covered by our IT Systems Management service will be configured to automatically patch based on our default patching policy. Workstations that fail to install patches or that do not meet patch compliance will **NOT** be automatically remediated under this Service. Remediation of failed workstation patching will be reported to the client monthly and will be remediate upon request under our IT Service Desk offering, or at an hourly rate at our discretion.
10. 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.

Hours of Support

Business support is provided 7:00 AM and 6:00 PM MST.

Service Level Objectives

Maintenance can occur at all times but will primarily be fulfilled during our normal business support hours.

Additional maintenance may also occur after-hours, at our discretion, during our recurring patching and maintenance windows.

Pricing

Pricing will be determined during Presales/Quoting process.

Additional setup and onboarding fees will be required.

IT Service Desk

Description

Our IT Service Desk offering provides our clients with reactive remote support for their IT Environments. Requests can include simple day-to-day IT operational requests, IT issue resolution, compliance reporting assistance, requests for IT project launches, etc. In addition to user requests, our IT Service Desk service also handles management and resolution for alerts raised by our IT Monitoring services, allowing us to monitor and attempt to resolve issues with minimal client involvement.

Verticomm aims to organizes all support issues into one of four different support categories; Level 1 for issues that are known, and a resolution path is documented, Level 2 for issues that are known but the resolution is undocumented, Level 3 for issues unknown with no documented resolution, and Level 4 for issues that require vendor engagement.

Our IT Service Desk offering is sold on a ticket-by-ticket model averaged out to a minimum monthly commitment. This allows us to support your needs while helping keep your costs consistent and predictable. For tickets handled over your monthly commitment you agree to pay for support on a time and materials basis at our then-current hourly labor rates as defined by the **Verticomm Rate Card**. Information on these current rates, and the Rate Card, is available upon request.

Sales Prerequisites

- Client must have an active IT Monitoring and IT Systems Management Service on the Covered Devices.
- Must meet minimum service value qualifiers.

Deliverables

1. Access for authorized staff to contact our IT support team through email, chat, or phone.
2. Access to four different Service Levels ("Service Levels") of IT support:
    a. **Level 1 support:**
        i. **For issues that are well known and the resolution is documented.** Provides frontline assistance to quickly address common user issues and inquiries. Our technicians are available to handle a wide range of IT-related concerns, including password resets, user account management, software installations, and basic troubleshooting. With Level 1 support, we aim to provide prompt response times and efficient problem resolution in an effort to provide minimal disruption to your daily operations. Our goal is to provide timely, friendly, and reliable support that enables users to get back to work swiftly.
    b. **Level 2 support:**
        i. **For issues that are known, but the resolution is not well documented.** For more complex technical issues, our Level 2 support offers advanced troubleshooting and problem-solving expertise. Our technicians possess in-depth technical knowledge and experience to tackle a wide variety of IT challenges. They can assist with software and hardware issues, network connectivity problems, application errors, and similar issues.
    c. **Level 3 support:**
        i. **For problems that are unknown and undocumented.** Our Level 3 support provides expert-level assistance for intricate and critical IT issues. This tier is staffed by our

most experienced and certified engineers who possess specialized knowledge in various areas, such as server administration, network infrastructure, and cybersecurity management. Level 3 support handles complex incidents that require advanced troubleshooting, in-depth analysis, and strategic problem resolution. Our team can work closely with clients to identify underlying causes, implement long-term solutions, and provide recommendations in an effort to optimize their IT environment. With Level 3 support clients have access to top-tier technical expertise that can help provide the highest level of system performance, security, and reliability.

d. **Level 4 support:**

   i. **External/Vendor Support management for Problems Not Supported by Verticomm.** This level of support is meant to provide our clients with assistance with vendor level support that may require technical expertise to maintain Covered Systems or Supported Software.

Constraints

1. All support levels are provided remotely using our Remote Management Tools. All on-site support needs will be billed at an additional rate.
2. Support will only be provided for systems covered by our IT Monitoring and IT Systems Management services.
3. Assistance for personal devices is not included and will be provided at our discretion and on a good faith basis only with no guarantees.
4. Any service ticket that is projected to take more than 8 hours to resolve or exceeds 200% of the estimated resolution time may, at our discretion, be escalated to a project-level engagement under our professional services offering. Additional fees will apply for such escalated services, and the client will be notified in advance to agree on terms.
5. Our IT Service Desk service does NOT include recovery or remediation in the event of a Disaster.
6. All Covered Devices must comply with constraints detailed by the Terms and Conditions outline in this document and the Master Services Agreement (MSA).

Hours of Support

1. Business support is provided 7:00 AM and 6:00 PM MST.
2. Support Desk hours are dependent on priority and severity of the issue at hand, with regular support provided from 7:00 AM to 6:00 PM MST.

Service Level Objectives

See Terms and Conditions for details on our Priority Level definitions and Service Level Objectives.

Pricing

Pricing will be determined during Presales/Quoting process.

Additional setup and onboarding fees will be required.

Add-on products and services

The below Add-on products and services (“Add-ons”) are designed to be enhancements to our core offerings and are meant to add flexibility and coverage to meet the varying needs of our client base. They 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 account manager.

Microsoft Tenant Management

Description

Our Microsoft 365 Entra ID Management service provides your company with proactive maintenance (as described below) across your Microsoft 365 Tenant to help keep the environment secure. We validate the environments configurations against our baselines and report the configuration status on a recurring basis to keep you informed.

Sales Prerequisites

1. It must be purchased with IT Systems Monitoring, IT Service Desk services, and IT Systems Management.
2. Microsoft 365 Tenant with at least Entra ID P1 license.

Deliverables

1. **Policy Configuration Management**: Deployment of baseline configuration policies to align to Verticomm standards.

    - Entra ID Policy Management
    - Intune Device Policy Management
    - Azure Tenant Policy Management

2. **Monitoring of Policy Configurations**: Automated validation of configuration policies and alerting on deviations.

    - Entra ID Policy validation
    - Intune Device Policy validation
    - Azure Tenant Policy validation

3. **Policy/Settings Backup**: Policies and settings are automatically backed up every night.

4. **Reporting**: Through this service, we can provide multiple reports on the environment including a tenant audit report.

Constraints

1. Verticomm must have the appropriate Global Delegated Admin Privileges.
2. Configuration changes that are outside of our security baseline are not covered under this service. Certain configurational changes can be handled under our IT Service Desk service, while other changes will need to be managed through our Projects team. Depending on the scope of the required changes additional charges may apply.
3. Client must NOT change the environment configuration unless expressly approved in writing by us.

Hours of Support

Business support is provided 7:00 AM and 6:00 PM MST.

Price

Pricing will be determined during Presales/Quoting process.

Software Licensing

Description

Verticomm's Software Licensing Add-on aims to simplify the process of acquiring and managing software licenses for your business. As an authorized reseller, we offer a wide range of software licenses from leading vendors, while also providing consolidating billing with our other Services.

Sales Prerequisites

1. Only available to customers of our IT Managed Service offerings.
2. Compatibility Assessment: Ensure the client's existing systems are compatible with the proposed software solutions. License Audit: A preliminary review of the client's current software licenses to avoid duplication and ensure cost-effectiveness.
3. Compliance Check: Verification that the client's organization complies with software usage policies and regulations, which could affect the type of licenses required (EDU/GOV licensing, etc).

Deliverables

1. Direct Procurement from Partners: Verticomm procures software licenses directly on behalf of clients through our partnerships with leading software vendors. This includes a wide range of products such as Office 365, Microsoft 365, Windows Server licenses, and other software available through our distribution channels.
2. License Allocation to Customer Accounts: Once purchased, Verticomm delivers the license(s) to the applicable system, ensuring that the license is ready for immediate deployment and use within the client's IT environment.
3. Consultation and Support: We are available to advise on the selection of software licenses, including cost-benefit analysis, feature comparison, and future scalability.
4. Automated Renewal (where applicable).
5. Monthly billing: Consolidated monthly statements for purchased licenses.

Constraints

1. Vendor Restrictions: Licenses are available only for software from vendors within our reseller program. Availability may vary based on vendor policies and market region.
2. Non-refundable Licenses: Once procured, software licenses cannot be returned or refunded. Clients should ensure the chosen solutions meet their needs before purchasing.
3. Some software licenses REQUIRE that support be provided through Verticomm (as the licensing reseller). Software support is NOT included in the license cost and is provided at an additional cost, through our IT Service Desk Offering.
4. Each individual software license may have its own constraints defined by the vendor and reseller.
5. Survivability of Software Licensing: The software licensing procured under this agreement shall remain in effect and continue to be valid until the actual expiration date of the license(s), irrespective of the termination or expiration of this agreement.
6. Compliance and Legal Use: Clients must adhere to the software vendor's End User License Agreement (EULA) and comply with all usage terms and conditions. Client must also adhere to our Terms and Conditions.

Price

- Price is dependent on numerous factors including but not limited to the specific software license, license term, commitment duration, vendor, etc.
- Additional on-time procurement, setup, or onboarding fees may apply.

Infrastructure-as-a-Service (IaaS)

Description

Infrastructure-as-a-Service (IaaS) is a cloud computing service that lets customers host their IT infrastructure in the cloud. IaaS provides scalable and flexible infrastructure for various workloads, such as web hosting, data storage, analytics, or development.

We offer IaaS through our Microsoft Indirect Reseller partnership, which enables us to resell Microsoft Azure services to our customers. Azure is a leading cloud platform that supports a wide range of IaaS solutions, such as virtual machines, containers, storage accounts, network services, backup and recovery, and security tools. By using Azure, our customers can benefit from the reliability, performance, and innovation of Microsoft's cloud infrastructure.

Sales Prerequisites

1. Must be purchased along with IT Systems Management Service.
2. Client infrastructure should primarily be running on Microsoft Windows.
3. Minimum Spend $1,400 in recurring monthly infrastructure costs

Deliverables

1. Setup Microsoft Azure IaaS subscription under new or existing Microsoft tenant account.
2. Provide passthrough billing of IaaS charges to client.
3. Manage IaaS support requests through Direct Reseller and Microsoft.

Constraints

1. All usage of services must adhere to Microsoft terms and conditions.
2. Our IaaS service offering is billed at a monthly recurring minimum base fee. Usage over this base fee will be charged directly to the client.
3. All IaaS services will only be monitored, managed, and/or serviced based on additionally purchased IT Services (Monitoring, Management, and Service Desk).
4. Migration, deployment, and configuration changes to the IaaS service offering that are not covered under our IT Management or IT Service Desk Services, can be provided as projects for an additional fee.

Price

The cost for IaaS Services will depend on how they are set up and used. The base cost for using Azure IaaS services will be determined in advance based on the planned environment architecture with the assistance of our System Engineers and Solution Architects. We charge and bill at MSRP prices, which we get from our direct reseller relationship with Microsoft. All IaaS costs including (but not limited to) usage, consumption, server licensing, Access licensing, and transaction fees will be invoiced to the client monthly. Any excess costs above the estimated base fee will be directly passed on to the client. Any IaaS usage below the estimated base fee will be charged, at a minimum, at the agreed base fee regardless of usage.

Cyber Security Stack

Description

Our Cyber Security Stack service is designed to help secure and align Covered Devices to our Minimum-Security Standards Baseline. This baseline includes Endpoint Detection and Response ("EDR") and threat hunting software that is monitored by a Security Operations Center ("SOC") operating 24x7x365 to provide strong security for your servers and endpoints. We also provide a Managed Detect and Response ("MDR") solution for Microsoft 365 that constantly checks for suspicious activity and signs of a possible breach. Security awareness training is also made available for employees to help them recognize and avoid common cyber threats.

Please note that delivery of our Cyber Security services may involve the implementation of multiple distinct security products depending on your needs. Each of these products will appear individually on your billing statements and will be charged at least the quoted minimum amount for the duration of the Agreement term. Any usage or consumption beyond the quoted minimum will be billed to the customer at the agreed-upon rate.

Sales Prerequisites

1. Must have an approved and supported backup system in place for all critical assets.
2. Must have an existing IT Monitoring and IT Service Desk agreement for all Covered Devices.

Deliverables

1. Installation and configuration of an **Endpoint Protection and Response (EDR)** tool on all covered servers and workstations.
2. Installation and configuration of **Threat Hunting software** on all covered servers and workstations.
3. Implementation of **Office 365 Identity Protection** tool.
4. Implementation of **Security Awareness Training** platform for authorized users.
5. Alert monitoring of EDR and Threat Hunting Software by a 24x7x365 Security Operations Center (SOC).
6. Validation of security alerts raised by tools, automated remediation of applicable alerts, automated and manual host isolation upon validation of threats.
7. Reactive support for security incidents (not remediated through automation) will be handled under our IT Service Desk service.

Constraints

1. All Covered Devices must be able to communicate outbound over the network to our cloud-hosted solution providers.
2. All Covered Devices must comply with constraints detailed by the Terms and Conditions outline in this document and the MSA.
3. Due to the nature of IT, subscription to this service does NOT guarantee complete protection from viruses, ransomware, hackers, or other cyber security risks. While our cyber security stack can be a valuable and effective component of your Cyber Security Program it cannot, on its own, protect your business from every possible risk.

4. Remediation and recovery from Cyber Security incidents is typically handled under our IT Service Desk offering. Incidents that require significant reconstruction of your environment, or more than commercially reasonable time, may require additional billable professional services (project) work.
5. Billing for Cyber Security services is based on the number of covered or protected assets and/or users. As with our other services, the Quote will outline the minimum quantity that will be billed for each product that is implemented, and quantity above the minimum will automatically be billed.
6. Each security product within the Cyber Security Stack will appear as an individual line item on your bill. Each product will incur at least the quoted minimum charge for the duration of the Agreement term, regardless of actual usage. Any usage beyond the minimum will be billed at the quoted rate.

Pricing

Pricing will be determined during Presales/Quoting process.

Backup-as-a-Service (Baas)

Description

Our Backup-as-a-Service offering is designed to provide backup services for client's on-premises infrastructure. We partner with industry leading backup vendors to source right-sized backup solutions in an effort to meet your backup and recovery needs.

Sales Prerequisites

1. The environment must be compatible with one of our backup solutions.
2. Must have IT Systems Monitoring service (enables us to triage backup alerts).
3. Must have IT Systems Management service (allows us to proactively manage backup configurations)
4. Must have IT Service Desk service (allows us to handle reactive restore requests and change requests).

Deliverables

1. Management of encrypted and secure On-site and Off-site backup repositories.
2. Development of Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) based on business needs, and configuration of backup systems to meet RTO and RPO requirements.
3. Periodic recovery testing.
4. Setup of backup environment to alert on backup failures. Alerts will be triaged under IT Systems Monitoring service offering and resolved under IT Service Desk service.

Constraints

1. All Covered Devices must be able to communicate securely outbound over the network to our cloud-hosted backup provider.
2. All Covered Devices must comply with constraints detailed by the Terms and Conditions outlined in this document and the Master Services Agreement (MSA).
3. File, Folder, System, or object recovery will be handled under IT Service Desk service.
4. Does not include Disaster Recovery.

Price

Pricing will be determined during Presales/Quoting process.

Additional setup and onboarding fees will be required.

Compliance Services Pro

Description

Compliance Manager GRC is a tool that allows customers to measure their own IT security compliance with industry standard frameworks, identify gaps with their compliance, and develop a plan to close those gaps. Through our service clients get access to this tool along with our assistance in setting up the tool, performing data collection, performing assessments, performing technical reviews, and helping develop milestones and a plan of action. We also provide blocks of consulting hours with our industry certified cyber security professionals.

Sales Prerequisites

1. Current active Managed Services Client

Deliverables

1. Development and configuration of Compliance Manager GRC
2. Team of dedicated Project Managers to keep your compliance efforts on track
3. Quarterly Execution Deliverable with prioritized roadmap and supporting GRC reports
4. Enhanced self-guided assessment with Compliance Services Pro guidance
5. Custom, role-based workbook and controls assignment mapping
6. Delivery preparation meeting with your MSP’s POC
7. Compliance Concierge Service including, up to four, one-hour, SME led control assessment guidance sessions
8. Direct end-customer. Third-party expert delivery assistance with compliance SME staff.

Constraints

1. The desired compliance framework must be supported by Compliance Manager GRC software suite. Compliance Manager GRC currently supports these industry standards:
    a. CIS Controls v8 (IG1, IG2, IG3), CMMC 2.0 (Level 1, Level 2), Cyber Insurance Readiness, Essential 8, EU GDPR (Controller and Processor), FTC Safeguards Rule (0-4999/5000-plus consumers – part 314), HIPAA (Security, Privacy, breach notification), NIST 800-171, NIST CSF, PCI DSS, and SOC 2.
2. Client MUST assign a designated internal resource to collect internal business information, processes, procedures, etc as required by the Standard selected.
3. In order to get the best results Compliance Manager GRC, ongoing Client involvement and ownership of tasks is REQUIRED.
4. The client acknowledges that the purchase of this software and service do not guarantee compliance.
5. Verticomm does not perform third-party audits and certifications. Client must work with an authorized third-party if they are looking to pass audits or gain certifications.

Price

Price includes a recurring licensing fee for access to the compliance manager system, as well as a fee based on client size and compliance requirements. Complex frameworks that have a larger number of controls will take an increased amount of time to handle and are priced accordingly.

IT Professional Services

Description

Our Professional Services encompass project-based work that is distinct from our core managed and add-on services, which are recurring in nature. These one-time services are designed to address specific client needs through dedicated projects. Each project is defined by a detailed Scope of Work (SOW), which outlines the deliverables, estimated pricing, hours, and other pertinent details. Professional Services ensure that unique client requirements are met with tailored solutions, enhancing the overall IT infrastructure and capabilities.

Sales Prerequisites

Project must align with one or more of the following Approved Projects:

- Onboarding
- Cloud Migration to Azure
- Addon Deployment (Security, backups, etc.)
- Office 365 migration
- Physical Site Migration
- Custom projects designed and scoped by the Verticomm presales and Systems Architect teams.

Deliverables

The deliverables for IT Professional Services are outlined separately in the Quote and attached Scope-of-Work (SOW) documents. Any changes to the deliverables after the project initiation will require a Change Order, which may affect the pricing and timeline of the project. The client is responsible for reviewing and approving the deliverables as specified in the SOW.

As part of the deliverables outline in the SOW, Verticomm will:

- Provide a single point of contact for the duration of the project
- Audit and review the installation design
- Gather all pertinent information for the project
- Create a Project Plan
- Achieve approval for the Detailed Project Plan by both Verticomm and the CLIENT
- Coordinate equipment rollout schedule in accordance with the Detailed Project Plan
- Schedule required resources
- Provide and receive project status updates on an agreed time basis and as milestones are achieved
- Schedule and attend status and planning meeting before actual configuration work commences
- Deliver the services specified in the “Scope of Work” Section(s)

Constraints

To successfully deliver the agreed upon services specified in the SOW, the CLIENT agrees to:

- Designate a person for this project communication, and who has the authority to act on all aspects of the services and responsible for testing per the project plan timeline (POC).
- Provide Verticomm with access to CLIENT’s facilities as required by the SOW.
- Provide current environmental documentation (EG: network diagram, system information, documentation, etc.) within five (5) business days either at the start of the project, or as requested by Verticomm, and as needed to complete delivery of the SOW.

- CLIENT will work with assigned Project Engineer in creating User Acceptance Testing (UAT) Plan
- CLIENT will follow UAT Plan to complete User Acceptance Testing
- CLIENT will sign off on UAT Migrate Acceptance form once UAT is complete

Hours of Support

1. Business support is provided 7:00 AM and 6:00 PM MST.
2. Professional Services work Is primarily provided between 7:00 AM to 6:00 PM MST, but will depend on project deliverables and may require work outside of normal business hours.

Price

Pricing will be determined during Presales/Quoting process.

IT Environment Assessment

Description

Our **IT Environment Assessment** is a comprehensive one-time evaluation of your organization’s IT environment. In this project-based service, Verticomm will analyze key areas – including hardware assets, identity and access management, network infrastructure, and overall cybersecurity posture – to identify strengths, weaknesses, and risks. We collect data using non-intrusive tools and expert technical review, then deliver detailed summary reports with findings and actionable recommendations. This assessment provides valuable insight into your IT environment’s current state so you can make informed decisions to improve reliability, security, and alignment with industry best practices.

Sales Prerequisites

1. A signed Scope of Work **(SoW)** or Quote for the assessment, with agreement to Verticomm’s Master Services Agreement (MSA) and Services Guide terms.
2. **Client cooperation and access:** The client must provide necessary administrative access, documentation (e.g. network diagrams, asset lists), and timely responses to facilitate data collection and interviews during the assessment.
3. **External Clients Only (non-**existing customers)
4. **Client meets Ideal Customer Profile**

Deliverables

1. **Executive Summary**: A cumulative report that consolidates all the reports below. This report contains scoping information, findings, maturity reports, and recommendations in one final draft report.
2. **Secondary Environment Summaries**: Detailed reports that summarize raw technical data into four specific categories. These reports provide a layer of detail between the executive summary and the raw data.
    a. **IT Asset Summary:** A report detailing the inventory and health of the organization’s IT assets (servers, workstations, cloud instances, and other key systems). This summary reviews hardware and system information such as operating system versions, patch levels, hardware age/warranty status, and backup status. It highlights any issues in asset life cycle or maintenance (e.g. outdated systems, capacity constraints, patch compliance gaps) and provides recommendations for upgrades or improvements in asset management.
    b. **IT Identity Summary:** A report evaluating the state of identity and access management. It analyzes user account inventories in on-premises Active Directory and cloud directories (e.g. Microsoft 365/Azure AD), including the use of **multi-factor authentication (MFA)**, password policies, and the management of administrative and service accounts. The summary identifies potential security gaps such as inactive or over-privileged accounts and weak credential practices. It offers recommendations to improve identity hygiene and align account management with best practices.
    c. **IT Network Summary:** A report examining the network infrastructure and connectivity across the organization’s sites and any cloud environments. It documents the network topology (with key network devices such as firewalls, switches, routers, and wireless access points) and assesses network configurations and performance. The summary highlights any network issues or risks—such as misconfigurations, single points of failure, or capacity bottlenecks—and reviews the effectiveness of current network design (including integration between on-premises and cloud networks). Recommendations are provided to enhance network reliability, security (e.g. firewall policies, segmentation), and performance.

d. **IT Security Summary:** A high-level report consolidating cybersecurity-related findings from the assessment. This summary evaluates the organization's security posture by mapping key technical findings from the asset, identity, and network reviews to industry-standard security controls (based on **CIS Controls**). It highlights strengths and critical vulnerabilities in areas like endpoint protection, account security, data backup, and network defense. The report includes an overall risk assessment and prioritized, actionable recommendations to address identified gaps and improve the organization's security posture and compliance with best practices.

3. **Raw Reports and data artifacts:** During our collection process, we generate a significant amount of data. Some of this data is highly valuable and is referenced directly in the final reports, but some provide little overall value. Regardless, we deliver all data, artifacts, and reports generated during this process back to you in a final file collection. This data can be used during remediation, for findings verification, for historical/compliance reasons.

Constraints

1. **Scope of service:** This assessment is an advisory and analytical service only. It is limited to evaluating and reporting on the environment's current state; it **does not include** implementation of remediations, configuration changes, or ongoing monitoring of the environment. Any remediation or follow-up services would be handled through a separate agreement or project.
2. **Information-dependent results:** Findings and recommendations are based on the information and access provided by the client and observed during the assessment period. Verticomm will make best efforts to uncover issues, but cannot guarantee identification of every potential problem, especially if certain data, systems, or locations are outside the agreed scope or inaccessible. The assessment provides a point-in-time snapshot; it should not be relied upon as a continuous audit or real-time monitoring solution.
3. **Non-disruptive process:** All assessment activities will be conducted in a read-only or non-intrusive manner. No invasive testing (such as penetration testing or intentional stress tests) is performed as part of this service. Verticomm's tools and agents used for data collection will be approved by the client and are designed to avoid impacting system performance or availability.
4. **Client responsibilities:** The client is responsible for promptly furnishing any required information, approvals, and resources to support the assessment. Delays or failure to provide access to critical systems or data may limit the completeness of the assessment.
5. **Standard terms:** All systems and data involved in the assessment must be within the client's legal authority to analyze, and all engagement activities must comply with Verticomm's standard Terms and Conditions and Master Services Agreement. Any findings or recommendations are provided for the client's internal use; Verticomm is not liable for third-party use of the assessment results.

Hours of Support

Work for the IT Environment Assessment is performed during Verticomm's regular business hours (7:00 AM to 6:00 PM MST, Monday–Friday). Scheduling will be coordinated with the client to minimize disruption. If project work is required outside of normal hours (for example, to accommodate off-hour data gathering or client availability), this must be arranged in advance and may incur additional fees as agreed in the SOW.

Price

IT Environment Assessment is offered as a fixed-price professional service engagement. Pricing for this service varies based on the size and complexity of the client's environment and will be defined in the

Quote/SoW. A custom proposal will be provided to the client, outlining the project fee for the assessment and any related expenses (e.g. travel or onsite work, if applicable).

Automated Network Penetration Testing

Description

Verticomm utilizes the vPenTest platform by Vonahi Security to perform automated network penetration testing, enabling us to offer our clients both internal and external network security assessments. This powerful tool combines the expertise, methodologies, and tools of seasoned penetration testers into a convenient SaaS platform, helping you and your organization meet compliance requirements and adhere to security best practices. With vPenTest, we simulate various attack scenarios, such as authentication attacks, privilege escalation, and data exfiltration, and provide detailed reports to help you continuously enhance your security posture.

Sales Prerequisites

1. Current active Managed Services Client

Deliverables

1. Access to the Vonahi Security portal and a Company tenant.
2. Setup of scheduled penetration tests with standard settings for schedule, scope, and coverage.
3. Assistance with configuration of internal and/or external systems for scheduled penetration assessments.
4. Review and assign reporting and administration responsibilities for associated scanners.
5. After assessment is completed, we will help finalize and generate all pen test reports and data.
6. Delivery of any reports to the client-authorized recipients.
7. Includes four 1-hour blocks of consultation time with one of our industry-certified cyber security staff.

Constraints

1. All target systems must be accessible via the network and have the necessary permissions and firewall configurations to allow scanning and testing activities.
2. Any form of remediation is NOT included in this service offering. Remediation services can be provided under our IT Professional Services (project) offering or within the constraints of an active and applicable Managed Services Agreement (IT Systems Management or IT Service Desk).
3. Internal network scanning requires the installation of an agent or device within the client's network environment to facilitate testing.
4. The time required to perform and complete the assessment depends on the number of systems targeted, available bandwidth, services, and the responsiveness of those services. While we aim to provide an accurate estimate for the expected scan duration and report delivery, actual assessment duration may vary due to environmental conditions.
5. Penetration testing depends on the availability of network resources. Any disruptions in service, such as power outages or network downtimes, may impact the test results and require rescheduling.
6. While testing aims to identify as many security weaknesses as possible, it is acknowledged that not every flaw within the environment may be identified during the allocated time frame.
7. Testing activities, especially those involving exploitation, may cause temporary disruptions or reduced performance in network services.
8. The assessment must be performed within the agreed-upon time frame. Any delays or changes to the schedule could require a change order and may impact the project’s duration and cost.

Price

Price includes a recurring licensing fee for access to the Vonahi Security, as well as a fees based on client size and testing scope. Larger networks that have a larger number of endpoints will take an increased amount of time to scan and are charged depending on number of IP's in the configured assessment.

Hours and further assistance with the results and reporting are billed for our Cybersecurity Team.

Pricing will be determined during Presales/Quoting process.

Terms and Conditions

Covered Environment

Managed Services will be applied to the number of devices indicated in the Quote ("Covered Devices"). The list of Covered Devices may be modified by mutual consent through a service ticket; however, we reserve the right to modify the list of Covered Devices at any time (i) if we discover devices that were not previously included in the list of Covered Devices and which are receiving Services, (ii) should be receiving services to prevent gaps in coverage, (iii) or as necessary to accommodate changes to the quantity of Covered Devices.

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

Services for devices that do not meet the "Covered Devices" definition will be provided to you on a good faith basis, at our discretion, and additional charges may apply. 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.

We will provide support for any software applications that are licensed through us ("Supported Software"). Such software will be supported on a commercially reasonable basis and any support required beyond Level 2 support will be facilitated with the applicable software vendor or producer.

Services for software that does not meet our "Supported Software" definition will be provided to you on a good faith basis, at our discretion, and additional charges may apply. 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.

In the event of a failure affecting software, Client may be required to provide software installation media and key codes necessary to facilitate reinstallation and setup.

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

IT Professional Services

The delivery of IT project work under our IT Professional Services offering can be challenging and complex. This section details expectations and information that is specific to Professional Services.

Professional Services - Assumptions

Verticomm creates SoWs under the following assumptions. If one or more of these assumptions proves to be invalid, costs and other project factors may be impacted.

- CLIENT acknowledges that the success of the proposed engagement relies on collaboration (response to questions, open accurate information sharing and periodic communication with Verticomm by phone or email) and participation by CLIENT staff members.
- Verticomm assumes that an accepted response time will be 24 hours or one business day.
- Upon acceptance of this Scope of Work (proposal), Verticomm Project Engineer will schedule the project with the CLIENT. The proposed schedule will be based on the availability of Verticomm resources. All efforts will be made to accommodate the client's specific scheduling needs.
- Verticomm does not commit any professional services resources until the client approves the project in writing.
- CLIENT has the proper infrastructure in place that meets or exceeds current standards for data and/or voice transmission.
- CLIENT has all cables properly terminated for desired workstations.

Professional Services - Deliverables

This SOW will produce the specific deliverables and/or objectives ("Deliverables") listed in the SoW(s) attached to this Quote. Costs contained in the SOW are created based on these Deliverables and objectives only. Tasks, deliverables and responsibilities not explicitly addressed within this SOW are beyond its scope and can only be provided pursuant to the change process described herein or pursuant to a separate SOW as mutually agreed to by both parties. Except as explicitly set forth in this SOW, Verticomm shall have no obligation to provide maintenance or support services for Deliverables or to modify or remediate Deliverables in any manner following CLIENT's acceptance thereof.

Professional Services – Additional Services Required

Should it become apparent that factors beyond Verticomm's control require for additional services in order to complete the project described herein, a written estimate of such additional services and their charges will be provided to the CLIENT by the Project or Account Manager prior to proceeding therewith. Upon receipt of the estimate, the CLIENT shall, within ten (10) days, provide a written acceptance or rejection of the estimate. Beyond the date of rejection of the estimate (either in writing or at end of the ten (10) day period), Verticomm shall have no obligation to perform the additional services.

Professional Services - Change Management Procedures

Effective change management is critical to ensure the success and seamless execution of any project. Throughout the lifecycle of the project, there may be circumstances where modifications to the Scope of Work (SOW), deliverables, or timelines are necessary. To address these changes systematically and collaboratively, Verticomm has established a comprehensive Change Management Procedure. This procedure outlines the steps for initiating, evaluating, and approving changes to ensure that all project adjustments are managed efficiently and transparently, minimizing disruptions and maintaining alignment with the client's objectives and expectations.

The following are key scenarios where change management procedures apply:

- **CLIENT-initiated changes** to the Scope of Work and/or specifications for the Services or Deliverables.
- **CLIENT-initiated changes** to the Point of Contact (POC), causing a delay in the project timeline.
- **Non-availability of resources** that are beyond either party’s control, such as vendors or partners.
- **Environmental or architectural impediments** not previously identified.
- **Failure of Verticomm or CLIENT** to act on the responsibilities of each party as stated in this SOW.

In the event either party desires to change this Statement of Work, the following procedure will apply:

1. Upon request, Verticomm will submit the Change Management Request and Authorization form (“Change Request”), which is attached as Appendix B, to the other party. The Change Request will describe the nature of the change, the reason for the change, and the impact the change will have on the Scope of Work, which may include changes to the Deliverables and the schedule.
2. A Change Request may be initiated either by the CLIENT or by Verticomm for any changes to the SOW. The designated Program/Project Engineer of the requesting party will review the proposed change with his/her counterpart. The parties will evaluate the Change Request and negotiate in good faith the changes to the Services and the additional charges to implement the Change Request. If both parties agree to implement the Change Request, the appropriate authorized representatives of the parties will sign the Change Request, indicating the acceptance of the changes by the parties.
3. Upon execution of the Change Request, said Change Request will be incorporated into, and made a part of, this SOW.
4. Whenever there is a conflict between the terms and conditions set forth in a fully executed Change Request and those set forth in the original SOW or previous fully executed Change Request, the terms and conditions of the most recent fully executed Change Request shall prevail.

Professional Services Completion

Notice of Completion: Upon reaching what we believe to be the completion of the project, we will issue a formal "Notice of Completion" to the CLIENT.

Client Acknowledgment: CLIENT is required to acknowledge receipt of the Notice of Completion by signing and returning it within five (5) business days of receipt.

Assumption of Completion: If CLIENT fails to sign or otherwise acknowledge the Notice of Completion within the specified five (5) business days, the project shall be deemed complete and accepted by the Client.

Disputed Completion: Should the CLIENT believe that the project has not been completed to their satisfaction, the CLIENT must notify us in writing within the same five (5) business day period. Upon receiving such notification, we will review the CLIENT's concerns and, at our sole discretion, determine whether the project is indeed incomplete.

Final Determination of Completion: The determination of project completion is ultimately at our sole discretion. If we concur that the project has not been completed in accordance with the agreed scope of work (SOW), we will collaborate with the Client to address and complete the remaining tasks. However, if the additional work required was not outlined in the original SOW, additional fees may apply.

Additional Fees: Any additional work not specified in the original SOW will be subject to a separate fee arrangement, which will be communicated to the Client before proceeding.

Physical Locations Covered by Services

Services will be provided remotely unless, in our discretion, we determine that an onsite visit is required. Verticomm visits will be scheduled in accordance with our Definition of Priority Levels and are subject to technician availability. Unless we agree otherwise, all onsite Services will be provided at Client's primary business location. Unless otherwise explicitly stated, additional fees will apply for all on-site visits. Please review the Service Level section below for more details.

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 always provided/maintained by Client. Should the Client fail to meet any of these minimum requirements, the Client is obligated to undertake all necessary measures to ensure their environment adheres to the stipulated standards and conditions. This includes, but is not limited to, updating, upgrading, or replacing software and hardware, securing necessary licenses, and implementing required security measures as specified by Verticomm. The Client must complete these adjustments within a timeframe determined by Verticomm in its reasonable discretion. If the Client fails to complete these adjustments Verticomm reserves the right to suspend or terminate services subject to a notice period and a reasonable opportunity for the Client to remedy the situation.

- Client must provide us with sufficient administrative privileges to the Environment where we have management responsibilities.
- Client must maintain an active vendor support contract on all devices within the Covered Environment. Devices without an active vendor support contract will only be supported at our discretion, and on a good faith basis. Should we decide to provide services on devices without an active vendor support contract, you agree to pay for these services on a time and materials basis at our then-current hourly labor rates as defined by the Verticomm Rate Card.
- All Supported Software must be genuine, licensed, and vendor- or OEM-supported.
    - Additionally, if necessary, all Supported Software must have an active support agreement that allows us to receive vendor support.
    - If we ask for proof of authenticity and/or licensing, you must provide us with such proof.
- All Covered Servers and Endpoints must have an approved Endpoint Detection and Response (EDR) tool installed.

- All externally exposed systems or environments must be configured to require multi-factor authentication (MFA) for all external authentication to that system (EG: Office 365, Azure, Citrix, OneDrive, Google Cloud, etc.).
- Client's employees should complete recurring security awareness training.
- The Covered Environment must have a currently licensed and vendor-supported backup solution covering all key assets including but not limited to servers, storage devices, networking equipment, etc.
- Mobile Devices – (Apple iOS and Android): Support for mobile devices is only provided for apps and services sold or provided by us and does not include the mobile device operating system (OS), or other third-party apps.
- All wireless data traffic in the Covered Environment must be securely encrypted.
- All physical servers must be connected to working Uninterruptable Power Supply (UPS) devices.

Any cost required to bring the Covered Environment up to these minimum standards is not included in our Services.

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

Patching and Maintenance Windows

Unless otherwise agreed upon by both parties in writing, we will perform routine patching and maintenance of the Covered Equipment as part of the IT Systems Management service.

OS patching will occur, by default, in accordance with our client patching policy. Additional patching may occur as needed at our discretion.

Maintenance Window: There is a standing maintenance window every third Saturday of the month, from 10:00PM to 6:00AM MT, during which we may perform any necessary maintenance tasks on the Covered Equipment, such as updates, backups, configuration changes, or optimization. We will make a good faith effort to notify you of any maintenance that is planned outside of this maintenance window.

We make every reasonable effort to minimize the impact of patching and maintenance on the client's operations and availability of the Covered Equipment. However, you acknowledge that some patching and maintenance activities may require temporary downtime, cause reduced performance, or cause other unexpected issues with the Covered Equipment. You further acknowledge that we are not liable for any damages or losses resulting from such downtime, reduced performance, or other issues unless caused by our negligence or misconduct.

The client may request changes to the patching and maintenance schedule to suit their specific needs, if the changes do not compromise the security, stability, or functionality of the Covered Equipment. The client must submit any such requests in writing to us at least two weeks before the desired change date. We will review the request and either approve it or propose an alternative solution. We reserve the right to reject any request that would violate our terms and conditions, our policies and procedures, or any applicable laws or regulations.

Business Support

Business support is meant to describe the administrative support component of our service delivery and includes communications such as billing questions, service delivery issues, contract renewal options, feedback collection, etc. Business support does not describe our hours of service or our Service Level objectives (SLOs). Hours of service and SLOs are specific to each independent service and are defined under each service item (and below) in more detail.

Business Support is offered Monday through Friday during our normal business hours from 8:00AM to 5:00PM MT. Business support will be limited or unavailable during Verticomm Observed Holidays.

Service Level Objectives

Service Levels Objectives define our intended response times for IT Service Desk Service Levels and are based upon the Priority Level of individual issues or requests (“Service Level Objective” or “SLO”). SLOs and Priority Level are determined by Verticomm in our discretion. The timing of response and resolution to issues and requests will generally be performed during our hours of support, which can be found under the individual service items.

In addition, Verticomm may offer on-site services for clients who require in-person assistance for remediation. On-site services are subject to Verticomm's discretion, availability, and scheduling, and will incur additional charges regardless of the service plan selected by the Client. Changes related to on-site services will be billed to the client upon completion.

Please note that the SLOs outlined in this document are targets and not guarantees. Verticomm will make reasonable efforts to meet the SLOs, but they may not always be achievable due to factors beyond our control, such as network outages, hardware failures, force majeure events, or other extenuating circumstances. Failure to meet the SLOs does not constitute a breach of contract or entitle the client to any refunds, credits, or compensation.

Priority Levels

Priority Levels are an internal metric used by Verticomm to determine the SLOs based upon the Scope and degree of business Impact of the given incident (“Priority Levels” or “Severity Levels”), as follows:

Scope

Verticomm defines “Scope” by how many users are affected.

- Company Wide: Whole Company is affected.
- Partial: Departments or large groups of users affected.

- Minimal: One or small groups of users affected.

Impact

Verticomm defines “Impact” as how many of your business processes are affected.

- High Impact: Major Business processes are stopped.
- Medium Impact: Business is degraded, but there is a reasonable workaround.
- Low Impact: More of a nuisance than a stoppage.

Priority level Chart			
	Scope		
Impact	Company Wide	Department	Single User
High	1	1	2
Medium	2	2	3
Low	3	4	4

Priority / Severity	**Response**	**Resolution**	**Escalation**
1 – Emergency/Urgent	30 minutes	4 hours	30 Minutes
2 – High	2 hours	8 hours	1 hour
3 – Medium	4 hours	16 hours	2 hours
4 - Low	8 hours	24 hours	3 hours

Note: All time frames start once we are fully notified of the issue by the Client via our support portal, help desk, or telephone (number provided in the Quote). Notifications through other channels may delay remediation. SLO times depend on the service’s support hours. Resolution and escalation times reflect active work on a ticket, not elapsed hours.

Disasters and Disaster Recovery

Within this Agreement, "Disaster" refers to (i) any significant event causing widespread disruption to the Client's operations where the event impacts either the entire company or significant departments (“company wide” or “partial” in scope) and halts major business processes ("High Impact"), and (ii) the resolution of the event anticipated to exceed 200% of the standard resolution time for Priority Level 1 incidents, translating to more than 8 hours from the time of notification. Recovery from Disasters is not covered under the standard IT Service Desk offerings and may require separate arrangements, potentially incurring additional charges.

Verticomm Observed 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 – Half Day

Offboarding

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

- Removal / disabling of monitoring agents in the Environment provided by Verticomm.
- Removal / disabling of endpoint software from the Environment provided by Verticomm.
- Termination, cancellation, and/or removal of any products we are providing as part of our Services, subject to applicable licensing constraints including but not limited to our Service constraints, the vendor end-user license agreement, and any other vendor agreement.
- Provide export of existing documentation and credentials from knowledgebase maintained by Verticomm upon request.

Note: once our monitoring and support agents are removed from the environment all services (monitoring, management, and support) will cease, consistent with the offboarded services.

Fees

The fees for the Services will be as indicated in the Quote. We reserve the right to cancel orders arising from pricing or other errors. Taxes, shipping, handling, and other fees may apply.

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 to pay all fees for third-party services that accrue 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. Initially, you will be charged the monthly fees as indicated in the Quote. Subsequently, if there are changes to the Covered Environment or modifications in the number of authorized users accessing the Covered Environment, the associated fees will be adjusted accordingly.

When Verticomm delivers specific Services or Add-ons, automated processes may be employed to monitor changes within the Covered Environment. This includes the automatic installation of software agents, such as monitoring tools, cybersecurity software, and other licensed software, to prevent inadvertent coverage gaps. You acknowledge and agree to pay the charges for these additional Services or Add-ons, billed according to the actual usage of the services.

It is your responsibility to identify any devices that should not be included as 'Covered Devices.' Upon request, or as stipulated in specific agreements, Verticomm will provide a list of the Covered Devices for your review. This provision may include automatic periodic reports, depending on the specific services and terms agreed upon. Should you identify any discrepancies, you must notify Verticomm. We will conduct a good faith review of the Covered Environment and, at our discretion, may issue a credit if a billing error attributable to Verticomm is confirmed.

Appointment Cancellations. You may cancel or reschedule any appointment with us at no charge (except for non-cancelable expenses) by providing us with notice of cancellation at least one business day in advance. If we do not receive a timely 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 scheduled appointment time, then you agree to pay us a cancellation fee equal to any and all expenses that are incurred.

Access Licensing. One or more of the Services may require us to purchase certain "per seat" or "per device" licenses ("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 cannot be transferred to any other customer. You understand and agree that regardless of the reason for termination of the Services, fees for Access Licenses are non-cancellable 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.

Term; Termination

The Services will commence, and billing will begin, on the date indicated in the Quote ("Commencement Date") and will continue through the initial term listed in the Quote ("Initial Term"). We reserve, in our discretion, the right to delay the Commencement Date until all onboarding/transition services are completed.

Removal of Software Agents: You acknowledge and understand that the presence of our software agents is crucial for the delivery of the Services outlined in our IT Services Guide. You understand and agree that, 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 Covered Environment. Should these agents be removed or disabled without our express written consent, it will directly impact our ability to fulfill the Service deliverables. Consequently, any failure on our part to deliver these Services, resulting directly or indirectly from the unauthorized removal or disabling of our software agents, will not be deemed a breach of our obligations under this Agreement. Furthermore, you agree to indemnify us against any claims or damages arising from such a failure to provide Services, acknowledging that this limitation of liability is a key element of the Agreement between us, given the reliance on these software agents for Service delivery.

Return of Equipment: Within ten (10) days after being directed to do so, you must remove, package and ship, to a location designated by Verticomm, at your expense and in a commercially reasonable manner, all hardware, equipment, and accessories leased, loaned, rented, or otherwise owned by Verticomm. 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 you agree to pay the replacement value of all such unreturned or damaged equipment.

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 the applicable Policy.

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 Verticomm, and Client shall not modify these levels without our prior written consent.

Modification of Covered Environment and Third-Party Service Configurations:

You acknowledge that changes made to the Covered Environment or to the configurations, features, and/or functions ("Configurations") of certain third-party services provided under a Quote—without our prior written authorization—may have a substantial and/or negative impact on both the delivery and effectiveness of the Services and may result in an increase in the fees charged. Therefore, you agree to refrain from moving, modifying, altering, or changing any portion of the Covered Environment or the Configurations of third-party services. This includes, but is not limited to, adding or removing hardware, installing applications, modifying the configuration or log files of the Environment, and altering Configurations of third-party services without our prior knowledge or written consent. Should unauthorized changes result in disruptions to the Services or an increase in fees, you agree to pay any additional costs arising from or related to such changes.

Cyber Security

Verticomm acknowledges the evolving and sophisticated nature of cyber threats and emphasizes that complete protection against all cyber incidents cannot be guaranteed, despite our commitment to employing robust cybersecurity measures.

As such, you understand and agree that no entity can guarantee absolute protection against all cyber threats. You acknowledge the inherent limitations in detecting, preventing, or eliminating all cyber threats and that Verticomm cannot assure the recovery of data compromised by cyber incidents.

You acknowledge that cyber threats may exist within your environment prior to the implementation of our Services and Verticomm cybersecurity solutions may not be able remediate the Covered Environment without engaging additional services, which may incur extra charges.

Lastly, you acknowledge that even upon purchasing Verticomm's Cyber Security Stack Add-on, designed to fortify the Covered Environment against cyber threats, Verticomm cannot and does not make any guarantees regarding the complete detection, prevention, or elimination of cyber threats.

Verticomm Data Collection and Privacy Policy

In the delivery of our IT Services, Verticomm aims to collect only the data necessary for the efficient delivery and continual improvement of our Services. We are committed to safeguarding your privacy and ensuring the security of your data. We do not sell or share your data with third parties except as necessary for the delivery of our Services or as mandated by law. Our full Data Collection Policy outlines our practices in detail and is available upon request. You may contact us at **support@verticomm.com** to obtain a copy or to inquire about any recent updates, which may reflect changes in our practices or legal requirements.

Third-Party Software Policy

In providing our IT Services, you acknowledged that these services may require or include third-party software or services, governed by their own set of policies including but not limited to privacy policies, data collection policies, End User License Agreements (EULA), Acceptable Use Policies (AUP), etc. By utilizing our Services and any associated or resold third-party software, you expressly agree to the collection and use of data as outlined by these third parties' policies. It is your responsibility to review and stay informed about these policies. Acceptance of our services constitutes agreement to these terms.

Licenses

As part of our Services, if we are required to re-install or replicate any software provided by you, it is your responsibility to ensure that all such software is properly licensed. Verticomm reserves the right, but not the obligation, to require proof of licensing before proceeding with installing, re-installing, or replicating any software into the managed environment. Please note, the cost of acquiring any necessary licenses is not included in the scope of the Quote unless expressly stated therein.

Additionally, you agree to pay for additional software licensing determined to be or to have been in use while being a customer of Verticomm, if required. This includes retroactive payment if an audit discovers non-compliance with licensing requirements.

Breach/Cyber Security Incident Recovery

Unless otherwise expressly stated in the Agreement, 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 at our then-current hourly labor rates, as defined by the Verticomm Rate Card. 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 Covered Environment, or (ii) prevents normal access to the Covered Environment, or impedes or disrupts the normal functions of the Covered 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 Agreement, 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.

Backup and Disaster Recovery (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 Verticomm nor its designated affiliates will be responsible for the outcome or results of such activities.

BDR services generally require a reliable, always-connected internet solution. Data backup and recovery time may depend on the speed and reliability of your internet connection. Infrastructure (power, internet, etc) outages may prevent the BDR services from operating correctly. In addition, all computer hardware is prone to failure due to equipment malfunction which may impact the functionality of BDR services, for which we will be held harmless, unless otherwise specified in the Agreement. 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. Verticomm cannot and does not warrant that data corruption or loss will be avoided, and Client agrees that Verticomm shall be held harmless if such data corruption or loss occurs. Client is strongly advised to keep a local and off-site backup of all data to mitigate against the unintentional data loss.

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.

Procurement

Equipment and software procured by Verticomm 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, Verticomm does not make any warranties or representations regarding the quality, integrity, or usefulness of the Procured Equipment or any related manufacturers warranties. 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. Verticomm is not a warranty service or repair center. In the event that Verticomm facilitates the return or warranty repair of Procured Equipment, 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 Verticomm will be held harmless, and (ii) Verticomm is not responsible for the quantity, condition, or timely delivery of the Procured Equipment once the Procured Equipment has been tendered to the designated shipping or delivery courier.

Business Review / IT Strategic Planning Meetings

From time to time, Verticomm may invite the client to participate in business reviews or IT strategy meetings. These meetings aim to provide the Client with information about recommended or, in some cases, critical changes to their IT infrastructure, alongside discussions on the client's current and anticipated IT needs. While recommendations for specific services or solutions may be made, this does not constitute an endorsement of any manufacturer or service provider.

The Client understands and agrees that Verticomm is not required to schedule these meetings on a regular basis. Should the client deem additional meetings necessary beyond those initiated by Verticomm, it is the client's responsibility to request such meetings.

Advisory Role and Limitations

The consultancy, advice, and suggestions provided by Verticomm are intended solely for informational and/or educational purposes and should not be construed as directives for business decisions. Verticomm expressly disclaims any assumption of a directorial, officer, or fiduciary role within the Client's organization. Consequently, Verticomm shall not be listed or represented as holding such positions in any of Client's corporate records, accounts, insurance policies, or during compliance audits. This exclusion extends to, but is not limited to, roles or titles such as a virtual Chief Information Officer (vCIO), virtual Chief Information Security Officer (vCISO), or virtual Chief Technology Officer (vCTO), whether formally or informally. The Client acknowledges that while Verticomm's input may be valuable in the decision-making process, the final decisions and their consequences rest solely with the Client. Verticomm's input is to be considered as part of a broader set of information the Client evaluates in making decisions related to their business operations.

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.

Access and Use of Internal Security Policies and Compliances

As part of our ongoing commitment to transparency and security, we may, upon request, share with you copies of our internal security policies or third-party attestations of our security practices ("Internal Security Documents"), such as our Service Organization Control 2 (SOC 2) Type 2 report. These documents are provided for informational purposes only to assist in understanding the security measures we employ in the provision of services to you.

It is important to note that these Internal Security Documents reflect our security practices and compliance status and are not intended to be, nor should they be used as, a representation or warranty of compliance on behalf of your business. You acknowledge and agree that:

1. **Non-Transferability of Compliance**: The security practices and compliance certifications or attestations provided by us pertain exclusively to our operations and services. They do not extend, transfer, or apply to your business operations or compliance requirements. Utilization of our services, or access to our Internal Security Documents, does not confer upon you or your business any form of compliance certification or attestation.

2. **No Substitution for Own Compliance**: You should not present any of our Internal Security Documents as evidence of your own compliance to insurance carriers, auditors, regulators, or any third-party. Doing so may constitute a misrepresentation of your compliance status and could have serious legal and contractual consequences.

3. **Seek Independent Advice**: We encourage you to consult with competent legal counsel or a compliance specialist to understand your own compliance obligations and to develop and implement policies and procedures that are appropriate for your business.

By accessing or using our Internal Security Documents, you agree to these terms and acknowledge that reliance on our compliance status for your regulatory or insurance requirements is inappropriate and may be misleading.

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 harm, 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.

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 costs incurred in response to the unauthorized Testing Activity are not covered under the Quote, and if you request us (and we elect) to perform additional services, those additional services will be billed to you at our then-current hourly rates.

Obsolescence

Unless expressly outlined within a specific Service purchased under this Agreement, you understand and agree that it is not our obligation to actively monitor or notify you regarding equipment or software that may become outdated, obsolete, reach the end of its useful life, or acquire "end of support" status from its manufacturer ("Obsolete Element"). It is your responsibility to ensure timely and adequate replacement of any such Obsolete Element to avoid disruption or degradation of the Services provided. Any Obsolete Element shall be automatically deemed as excluded from the definition of Covered Devices under this Agreement.

Should an Obsolete Element remain in use we may, at our discretion, but shall have no obligation to, continue providing Services to the Obsolete Element, exerting good faith efforts without any warranty, guarantee of functionality, operability, or obligation to remedy any issues that may arise.

It is expressly understood and agreed that we make no representations, warranties, or guarantees regarding the performance, support, or service level outcomes related to any Obsolete Element. Furthermore, should an Obsolete Element cause any system-wide issue, such as facilitating unauthorized access or causing network failures, the services required for recovery or mitigation will be charged at our then-current rates. Under such circumstances, we offer no assurance of successful recovery, nor do we commit to any specific service level outcomes (SLO).

By agreeing to this provision, you acknowledge and agree to bear the responsibility for monitoring and replacing Obsolete Elements within your environment to maintain eligibility for full support under this Agreement. Additionally, you agree to hold harmless and indemnify us against any liabilities, losses, or expenses arising directly or indirectly from the failure to replace Covered Devices before they become Obsolete Elements.

Fair Usage Policy

To ensure high-quality service and availability for all clients, our Fair Usage Policy applies to all Services delivered by us.

Clients are expected not to misuse Services, including but not limited to:

- Creating support tickets marked urgent for non-urgent issues.
- Requesting excessive support outside typical usage patterns, such as using support as a substitute for user training.
- Initiating requests that significantly impact service delivery to other clients. We prioritize issues based on their urgency and impact, balancing support across our client base.

Services and products may be provided by third-parties or hosted on third-party SaaS or public cloud platforms. These services have their own Fair Usage Policies that You agree to comply with. It is your responsibility to review and stay informed about these policies.

Acceptable Use Policy

Our Acceptable Use Policy (AUP) applies to all Services and/or Add-ons accessed through or provided by Verticomm. You understand and agree to act in compliance not only with our AUP but also with the AUPs of third-party service providers. Our AUPs include but are not limited:

- Legal and Harmful Use: You must not use services for illegal activities or any actions that harm or may potentially harm individuals, transmit harmful or threatening materials, or harass others.
- Fraud and Deception: You must not engage in fraudulent activities or deceptive practices using the services is prohibited.
- Content and Communication: You shall not disseminate SPAM, use anonymous proxies, or distribute malware through hosted services.
- Resource Usage: You must avoid excessive use of shared resources which could impair service levels.
- Security: You shall not attempt to obtain access to accounts that you are not authorized to access, commit data theft, or commit other activities that could be considered cybercrime.
- Credentials: You acknowledge that you and your users are responsible for securing their own access credentials and managing permissions appropriately.
- Compliance with Third-party Policies: Clients must adhere to the AUPs of all third-party platforms utilized, ensuring that their activities do not violate these policies. It is your responsibility to review and stay informed about these policies.

We reserve the right to take necessary action, including suspension of services, to maintain security, integrity, and compliance with these policies. We may update this AUP at any time, with changes becoming effective immediately. Clients are encouraged to review this AUP regularly to ensure continued compliance.

VOIP – Dialing 911 (Emergency) Services

The following terms and conditions apply to your use of any VoIP service that we facilitate for you or that is provided to you by a third-party provider of such service. Please note, by using VoIP services you agree to the provisions of the waiver at the end of this section. If you do not understand or do not agree with any of the terms below, you must not subscribe to, use, or rely upon any VoIP service and, instead, you must contact us immediately.

There is an important difference in how 9-1-1 (*i.e.*, emergency) services can be dialed using a VoIP service as compared to a traditional telephone line. Calling emergency services using a VoIP service is referred to as "E911."

Registration: You are responsible for activating the E911 dialing feature by registering the address where you will use the VoIP service. **This will not be done for you, and you must take this step on your own initiative.** To do this, you must log into your VoIP control panel and provide a valid physical address. **If you do not take this step, then E911 services may not work correctly, or at all, using the VoIP service. Emergency service dispatchers will only send emergency personnel to a properly registered E911 service address.**

Location: The address you provide in the control panel is the location to which emergency services (such as the fire department, the police department, etc.) will respond. For this reason, it is important that you correctly enter the location at which you are using the VoIP services. PO boxes are not proper addresses for registration and must not be used as your registered address. Please note, even if your account is properly registered with a correct physical address, (i) there may be a problem automatically transmitting a caller's physical location to the emergency responders, even if the caller can reach the 911 call center, and (ii) a VoIP 911 call may go to an unstaffed call center administrative line or be routed to a call center in the wrong location. These issues are inherent to all VoIP systems and services. **We will not be responsible for, and you agree to hold us harmless from, any issues, problems, incidents, damages (both bodily- and property-related), costs, expenses, and fees arising from or related to your failure to register timely and correctly your physical location information into the control panel**.

Address Change(s): If you change the address used for E911 calling, the E911 services may not be available and/or may operate differently than expected. Moreover, if you do not properly and promptly register a change of address, then emergency services may be directed to the location where your services are registered and not where the emergency may be occurring. **For that reason, you must register a change of address with us through the VoIP control panel no less than three (3) business days prior to your anticipated move/address change**. Address changes that are provided to us with less than three (3) business days' notice may cause incorrect/outdated information to be conveyed to emergency service personnel. If you are unable to provide us with at least three (3) business days' notice of an address change, then you should not rely on the E911 service to provide correct physical location information to emergency service personnel. Under those circumstances, you **must** provide your correct physical location to emergency service dispatchers if you call them using the VoIP services.

If you do not register the VoIP service at your location and you dial 9-1-1, that call will be categorized as a "rogue 911 call." **If you are responsible for dialing a rogue 911 call, you agree to pay a non-refundable and non-disputable fee of $250/call, and any additional fees incurred.**

Power Loss: If you lose power or there is a disruption to power at the location where the VoIP services are used, then the E911 calling service will not function until power is restored. You should also be aware that after a power failure or disruption, you may need to reset or reconfigure the device prior to utilizing the service, including E911 dialing.

Internet Disruption: If your internet connection or broadband service is lost, suspended, terminated, or disrupted, E911 calling will not function until the internet connection and/or broadband service is restored.

Account Suspension: If your account is suspended or terminated, then all E911 dialing services will not function.

Network Congestion: There may be a greater possibility of network congestion and/or reduced speed in the routing of E911 calls as compared to 911 dialing over traditional public telephone networks.

WAIVER: You hereby agree to release, indemnify, defend, and hold us and our officers, directors, representatives, agents, and any third-party service provider that furnishes VoIP-related services to you, harmless from any and all claims, damages, losses, suits or actions, fines, penalties, costs and expenses (including, but not limited to, attorneys' fees), whether suffered, made, instituted or asserted by you or by any other party or person (collectively, "Claims") arising from or related to the VoIP services, including but not limited to any failure or outage of the VoIP services, incorrect routing or use of, or any inability to use, E911 dialing features. The foregoing waiver and release shall not apply to Claims arising from our gross negligence, or willful misconduct.