SecureData™ TECHNOLOGIES

SecureAssist

[Managed Services]

Default Terms and Conditions
SecureAssist Managed Services

Contents

Default Terms and Conditions
SecureAssist Managed Services

1. SecureAssist Overview

SecureAssist is designed to provide customers with master level expertise in Secure Data's five pillars of infrastructure (Networking, Data Center, Collaboration, Cloud, and Security) and our world-class helpdesk. The various offerings of SecureAssist provide a consistent approach to integrating our top-level engineering resources with our customers by providing a suite of expertise at our customers' fingertips. Secure Data specializes in high-touch, flexible, and truly custom programs to help customers achieve success.

2. Scope

These referenced Default Terms and Conditions, together with any specific terms and conditions agreed to in writing within the Ordering Document (collectively, the "Conditions") represent the exclusive terms and conditions for the delivery of the specified Services by Secure Data Technologies, Inc. ("Secure Data") for the benefit of the Customer within this Services Contract. Where applicable, specific terms and conditions agreed to in writing within the Ordering Document shall supersede only the contradictory provisions of these Default Terms and Conditions.

Service Contracts are formed upon the acceptance of an Ordering Document (including, but not limited to a proposal or quote document) for Services by the Customer. Secure Data will provide the Services to the Customer indicated on the Ordering Document as set out in these Conditions.

3. Period of Service and Automatic Renewal

This Services Contract shall be effective upon execution of the Ordering Document by the Customer and shall be for an initial term of thirty-six (36) months, unless sooner terminated in accordance within the Conditions of this Services Contract. Thereafter, Services Contract will automatically renew for a period of thirty-six (36) months, unless otherwise requested in writing at least three (3) months prior to the end of the Services Contract term.

Contracts which transition to a shorter term upon renewal will subject to the following price increases:

- 20% price increase for 12- to 35-month renewal when original contract was thirty-six (36) months
- 20% price increase for 1- to 11-month renewal when original contract was twelve (12) months
- 40% price increase for 1- to 11-month renewal when original contract was thirty-six (36) months

4. Managed Service Levels

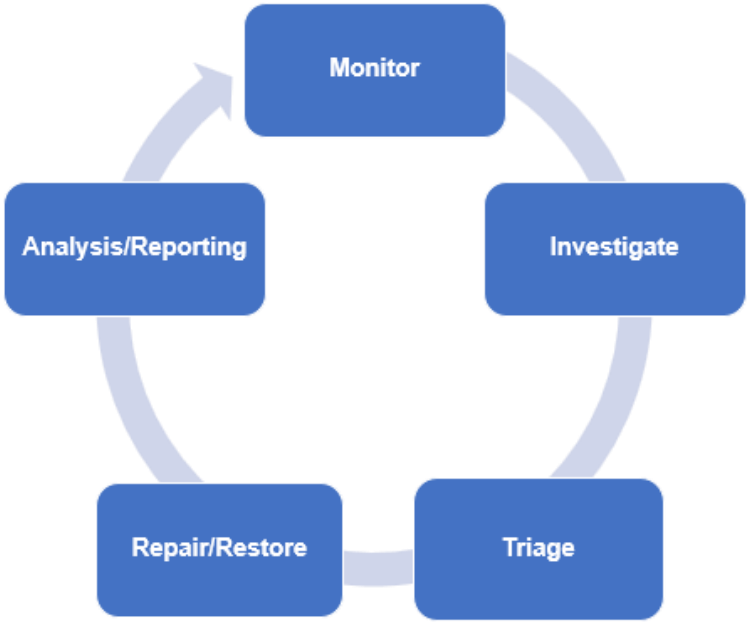
SecureAssist Services will be provided through one of three Service Levels, each defined below:

- Essential
- Enhanced
- Comprehensive

The applicable Service Level for covered device(s) and/or system(s) will be set and agreed upon by the Customer and Secure Data and identified within the language in the Ordering Document.

5. Incident Response

For incidence response covered devices and/or systems, Secure Data will use a specific Response process for any identified incidents:



Monitor: For SecureNOC, SecureFoundation, and SecureVoice: All covered devices are monitored 24x7x365, including trending statistics. Exclusion for other SecureAssist services.

Investigate: Identify the validity of the incident and the systems involved.

Triage: Restore services as quickly as possible. If the incident is a valid Business Impacting Event, the Secure Data engineer(s) will escalate to the Customer and work to contextualize the incident and suggest remediation steps. A Business Impacting Event is defined as a down device that is causing a disruption to normal business operation.

Repair/Restore: Correct service impacting issues to restore service. Restoring may be performed by Secure Data engineers or through OEM support. Implement a long-term, permanent fix based on Secure Data's recommendation. Hardware and software recommendations and purchases are not included as part of this Service Contract.

Analysis/Reporting: Findings and actions taken are compiled and shared to the Customer within the incident ticket.

Incident Definition

An incident will be defined as an event where an eligible covered device and/or system exceeds defined thresholds, as defined by the Device List provided by the Customer. Device List shall include categorization for each covered device and/or system as a (1) Critical Device or (2) Non-Critical Device. Incident thresholds are defined as:

Down	• A device is unreachable for a period exceeding 15 minutes • Default to Priority 1 for Critical Device, Priority 2 for Non-Critical Device
Device Capacity	• Usage exceeds 80% of total capacity for more than 30 minutes • Defaults to Priority 2 Incident
Component Failures	• Component failure reported by the monitored device • If failure leads to a Down Incident, down device definition will apply • Defaults to Priority 2 Incident

Licensing	• May vary by covered device and/or system • Defaults to Priority 2 Incident

6. Supported Technologies

Secure Data will support technologies for which it has domain expertise. We have partnerships with several leading technology companies, currently including Cisco, Tegile, Nimble, Pure, HPE, and VMWare – and therefore support the majority of these technologies.

Customer agrees to maintain valid vendor support on all covered devices and software in order to open incidents under SecureAssist Monitor and Response. If Secure Data is not the reseller of record on a covered device or software, Customer may be required to open vendor support cases on behalf of Secure Data. In some instances, Customer may sign a Letter of Authorization (LOA) with the vendor to allow Secure Data access to their maintenance agreements, as is required for full Monitor and Response support.

The following technologies are expressly supported and are eligible for Monitor and Response Service:

Network Infrastructure	Switches, Firewalls, Routers, Wireless LAN Controllers and Access Points, Meraki
Compute	Cisco UCS, Dell/HPE
Collaboration	Webex, Webex Contact Center, Communications Manager, Contact Center Express*, Unity Connection, Unified Presence (Jabber), Expressway, Microsoft Teams Voice
Virtualization	ESX Hosts, VCenter, VDI**
Storage	Nimble, Tintri IntelliFlash (fka Tegile/Western Digital), ExaGrid, Pure, HPE
Backup Solutions	Veeam, Barracuda (365)
Carrier Incidents	Secure Data will help Customer isolate/identify carrier related issues. Working with the provider to restore service is not included.

*Script changes require testing. After-hours cutover and/or migration is NOT included.
**Support is for existing images and VDI desktop connectivity. Creating new base images is not included.

Core Features

The following core features are included for all covered devices and/or systems:

- Break/Fix
  - Unlimited support for outage and degradation
- Configurations, Moves/Adds/Changes/Deletes
  - Up to five (5) per managed device per month
- Lifecycle Management
  - Security & EOL updates, lifecycle reviews

7. Service Priority Definitions

The following Service Priority definitions shall be applied to all Incidents (with the exclusion of SecureDesk).

	Incident Definition	Service Level Agreements	Getting Help
Priority 1 (P1) Critical	An existing network or service is down, or there is critical impact to the Customer's business operation. Impact and severity are high. Examples: - Device failure/site inaccessible - Phone system failure	Secure Data Technologies will: - Respond to P1 calls 24x7 - Call Customer contact within 60 minutes - Secure Data Technologies and the customer will commit necessary resources 24x7 to resolve the situation - Resolution time cannot be guaranteed	Priority 1 incidents are required to be phoned into our help line: 888-599-1480. We monitor the help line 24x7x365 and will respond within 60 minutes. Priority 1 issues should NOT be reported by email or through our portal. These are NOT monitored after normal working hours.
Priority 2 (P2) High	Operation of an existing network or service is impaired, but most business functions remain operational. Examples: - Primary device failure, but backup device running - Subscriber failure (phone service active but server is down) - Degraded performance or features	Secure Data Technologies will: - Respond to P2 calls during normal business hours (M-F, 8x5) - Call Customer contact within 2 hours - Secure Data Technologies and the customer will commit necessary resources full time during normal business hours to resolve the situation - Resolution time cannot be guaranteed	Priority 2 incidents can be called in or sent in via email or portal. We will respond within two hours during normal business hours.
Priority 3 (P3) Standard	Operation of a service or device is not optimal or a move, add or change has been requested. Overall functionality is intact. Impact and severity are normal. Examples: - Move, add or change - Single user or small branch issue Password reset	Secure Data Technologies will: - Respond to P3 issues during normal business hours (M-F, 8x5) - Contact Customer within 24 hours through the ticketing system - Secure Data Technologies and customer will commit resources during normal business hours to resolve the issue - Resolution time cannot be guaranteed	Priority 3 incidents can be called in or sent in via email or portal. We will respond within 24 hours during the normal business day. For

*SecureDesk SLA's are identified in the SecureDesk section

8. Service Priority Escalations

If the default classification of an Incident or ticket does not meet the Customer's needs, an Incident may be escalated in multiple ways. To escalate an Incident's Service Priority classification, Customer shall take the following steps:

- To escalate an Incident to a P2, Customer can email support@securedatatech.com to increase the priority.
- To escalate an Incident to a P1, Customer should call the support number at 888-599-1480

Upon receiving a request to escalate, Secure Data will make a best effort to honor the Customer's requested priority level. However, final assignment of Incident priority is at the discretion of Secure Data Technologies based on the circumstances of the issue.

9. Measurement and Penalties of SLA's

If an SLA is not achieved per the above Service Level Agreements, a penalty will be applied in the form of a credit per the and will be applied to the Customers next invoice. SLA penalties do not apply to Essential covered devices.

SecureBackup/Secure365 Restore Request Service Level Agreement:

The Restoration SLA is measured from the time a ticket is opened requesting a restore of Data to the time that restoration job is started. If a non-emergency restore is requested after hours, SLA will be measured from the start of the next business day. Due to the potential variation in restoration job sizes no guarantee can be made as to when the restoration will be completed.

For emergency SLA to apply, customer must call the Secure Data Global Operations Team support number at: 888-599-1480 and state that restoration request is an emergency. This must be noted as such in the restoration request ticket. Emergency SLA will not apply for an unstated emergency request.

Secure Data will begin restoration process within one hour for emergency restores and two hours for standard restores. ***Please note standard restores are only performed during normal business hours.

Penalties for SecureBackup/Secure365 Restores

Each failure to meet the SecureBackup/Secure365 restore requests SLA qualifies for a credit of 5% of MRC (monthly recurring charge) for the SecureBackup/Secure365 service only and shall not exceed 50% of the monthly contracted value. Example: SecureBackup/Secure365 monthly charge X 5% = credit.

Process for requesting Service Credit

Service credits are Customer's sole and exclusive remedy for any failure to meet any Service Level. To request a service credit, customer must be in good standing and email: billing@securedatatech.com reporting SLA violation within thirty (30) calendar days of the conclusion of the month in which the Service Level Failure(s) occurs. Customer waives any right to credits not requested within thirty (30) calendar day period.

Limitations to Service Credits

Credits will be issued once validated by Secure Data Technologies and applied toward the customer's invoice no later than two (2) months following customer's service credit request. The total service credits due to customer for any backup service that failed to meet the SLA may not exceed 50% of the monthly fees charged for use of the backup service during the month for which the service credit is to be issued. Any unused credits existing upon termination of the agreement shall lapse without reimbursement to customer.

Secure Data Holiday Schedule (2023)

New Year's Day
Memorial Day
Independence Day
Labor Day
Veterans Day
Thanksgiving Day
Friday after Thanksgiving
Christmas Eve
Christmas Day

10. SecureNOC

If Applicable, and part of your service contract, Secure Data's SecureNOC is a highly customizable managed network offering ranging from monitoring only to 24x7x365 fully managed infrastructure options. Flexibility is the key to this offering, allowing customers to choose which pieces of their network are covered and by which service level. You can monitor everything and select just the core pieces to have 24x7 coverage. We can partner with your teams and provide the expertise Secure Data is known for in the industry.

Customer responsities are identified in the Customer Responsibility section. If there is not a virtual environment, customer will provide a server meeting the required specifications. Secure Data can include one in the contract for an additional charge.

A. SecureNOC Essentials

- 24x7x365 monitoring of anything with an IP address
    - Everything from network infrastructure to IOT devices
- Secure Data expert's setup and manage the platform to monitor your devices/environment
    - Our team will handle the care and feeding of the tool to ensure you're receiving critical information about your environment
- Project management onboarding included
    - Get up and running receiving alerts quickly with our team managing the onboarding process

- Customizable email alerts
    - Choose multiple points of contacts, including distribution lists to be alerted
- Customer Portal Access includes:
    - Login to see history on your environment's alerts
    - SNMP polling
        - Up/Down
        - CPU
        - Memory
        - Interface monitoring
        - Storage (where applicable)
    - Dashboards - default dashboards provided
        - Custom dashboards available for additional fee
        - Limited to SNMP and API (where available)

B. SecureNOC Enhanced

- Everything included in Essentials plus
- Managed Service Quarterly Business Reviews
    - Used to discuss strategic business initiatives
- Remote troubleshooting and remediation during normal business hours
    - Root Cause Analysis provided on P1 issues
- 8x5 Mon-Fri for covered devices
    - After hours available for additional fee
- Moves - Adds - Changes - Deletes (New devices will be charged at the appropriate rates)
    - Switches - VLANs, Port Channels, Base Config
    - Routers - Interface Changes, Base Routing Config
    - Firewalls - Base Security Policies
    - Wireless Access Points - SSIDs, VLANs
    - SD-WAN controller and appliances - Base Config
- Full ticket visibility via Secure Data customer portal
    - View/update tickets and history
- Circuit vendor management option available for additional fee
    - Device access must be provided to affected equipment for troubleshooting purposes
    - Secure Data will work with Customer to isolate/identify Covered Carrier related issues, working with the provider to restore service
        - For network issues isolated to the circuit, Secure Data will open/manage troubleshooting ticket(s) with the carrier.
        - In some cases, Secure Data will not have access to open these tickets. In these cases, the Customer will be responsible for this effort.
    - Script changes requiring testing, after-hours cutover and or migration support are NOT included.
    - Contract management excluded

C. SecureNOC Comprehensive

- Everything included in Essentials and Enhanced plus
- Unlimited remote after-hours support
    - Priority 1 issues
- Manufacturer Specified Critical Network Patching – Up to one per month
    - Switches, Routers, Firewalls, Wireless Access Points, SD-WAN controller, and appliances
        - Secure Data will make every effort to apply patches within 30 days of request, subject to customer approval for scheduling
        - Scheduling will be dependent on customer maintenance windows and accepted risk of applying patches
            - High, medium, low, informational patches available for additional fee
- Prioritized ticket response on issues with non-covered devices
    - Ensure your non-managed devices receive priority within the Secure Data ticketing system
- Network device configuration backups - Must be Secure Data supported vendor (Meraki not included)
    - Router, switch, firewall

- Documentation of customer environment as part of onboarding process
    - Covered devices only
        - Up to one hour of customer review during onboarding
        - Topology map/diagram
        - Naming convention recommendations/best practices
        - Inventory review of existing alerts and alarms
            - Post remediation review provided during quarterly business reviews (QBRs)
        - Setup/configuration/review of customer dashboards
        - Identification of end of life/support devices
        - Escalation process and Service Level Agreements
        - Identification of critical vulnerabilities with recommended remediation plan
    - Advanced reporting/dashboards available

Exclusions to SecureNOC service

This SecureNOC Service Contract does not include any work related to the following.

- Major software releases excluded from patching
- Routing Architecture Changes
    - Static to Dynamic
    - Dynamic to Static
    - Dynamic to Dynamic
- Router/Firewall Changes
    - Converting to zone-based policy firewalls.
    - Implementation of new licensing features
- New QoS Policy Creation
    - Security Alerts
    - Firewall Threat Alerts
    - Policy Violations
- Security Information Event Management (SIEM) log collecting or monitoring.
- IP Address Management (IPAM).
- Threat prevention and adds malware or URL filtering.
    - License conversions
- PAK to Subscription based licensing through Smart account.
    - iSCSI to FC or FCOE storage traffic protocol conversion.
- New infrastructure deployment.
- Including new site deployment or new device deployment.
- Internet service migration, or any other circuit activations.
- Onsite services.
- End-of-life software or hardware; software or devices for which the Customer does not maintain valid vendor support; and root cause analysis related to unsupported technologies and services.
    - Limited support on EOL/EOS. Will be evaluated at the time of request for service
- Client has made unauthorized changes to the configuration or setup of affected, hardware, software, services, information and data or other parts of the IT environment that has affected managed devices.
- Any hardware, software, services, information and data or other parts of the IT environment not managed by Secure Data Technologies.

D. SecureNOC requirements

- Devices must be under current manufacturer support agreement.
- Software/Firmware versions must be under manufacturer supported versioning.
- For devices not under manufacturer support, troubleshooting is provided on best effort basis.

11. SecureFoundation

Secure Data's SecureFoundation is a highly customizable managed server/storage infrastructure offering ranging from monitoring only to 24x7x365 fully managed options. Flexibility is the key to this offering, allowing customers to choose which pieces of their environment are covered and by which service level. You can monitor everything and select just the

core pieces to have 24x7 coverage. We can partner with your teams and provide the expertise Secure Data is known for in the industry.

Customer responsities are identified in the Customer Responsibility section. If there is not a virtual environment, customer will provide a server meeting the required specifications. Secure Data can include one in the contract for an additional charge.

A. SecureFoundation Essentials

- 24x7x365 monitoring of anything with an IP address
    - Everything from server/SAN infrastructure to IOT devices
- Secure Data expert's setup and manage the platform to monitor your devices/environment
    - Our team will handle the care and feeding of the tool to ensure you're receiving critical information about your environment
- Project management onboarding included
    - Get up and running receiving alerts quickly with our team managing the onboarding process
- Customizable email alerts
    - Choose multiple points of contacts, including distribution lists to be alerted
- Customer Portal Access includes:
    - Login to see history on your environment's alerts
    - SNMP polling
        - Up/Down
        - CPU
        - Memory
        - Interface monitoring
        - Storage (where applicable)
    - Dashboards - default dashboards provided
        - Custom dashboards available for additional fee
        - Limited to SNMP and API (where available)

B. SecureFoundation Enhanced

- Everything included in Essentials plus
- Managed Service Quarterly Business Reviews
    - Used to discuss strategic business initiatives
- Remote troubleshooting and remediation during normal business hours
    - Root Cause Analysis provided on P1 issues
    - 8:00 AM to 5:00 PM CST Mon-Fri for covered devices
        - After hours available for additional fee
- Base Storage configuration supported
    - Changing/managing storage pools included
- Moves - Adds - Changes - Deletes
    - LUN Management
    - Base Storage Configuration
    - SAN Plugins
- Physical ESXi Host
- Management of VMware clusters
    - vCenter
        - Networking supported
        - Standard and distributed switching
    - vMotion
    - vROPS
    - vSphere
- Resource monitoring and alerting

        - Secure Data will alert to high utilization with basic analysis of environment with suggested improvements
        - Secure Data will call the customer for any covered devices at time of alert
    - Full ticket visibility via Secure Data customer portal
        - View/update tickets and history

C. SecureFoundation Comprehensive
- Everything included in Essentials and Enhanced plus
- Unlimited remote after-hours support
    - Priority 1 issues
- Prioritized ticket response on issues with non-covered devices
    - Ensure your non-managed devices receive priority within the Secure Data ticketing system
- Manufacturer Specified Critical SAN and VMware Patching - Up to one per month
    - Secure Data will make every effort to apply patches within 30 days of request, subject to customer approval for scheduling
    - Scheduling will be dependent on customer maintenance windows and accepted risk of applying patches
        - High, medium, low, informational patches available for additional fee
- SAN Software Upgrades - Requires customer coordination
    - One upgrade per year included
        - As part of the upgrade process hardware/software compatibility will be checked and verified
        - Pre-upgrade Checks and analysis
            - Compatibility review against other known technologies to ensure compliance
                - Customer responsible for sharing outside technologies and providers
- SAN Reporting - Provided at Quarterly Business Reviews as available
    - General usage reports - utilization and storage consumption
    - Current performance - IOPS, latency, disk IO, throughput
    - Lifecycle information - Warranty/support information and renewals
- VMWare Reporting - Provided at Quarterly Business Reviews as available
    - General usage/performance reports - utilization and consumption RAM/CPU
    - Lifecycle information - Warranty/support information and renewals
- Documentation of customer environment as part of onboarding process
    - Covered devices only
        - Up to one hour of customer review during onboarding
        - Topology map/diagram
        - Naming convention recommendations/best practices
        - Inventory review of existing alerts and alarms
            - Post remediation review provided during quarterly business reviews (QBRs)
        - Setup/configuration/review of customer dashboards
        - Identification of end of life/support devices
        - Escalation process and Service Level Agreements
        - Identification of critical vulnerabilities with recommended remediation plan
    - Advanced reporting/dashboards available

D. SecureFoundation Exclusions - These items would be considered projects and EaaS can be used to supplement
- Major software releases excluded from patching
- VMWare Exclusions:
    - VMware tools and VMware hardware
    - Additional Host Installations
    - Cloud integration
    - VXRail
    - NSX
    - Resource pooling
    - vSphere Host Profiles
    - Resource forecasting not included as detailed analysis is required and can be provided as a separate billable support engagement

- SAN Exclusions
    - Switching from iSCSI to Fiber Channel not included and would be a separate project and billable
    - Changing block levels is not included
    - Re-claiming used space not included as
        - Detailed data analysis would be required and would require a statement of work and is billable
    - Creation of new LUNs included but re-architecture of LUN environment is considered a project and billable
    - Storage forecasting not included as detailed analysis is required and can be provided as a separate billable support engagement
- Supported SAN technologies:
    - NFS
    - Fiber Channel
    - FCoE
    - iSCSI
    - VX

- Supported Vendors:
    - Contact your Account Manager for a list of supported vendors

E. SecureFoundation requirements

- Devices must be under current manufacturer support agreement.
- Software/Firmware versions must be under manufacturer supported versioning.
- For devices not under manufacturer support, troubleshooting is provided on best effort basis.

12. SecureBackup

SecureBackup is a Secure Data offering that allows us to help customers with their server backup needs. We have the flexibility to provide the basics with a secure off-site Cloud Connect repository powered by our partners, all the way to a fully managed backup solution where you turn daily backup hassles over to us!

With our Enhanced and Comprehensive plans, Secure Data's Managed Services team supports the underlying hardware and software used to deliver the SecureBackup Service, as well as administers and monitors the backup and recovery processes put in place. Customers receive a daily report detailing the status of backup jobs, completion of jobs, and any other information about the jobs. Customers open support requests to create or alter backup jobs, change data retention policies, or get any additional information about the service. Application-Aware, Image-Based backups creates application-consistent, image-level VM backups with advanced, application-aware processing including transaction log truncation.

SecureBackup decreases backup storage requirements and network traffic with built-in deduplication. Additionally, multiple compression options are used to balance storage consumption with performance and backup proxy load.

A. SecureBackup - All Plans

- **Ownership of the Data**: The backup data being stored on the Hardware and at the Data Center remains the sole property of the customer. If the customer chooses to terminate services, Secure Data will assist customer in the orderly termination of services. The customer agrees to pay Secure Data the actual costs of rendering such assistance. You warrant that You are the owner or legal custodian of the data transmitted to Cloud Storage pursuant to the terms of this Agreement and that You have full authority to transmit said data and direct its disposition in accordance with the terms of this Agreement.
- **Data Security**: All data is fully encrypted during transmit off-site and while stored off-site using:
    - Files encrypted with 256-bit AES
    - Transmittal to off-site remote servers using TSL (Transport Layer Security) technology
    - Data stored off-site remains encrypted at all times
- **Support Hours**: Support hours are Mon-Fri 8:00am – 5:00pm (CT). Simple file or directory restoration up to a single VM restore is covered under this agreement. Restoration outside of these hours will constitute a billable event.

        - Major incident recovery services: Major incident recovery services such as recovery services after a complete server hardware failure, a failure resulting from third party vendors updating a system, a failure caused by force majeure, theft, vandalism, etc., are not covered under this agreement and will constitute a billable event, both to recover the data from offsite as well as to restore any services.
        - Customer will bear responsibility for getting server and applications up and running. Remote support can be provided at rates outlined in in the Services Agreement.
        - Data contained within a backup job that has expired or has exceeded defined retention cannot be recovered.
- **Service Conditions**: Customer acknowledges that certain conditions outside of Secure Data's control may adversely impact the ability of Secure Data to perform successful backups or restores of Image. Examples of such conditions are listed below:
    - Customer task, software, scheduled job or other human intervention intentional or otherwise renders portions, complete files, or complete file systems unavailable to Service.
    - Failure of customer software, operating system, Agent or Service
    - Network connectivity issues between customer server and cloud including but not limited to packet loss, lack of sufficient network capacity to support required backup bandwidth
    - Backup job in seeding status
- Customer acknowledges that in the event of a support issue, customer is responsible for on-site cooperative testing with Secure Data support to assist in the diagnosis of the issue
- **Compatibility**: Secure Data controls the version of hardware and software running on its infrastructure and does not guarantee that it is compatible with any version changes made by the customer on their network, server, OS or application infrastructure. It is the Customer's responsibility to ensure that any version changes planned on their infrastructure is compatible with Secure Data equipment and software including cloud services.
- Insider Protection (service provider recycle bin) provided for 7 days to help prevent malicious deletion of customer backups is an optional add-on available for all SecureBackup plans at an additional fee

- **Maintenance**
    - **Scheduled Maintenance:** In order to maintain performance, Secure Data performs Scheduled Maintenance within its published maintenance windows. This may require that specific Services be suspended during the maintenance period. Loss of Service Availability due to Scheduled Maintenance is not deducted in calculating Service Availability. Secure Data will use commercially reasonable efforts to notify customer in advance of any Scheduled Maintenance that may adversely affect customer's use of the Services.
    - **Emergency Maintenance:** Secure Data may need to perform emergency maintenance, including security patch installation and hardware replacement. Secure Data will not be able to provide customer with advance notice of emergency maintenance. Loss of Service Availability due to emergency maintenance is not deducted in calculating Service Availability.

B. SecureBackup Essentials Plan

- **Cloud**: Secure cloud repository will be provided in a Tier 3 data center via Secure Data's partnerships.
    - Storage will be provided in 1TB increments
        - 1TB = 1000GB
    - Once a customer's cloud backup repository hits 90%, it will trigger an increase to the next 1TB to ensure backups continue to run successfully
        - Update will be reflected in the customer's next monthly billing cycle
    - All ingress/egress fees are included with the monthly fees
    - VMware and Hyper-V along with Windows and Linux physical servers supported for backup
    - Veeam Block Storage Repositories:
        - Optional Insider Protection (service provider recycle bin) may be purchased and will be provided for 7 days to help prevent malicious deletion of customer backups
    - Veeam Object Storage Repositories
        - Optional Object Lock (prevents data deletion and manipulation for a specific period of time) may be used

- Project management provided to ensure timely onboarding
- Data seeding will be done utilizing customer WAN connection unless requested
    - Additional one-time $750 fee will be assessed to cover USB drive, shipping, and engineering time
- Customer is responsible for procuring and maintaining all required software/ hardware, other equipment, all Internet, communication, and other services necessary to access and use the services
    - All hardware/software must meet vendor minimum requirements

C. SecureBackup Enhanced Plan

- **Backup Server**: The customer agrees that the local backup server utilized by Secure Data, in the execution of this service shall remain the property of Secure Data and must be returned if requested.
    - Customer further agrees to cease the use of any technology that remains the property of Secure Data upon termination of this agreement.
    - If the local backup server is stolen, damaged or destroyed, the customer must pay current market prices at the time of the loss for a replacement unit.
    - Local backup server will remain under active vendor support for the life of the agreement and will be monitored with Secure Data monitoring software/agents
        - Next business day shipping on hardware replacements
        - Secure Data will ensure the hardware/software remains under support and will replace or upgrade platforms no longer supported by the manufacturer
    - Secure Data will ensure local Veeam backup server is patched with critical Microsoft patches as defined by the Microsoft Security Update Severity Rating System
    - Endpoint anti-virus will be provided on the local backup server as part of the managed service
    - Local backups will be stored on the Secure Data backup server with disks configured in a RAID 6 level for redundancy
    - Restore only customer access will be provided to the local backup server if requested
- **Software**: Secure Data will provide Veeam backup software on the local repository
    - Updates of the software will be performed as needed to maintain compatibility with Cloud provider's requirements
    - Troubleshooting of the software will be provided as part of the SecureBackup managed service
- **Backup Jobs**
    - Retention policies can be customized to create as many archived versions of data and full recovery points as needed. Default retention is 30 days on the local backup server and 30 days in the cloud
        - Customer may request longer retentions both locally and in the cloud for additional fees
    - Backup Frequency: Servers can be backed up as frequently as every hour. Off-site and local backup frequency is daily by default and may be customized to meet Internet bandwidth limitations. Off-site backup frequency is ultimately dependent on total data size, data changes, and available Internet bandwidth.
        - Performance may be affected if Veeam SAN integration is not enabled
    - On-demand Backups: Secure Data can perform an on-demand backup at customer request. Each On-demand request for a Server will be subject to fees based on Secure Data T/M rates, outlined in the agreement. Such rates may vary dependent on Customer request or on technical requirements. Customer will define the retention time for the on-demand backup. Customer will be subject to usage billing at contracted rate for on-demand backup data as long as such data is retained on the Secure Data platform.
    - Daily backup checks Daily backup checks will be performed by Secure Data during normal business days (M-F, 8am – 5pm) or as outlined in the Services Agreement. Daily backup checks consist of reviewing internal monitoring and alerting of jobs and addressing anything in a warning or error state.
        - Errors in backup jobs will have a ticket opened proactively with customer to alert issues are being researched and resolved
            - Once errors have been resolved, backup jobs will be re-run with approval from the customer to ensure there is no impact to production performance
    - Backup jobs will be set to re-run 3 times by default before a failure is reported

        - Backup jobs can fail for various reasons including connectivity issues. Jobs that fail due to connectivity issues may not be subject to SLA terms.
    - Warnings in the backup jobs will be reviewed by engineers and tickets will be opened if action is needed to prevent future issues/job failures
    - Reporting/Ticketing
        - Daily backup reports will be sent to email addresses as specified by the customer in the Secure Data backup onboarding form(s)
            - A Distribution list may be provided if multiple people need to be notified
        - Support tickets will be opened with the technical contact as needed

D. SecureBackup Comprehensive Plan

- VeeamOne will be provided with Protected VMs and Backup Infrastructure audit reporting as part of Quarterly Business Reviews
- Secure Restores will be included with AV scanning before files/folders are restored to customer environments
- SAN snapshot integration will be setup at customer request for Veeam supported/integrated SAN manufacturers

13. Secure365

Secure Data's Secure365 products provide options to protect and secure your Microsoft/Office365 environment. From the basic must-have of backup to securing your environment with Advanced Threat Protection and Phishing prevention. Secure Data can remediate issues when they occur along with providing Moves, Adds, Changes, and Deletes of users within your Microsoft 365 tenant. We have options to help migrate your email to the cloud and educate users with Phishing training to provide complete email protection!

A. Secure365 - All Plans

- **Ownership of the Data:** The Microsoft/Office365 backup data being stored remains the sole property of the customer. You, “the customer” warrant that You are the owner or legal custodian of data transmitted to Cloud Storage pursuant to the terms of this Agreement and that You have full authority to transmit said data and direct its disposition in accordance with the terms of this Agreement.
- **Billing:** Billing automatically updates monthly as users are added to the system and aligns with Microsoft licensing practices/requirements for users within Microsoft 365. Shared resources will not be counted assuming they are not counted as a user by the Microsoft license agreement. Customer may not drop below originally contracted user count.
- **Support Hours:** Secure Data’s support hours are Mon-Fri 8:00am – 5:00pm (CT). Support requests outside of these hours will constitute a billable event.
- **Software:** Secure Data will provide Backup and email security software as part of the Secure365 offerings. Microsoft 365 licensing may be provided as an optional add-on to Secure365 service or customer may bring their current licensing

Secure365 Essentials Plan

- **Secure Cloud Backup:** Unlimited storage and retention for Microsoft/Office365 with the following items protected:
    - Exchange
        - Email messages, attachments, and the complete folder structure of each user's mailbox
    - OneDrive
        - All files under the Documents Library, including the entire folder structure
    - SharePoint
        - Item-level SharePoint Online protection
    - Teams
        - Mail, calendar, and site data, along with file data shared within Teams that includes the Group membership associated with Teams
- **Fully Managed Solution:** Secure Data experts provide restores with flexible full and granular recovery options listed by product below:
    - Exchange

        - Messages, folders, or entire mailboxes to the original account or export via the download feature
    - OneDrive
        - Files, folders, or entire accounts can be restored to the original account, a different account, or exported via the download
    - SharePoint
        - Full sites down to items can be restored directly into SharePoint Online from backup
    - Teams
        - Full Team sites down to items can be restored directly into Teams from backup
    - Restore only customer access will be provided to the customer tenant if requested
- **Data Security:**
    - User data is encrypted in transit (TLS) and at rest using industry standard AES 256-bit encryption
    - Retains three copies of backed up data
    - Cloud storage is SSAE Type II Certified
- **Backup Jobs:**
    - Retention cannot currently be changed from unlimited, and all data will be kept forever
        - Retention options are planned for a future release
    - Backups will be run at various points during the day and cannot be specified as to when the jobs will run
        - On-demand Backups: Secure Data can perform an on-demand backup at customer request
- **Daily Backup Checks:** Performed by Secure Data during normal business days (M-F, 8am – 5pm) or as outlined in the Services Agreement. Daily backup checks consist of reviewing internal monitoring and alerting of jobs and addressing anything in a warning or error state
    - Errors in backup jobs will have a ticket(s) opened proactively with customer with information on issues being researched and resolved
    - Once errors have been resolved, backup jobs will be re-run as there is no impact to production performance for 365 backups
    - Warnings in the backup jobs will be reviewed by engineers and tickets will be opened if action is needed to prevent future issues/job failures
- **Reporting/Ticketing**
    - Daily backup reports will be sent to email addresses as specified by the customer in the Secure Data Secure365 onboarding form(s)
        - A Distribution list may be provided if multiple people need to be notified
        - Support tickets will be opened with the technical contact as needed
    - Full ticket visibility available via the Secure Data customer portal
        - ConnectWise portal
        - Can view/update tickets and history

C. Secure365 Enhanced Plan - **Includes everything from Essentials plus:**

- **Secure Cloud Archiving:** Retain email with granular retention policies ensuring that original data is kept for as long as needed without risk of amendment or deletion.
    - Indexed archive provides multilevel search and tagging capabilities, for support of complex audit and discovery exercises
    - Data can be preserved on legal hold for as long as needed, and exported when required for analysis or disclosure
    - Archiving covers: Email messages, calendars, tasks, contacts, notes and public folders
    - Unlimited Storage and retention
    - Customer access to archives provided via Role Based Access Controls/permissions
- **Data Security:**
    - User data is encrypted in transit (TLS) and at rest using industry standard AES 256-bit encryption
    - Data stored in a dedicated and secure immutable store outside of the production environment
- **Email Continuity:**
    - Ability to failover to cloud-based email service in the event Microsoft 365 experiences and outage
    - Up to 96 hours of failover
    - Provides emergency mailbox to send and receive email via login to cloud portal
- **Email Security:**
    - Fully managed cloud-based protection against spam, malware, and viruses
    - Advanced Threat Protection (ATP) utilizing a full system emulation sandbox
    - Agentless email encryption provided via subject key word(s)

        - Link and typosquatting protection
    - **Microsoft 365 Administrative Changes:**
        - Moves, Adds, Changes, and Deletes (MACDs) of users within Microsoft 365 portal
            - Up to 5 MACD's per month included
                - Additional MACD's may be charged as a billable event
            - Must ensure Secure Data is listed as Partner of Record (POR)
    - **Customer Access:**
        - Help Desk role which allows admins to deliver messages, view message headers, view all domain settings and users for the assigned domains will be provided to the customer tenant if requested

D. Secure365 Comprehensive Plan - **Includes everything from Enhanced plus:**

- **API Based Inbox Defense:**
    - Artificial Intelligence that detects and stops email attacks
    - Helps prevent spear-phishing, business email compromise, and extortion attacks
    - Automatic message quarantine
        - Alerts provided to end users and administrators with details on why message was quarantined
- **Account Takeover Protection:**
    - Detects and alerts account takeover activity
    - Notifies users and deletes compromised emails
    - Blocks attackers' access to compromised accounts
    - Provides visibility into rule changes and suspicious sign-ins
- **Incident Response:**
    - Outlook Add-in and one-click threat reporting
    - Threat Hunting
    - Ability to review users who interacted with malicious emails
    - Blocking of future emails from specific regions
    - Deletion of emails directly from user inboxes
    - Alerts sent to impacted users

E. Secure365 Exclusions

- **DNS Management:** Secure Data will provide guidance on required changes to records, but customer is responsible for managing DNS records with registrar
- **365 Management:** Any management outside of MACD's noted above are exclude from Secure365 service

14. SecureReplica

SecureReplica is a Secure Data offering that allows us to help customers with their disaster recovery needs. We have the flexibility to provide the basics with a secure off-site Cloud Connect Replication repository powered by our, all the way to a fully managed disaster recovery solution where you turn your disaster recovery hassles over to us!

With our Enhanced and Comprehensive plans, Secure Data's Managed Services team supports the underlying hardware and software used to deliver the SecureReplica Service, as well as administers and monitors the replication and recovery processes put in place. Customers receive a daily report detailing the status of replication jobs, completion of jobs, and any other information about the jobs. Customers open support requests to create or alter replication jobs, change data retention policies, or get additional information about the service.

SecureReplica decreases RTOs allowing customers to recover quickly when disaster strikes and get back to normal operations preventing loss of revenue.

****Note: SecureBackup Enhanced or Comprehensive is a pre-requisite for SecureReplica Enhanced and Comprehensive*

A. SecureReplica - All Plans

- **Ownership of the Data**: The replicated data being stored on the Hardware and at the Data Center remains the sole property of the customer. If the customer chooses to terminate services, Secure Data will assist customer in the orderly termination of services. The customer agrees to pay Secure Data the actual costs of rendering such assistance. You warrant that You are the owner or legal custodian of the data transmitted to

Cloud Storage pursuant to the terms of this Agreement and that You have full authority to transmit said data and direct its disposition in accordance with the terms of this Agreement.

- **Data Security**: All data is fully encrypted during transmit off-site and while stored off-site using:
    - Files encrypted with 256-bit AES
    - Transmittal to off-site remote servers using SSL (Secure Socket Layers) technology
    - Data stored off-site remains encrypted at all times
- **Support Hours**: Support hours are Mon-Fri 8:00am – 5:00pm (CT). Simple file or directory restoration up to a single VM restore is covered under this agreement. Restoration outside of these hours will constitute a billable event.
    - Major incident recovery services: Major incident recovery services such as recovery services after a complete server hardware failure, a failure resulting from third party vendors updating a system, a failure caused by force majeure, theft, vandalism, etc., are not covered under this agreement and will constitute a billable event, both to recover the data from offsite as well as to restore any services.
    - Customer will bear responsibility for getting server and applications up and running. Remote support can be provided at T&M rates.
    - Data contained within a replication job that has expired or has exceeded defined retention cannot be recovered.
- **Service Conditions**: Customer acknowledges that certain conditions outside of Secure Data's control may adversely impact the ability of Secure Data to perform successful backups or restores of Image. Examples of such conditions are listed below:
    - Customer task, software, scheduled job or other human intervention intentional or otherwise renders portions, complete files, or complete file systems unavailable to Service.
    - Failure of customer software, operating system, Agent or Service
    - Network connectivity issues between customer server and cloud including but not limited to packet loss, lack of sufficient network capacity to support required replication bandwidth
    - Replication job in seeding status
- Customer acknowledges that in the event of a support issue, customer is responsible for on-site cooperative testing with Secure Data support to assist in the diagnosis of the issue
- Customer does not have access to the hypervisor, meaning no VMware vCenter access
    - Applications such as Virtual Desktops will not be able to be replicated without vCenter access
    - **Compatibility**: Secure Data controls the version of hardware and software running on its infrastructure and does not guarantee that it is compatible with any version changes made by the customer on their network, server, OS, or application infrastructure. It is the Customer's responsibility to ensure that any version changes planned on their infrastructure is compatible with Secure Data equipment and software, including cloud services.
        - VMware only supported for replication
- **Maintenance**
    - **Scheduled Maintenance:** In order to maintain performance, Secure Data performs Scheduled Maintenance within its published maintenance windows. This may require that specific Services be suspended during the maintenance period. Loss of Service Availability due to Scheduled Maintenance is not deducted in calculating Service Availability. Secure Data will use commercially reasonable efforts to notify customer in advance of any Scheduled Maintenance that may adversely affect customer's use of the Services.
    - **Emergency Maintenance:** Secure Data may need to perform emergency maintenance, including security patch installation and hardware replacement. Secure Data will not be able to provide customer with advance notice of emergency maintenance. Loss of Service Availability due to emergency maintenance is not deducted in calculating Service Availability.
- **Connectivity:** Client SSL VPN will be established for connectivity to DR site in the cloud via a virtual NSX firewall
    - Additional connectivity options available for additional fee:
        - Site to site VPN
        - Direct connectivity to data center
        - Extension of MPLS into data center
        - Physically collocated firewall in data center

- Public IP addresses can be provided for an additional monthly fee

- **Customer Responsibilities**
  - Designating a technical point of contact to work with Secure Data for a successful implementation and ongoing support
    - Cooperating in scheduling installations as required by Secure Data personnel
  - Providing Secure Data with all required infrastructure and system information to successfully complete the implementation
  - Authorizing any and all modifications, updates, additions/deletions, etc. to the SecureBackup/Replica services through a support ticket submitted by an authorized contact
  - IT support and troubleshooting on customer owned servers
    - Customer may request assistance from Secure Data which will be billable
  - Configuration, management, maintenance, and support of any equipment not provided by Secure Data for use with the SecureBackup/Replica services
  - The performance of its applications across the network
  - Requesting restores through a support ticket submitted via email/phone
  - Reviewing service status report(s) for completeness and accuracy
  - Notifying Secure Data, through a support ticket, of any critical changes in the non-managed customer environment that may impact the services provided
  - Provide the appropriate skills and knowledge required to recover, support, and maintain the business applications being recovered in the DR environment
  - Be responsible for all configurations of any third-party software according to third party vendor specifications
  - Resolving incompatibilities between Client infrastructure and the backup software
  - DNS changes to re-route traffic to the cloud during a DR event
- **Fees**
  - Disaster fees will be charged on a per hourly basis on a per CPU, per GB of RAM basis at current hourly rates
  - Rates are charged when DR servers are spun up either from a DR test or full DR event

B. SecureReplica Essentials Plan

- **Cloud**: Secure cloud repository will be provided in a Tier 3 data center via Secure Data's partnerships.
  - Veeam Cloud Connect Replication will be utilized to send replications to the cloud data center
  - Storage will be provided in 1TB increments
    - 1TB = 1000GB
  - Once a customer's cloud replication repository hits 90%, it will trigger an increase to the next 1TB to ensure replications continue to run successfully
    - Update will be reflected in the customer's next monthly billing cycle
  - All ingress/egress fees are included with the monthly fees
  - Project management provided to ensure timely onboarding
  - Data seeding will be done utilizing customer WAN connection unless requested
    - Additional one-time fee will be assessed to cover USB drive, shipping, and engineering time (Fee TBD per seeding request)
  - Customer is responsible for procuring and maintaining all required software/ hardware, other equipment, all Internet, communication, and other services necessary to access and use the services
    - All hardware/software must meet vendor minimum requirements
  - Customer is responsible for implementing a high-quality uplink to the Internet to ensure the availability of the services

C. SecureReplica Enhanced Plan

****Note: SecureBackup Enhanced or Comprehensive is a pre-requisite for SecureReplica Enhanced and Comprehensive*

- **Disaster Declaration:** A disaster may be declared only by placing a phone call to Secure Data to enact the plan within the DR Playbook
    - A disaster may be declared only by authorized contacts listed within in DR Playbook
    - Customer may change the authorized contacts by submitting a support ticket via email/phone to Secure Data
    - Customers access their VMs through remote access, protected by a VPN
    - It's recommended that remote access be enabled on the protected VMs locally at the customer site prior to replication
- **DR Playbook:** A disaster recovery playbook will be provided for both Secure Data and the customer to follow in the event of a disaster and/or failover testing. The playbook will consist of:
    - Customer authorized contacts and role within the customer's environment
        - Systems Lead
        - Network Lead
        - Application Lead
    - Customer call tree
    - Secure Data contact information
    - Disaster definition(s)
    - VM Boot order
        - Server names
        - IP addresses
        - Resources (CPU/RAM)
        - Application information
        - Software dependencies
            - Example: Domain Controller with SMO roles, then Database Server, then Application and/or Web Server
    - Prerequisite steps during setup
    - Failover process – Steps needed for bringing up the DR environment in the cloud
    - Failback process – Process for failing the environment back over once service has been restored to the original location
        - Reverse replication or re-seeding are available options
    - Testing procedures – Detailed steps on testing the plan
- **DR testing:** Two types of testing exist; Planned failover and Live failover
    - Planned Failover - A planned failover test is a safe, non-disruptive option that will bring up the VMs that have been replicated to your DR environment and allow you to do testing without impacting anything in your production environment. Once the test ends, the VMs are removed-This is what comes with our Enhanced and Comprehensive plans – One Planned Failover will be provided per year and must be scheduled by the customer 30 days in advance
    - Live Failover - This is designed to simulate a full disaster. A live failover will assume that your production environment is down, and the VMs being failed over are now supposed to be the primary systems. Once you have failed over, replication stops coming from your production site, since the original environment would be destroyed or inaccessible due to the disaster (during such a test, often replication is reversed, therefore, storing changes back in your on-premises environment as if it were the DR target). This is clearly a more extreme type of testing, but it isn't uncommon among companies who want complete assurance that their DR plan will work-This would be charged for at T/M rates for customers that want to "pull the plug"
- **Replication Jobs:**
    - Troubleshooting of the software will be provided as part of the SecureReplica managed service
    - Retention policies can be customized to create as many restore points as needed
        - Default replication occurs daily with the initial full and 2 daily incremental snapshots
        - Customer may request additional restore points as needed, additional fees will apply based on storage consumed

        - Replication Frequency: VMs can be replicated as frequently as every hour. Replication frequency is daily by default and may be customized to meet Internet bandwidth limitations. Replication frequency is ultimately dependent on total data size, data changes, and available Internet bandwidth.
- On-demand Replications: Secure Data can perform an on-demand replication at customer request. Each On-demand request for a VM will be subject to fees based on Secure Data T/M rates, outlined in the agreement. Such rates may vary dependent on Customer request or on technical requirements. Customer will define the retention time for the on-demand replications. Customer will be subject to usage billing at contracted rate for on-demand replication data as long as such data is retained on the Secure Data platform.
- Daily checks will be performed by Secure Data Managed Services engineers during normal business days according to the standard support hours as defined by the agreement.
    - Daily checks consist of reviewing internal monitoring and alerting of jobs and addressing anything in a warning or error state
        - Errors in jobs will have a ticket opened proactively with customer to alert issues are being researched and resolved
            - Once errors have been resolved, jobs will be re-run with approval from the customer to ensure there is no impact to production performance
    - Replication jobs will be set to re-run 3 times by default before a failure is reported
        - Jobs can fail for various reasons including connectivity issues. Jobs that fail due to connectivity issues may not be subject to SLA terms.
    - Warnings in the jobs will be reviewed by engineers and tickets will be opened if action is needed to prevent future issues/job failures
- Reporting/Ticketing
    - Daily reports will be sent to email addresses as specified by the customer in the Secure Data onboarding form(s)
        - A Distribution list may be provided if multiple people need to be notified
    - Support tickets will be opened with the technical contact as needed

D. SecureReplica Comprehensive Plan

- All features of the Enhanced SecureReplica plan are included in the Comprehensive plan with the addition of Zerto replication
    - Zerto replication allows for CDP (Continuous Data Protection) and provides shorter RPOs and RTOs
- A combination of Enhanced and Comprehensive may be selected for your environment based upon the RPO/RTO requirements
    - Prioritization of tier 1 applications with the shortest RTOs will be replicated with Zerto while tier 2 applications will utilize Veeam replication

15. SecurePhish

Secure Data's solution for Security Awareness Training and Simulated Phishing Attacks is an all-encompassing managed solution. SecurePhish utilizes the world's largest integrated platform for security awareness training combined with simulated phishing attacks that help train your users what to look for and helps protect your organization against external threats.

A. SecurePhish Comprehensive Plan

- Training
    - Award-winning, on-demand, engaging interactive browser-based training
    - The world's largest library of well over 1300 security awareness training content items
    - AI-Recommended training offers informed training suggestions based on the simulated phishing test results
    - Brandable content
    - Hints & Tips Security Awareness emails for compliance
    - Visible training results: percentage for whole organization graphed over time in your console for reporting

        - Enhanced training campaigns
    - Phishing
        - AI-Driven Phishing Feature helps deliver a personalized simulated phishing experience to every user
        - Industry Benchmarking Feature to compare your organization with other same-size organizations
        - Year-round all-you-can-eat simulated phishing attacks
        - Unlimited yearly use of all phishing templates
        - Pre-made regular “Current Events” templates you can send to users
        - Set-it-and-forget-it schedules of phishing campaigns
        - Full Library with 15,000+ successful phishing templates
        - Customizable phishing attacks
    - Reporting
        - Advanced reporting provides metrics and insights into the effectiveness of your security awareness training
        - Use each employee’s behavior and user attributes to tailor phishing campaigns, training assignments, remedial learning and reporting
        - Training reports for all users or a specific group (started, completed, never finished)
        - Individual user report cards with their open and click history
        - Reports on browser/device used to open a phishing email and vulnerable browser plugins the user has installed
        - Top 50 clickers report
        - Print to PDF so reports can be sent to management
        - Personal timeline overview for every individual user

16. SecureDesk

SecureDesk is our solution to providing the first line of support that your employees work with when they have IT questions or need assistance. Secure Data has an extensive team of Level One support engineers available at multiple tiers for end user and workstation support.

A. SecureDesk Essentials Plan

- Remote troubleshooting and remediation for end users
- 8 AM to 5 PM CST Monday through Friday
- Ticketing system
- Phone and email to open tickets
- Open, work, route, and manage various types of tickets for fast resolution
- RMM Tool - Remote agent installation
- Firewall rules need to be adjusted to allow
- End User Support – Problem and Incident Management
- Password resets
- Microsoft Office issue support
- AD local user account support
- End User Account Creation and Deletes
- User Setup by department
- Windows PC Workstation Support
- Operating System (OS) Troubleshooting and configuration
- Antivirus Support
- Microsoft support and support escalations
- Active Directory local user account support
- Local and networked printer and copier support

- Printer and copier support escalations
- Endpoint Security
- Mobile Device Support – Tablets Only – Does not include Mobile Phone Support
- Support for MS Outlook email application
- Current OS and supported device
- Certain Conditions Apply
- 3rd Party Application Escalation Support
- Open ticket with 3rd party and provide status updates
- Remote Desktop Support - VPN Support

B. SecureDesk Enhanced Plan
- Everything included in Essentials plus:
- Remote troubleshooting and remediation for end users
  - 24x5 CST Monday through Friday (Monday 12:00 AM CST to Friday 11:59 PM CST)
  - Excluding holidays defined in Secure Data Terms & Conditions Holiday schedule

C. SecureDesk Comprehensive Plan
- Everything included in Essentials and Enhanced plus:
- Remote troubleshooting and remediation for end users
  - 24x7x365
  - Holidays Included
- Dedicated Support Line for customer organization

D. Exclusions to SecureDesk service
- End user devices are not monitored
- Mobile Phone Support
- Linux and Unix
- Home office equipment
- Home networking issues

E. SecureDesk requirements
- End user devices must be under current manufacturer support
- Manufacturer Supported Versions only
- End user devices must have Antivirus software deployed and maintained

17. SecureDesk Service Priority Levels

	Incident Definition	Service Level Agreements	Getting Help
Priority 1 (P1) Critical	Issues impacting business operations and affecting ALL users with no immediate workarounds. Examples: - Complete point of sale environment down - Company-wide email issues - Immediate Account Termination	Secure Data Technologies will: - Respond to P1 calls based on selected plan (essentials, enhanced, comprehensive) - Call Customer contact within 60 minutes - Secure Data Technologies and the customer will commit necessary resources to resolve the situation - Resolution time cannot be guaranteed	Priority 1 incidents are required to be phoned into our help line: 618-726-4040. We monitor the help line 24x7x365 and will respond within 60 minutes. Priority 1 issues should NOT be reported by email or through our portal.

Priority 2 (P2) High	The operation of an existing device or service is impaired, but most business functions remain operational. Examples: - Device failure/unresponsive - Drive capacity full - Issues affecting multiple users	Secure Data Technologies will: - Respond to P2 calls based on selected plan (essentials, enhanced, comprehensive) - Call Customer contact within 2 hours - Secure Data Technologies and the customer will commit necessary resources full time during normal business hours to resolve the situation - Resolution time cannot be guaranteed	Priority 2 incidents can be called in (618-726-4040) or sent in via email (helpdesk@securedatatech.com) or portal. We will respond within two hours during normal business hours.
Priority 3 (P3) Standard	Operation of a service or device is not optimal or a move, add or change has been requested. Overall functionality is intact. Impact and severity are normal. Examples: - Computer peripherals not working - Single user or small branch issue - Password reset - Account Creation/Termination	Secure Data Technologies will: - Respond to P3 calls based on selected plan (essentials, enhanced, comprehensive) - Contact Customer within 3 hours through the ticketing system - Secure Data Technologies and customer will commit resources during normal business hours to resolve the issue - Resolution time cannot be guaranteed	Priority 3 incidents can be called in (618-726-4040) or sent in via email (helpdesk@securedatatech.com) or portal. We will respond within 3 hours during normal business hours.
Priority 4 (P4) Low	The issue is an inconvenience or annoyance but there are clear workarounds or alternatitives. Limited to a single user. Informational or procedure changes. Examples: - Email connectivity issues - Company approved application installation	Secure Data Technologies will: - Respond to P4 calls based on selected plan (essentials, enhanced, comprehensive) - Contact Customer within 4 hours through the ticketing system - Secure Data Technologies and customer will commit resources during normal business hours to resolve the issue - Resolution time cannot be guaranteed	Priority 4 incidents can be called in (618-726-4040) or sent in via email (helpdesk@securedatatech.com) or portal. We will respond within 4 hours during normal business hours.

18. SecureDesk VIP Service Priority Levels

	Incident Definition	Service Level Agreements	Getting Help
Priority 1 (P1) VIP	Users designated on the VIP list have an issue preventin them from performing daily task, work, or other business operations.	Secure Data Technologies will: - Respond to P1 calls based on selected plan (essentials, enhanced, comprehensive) - Reply to VIP tickets and emails within 30 minutes - Secure Data Technologies and the customer will commit necessary resources to resolve the situation - Resolution times cannot be guaranteed	P1 VIP incidents must be called in to our helpline: 618-726-4040. Response to VIP will occur within 30 minutes. VIP will need to be on the approved list and provide full name as well a description of the issue.

*Additional charges may apply

**Changes to VIP list will go in effect 5 business days after request

19. SecureAssist Engineering-as-a-Service

Engineering-as-a-Service (EaaS) is designed to integrate Secure Data's talent into the Customer's team by providing a suite of expertise at the Customer's fingertips with consistent communication and resource management. EaaS provides exclusive access to a suite of highly focused and certified talent.

Where applicable, EaaS will be priced according to the Ordering Document and may be consumed as needed over the Service Contract term, unless otherwise agreed in writing.

20. Customer Responsibilities

- Customer agrees to provide remote network access, connectivity, and privileges.
- Customer will provide a virtual machine (VM) configured as follows: Windows Server Version that does not exceed the Microsoft “extended Support End Date”; 2 CPU Cores; 8GM RAM; 80GB Hard Drive Space with Full Admin Rights.
- Customer will provide full administrative-level account access privileges to Secure Data for use while supporting the environment.
- Customer agrees to provide the following information on monitored devices:
- Device Model, Device IP, Username/Password, Virtual Environment Access Credentials and Escalation Path
- Customer will provide access to monitoring tools and reports in order to complete any assessment work.
- Customer will provide a site contact that we will work with to schedule work and answer questions in order to resolve issues.
- Onsite services are not covered. For example, a hardware failure will require an onsite resource to rebuild the OS or install new hardware.
- Network issues isolated to the circuit will be opened with the carrier. In some cases, Secure Data will not have access to open these tickets. In these cases, the customer will be responsible for this effort.
- This service is best effort, meaning we cannot guarantee services will be restored within a specific amount of time.
- Secure Data cannot be held liable for data loss of any kind.
- Customer will notify Secure Data of any major deployment and or infrastructure change that could cause major network issues.
- Customer will maintain support agreements for all hardware. If agreement does not exist hardware replacement time will vary depending on availability and will limit Secure Data’ capability to support the aforementioned hardware.
- Customer will maintain software agreements for all systems and business applications.

21. Billing Based on Actual Services Provided

Adding, Removing, and Modifying Services

From time to time, Customer may request that Secure Data add or remove services (such as devices, data, or users), from the Service Contract, and/or modify the service level provided (such as essentials, enhanced, and comprehensive). These adjustments may be requested in writing to Secure Data, with the primary method of communication being through a Service Ticket.

Each month, Secure Data will adjust the Services Contract billing based on the actual quantity of devices, data, and/or users for which services were provided, and based on the level of service provided, and will bill Customer based on the prices included in the signed Ordering Document.

Minimum Commitment

Customer agrees to a minimum commitment of eighty percent (80%) of the monthly contract amount included in the signed Ordering Document. If, as a result of adding, removing, and/or modifying services during the contract term, the monthly billing would drop below eighty percent of the monthly contract amount included in the signed Ordering Document, Secure Data will bill Customer for eighty percent of the monthly contract amount. Exclusions to minimum commitment are Secure365 and any storage resources within SecureBackup, as these items cannot decrease during the contracted term.

22. Modification or Termination of Service Contract

Secure Data reserves the right to renegotiate rates based on additions of locations, hardware, software, hardware support requirements, service adjustments, service enhancements, as well as modify this Service Contract (or any portion thereof) with a thirty (30) day notice.
Customer may request, in writing to Secure Data, modifications to this agreement (or any portion thereof). Secure Data will implement any reasonable requested modifications within 30 days of receiving such written request from the Client.

This Service Contract may be terminated by the Customer upon sixty (60) day’s written notice if Secure Data:

- Fails to fulfill in any material respect its obligations under this Service Contract and does not cure such failure within sixty (60) days of receipt of such written notice.
- Breaches any material term or condition of this Service Contract and fails to remedy such breach within sixty (60) days of receipt of such written notice.
- Terminates or suspends its business operations unless it is succeeded by a permitted assignee under this Service Contract.

If either party terminates this Service Contract, Secure Data will assist Customer in the orderly termination of services, including timely transfer of services to another designated provider. Customer agrees to pay Secure Data the actual costs of providing such assistance.

If Customer terminates this Service Contract for any reason other than those included above, Customer agrees to pay Secure Data the Minimum Commitment amount through the end of the current contract term.

23. Monthly Charges, Fees, and Payment

Customer is purchasing Secure Data's Services under this Agreement for the charges and fees outlined in the Ordering Document(s). Onboarding fees, if applicable, will be invoiced upon execution of the Ordering Document. Thereafter, monthly charges and fees shall be invoiced by Secure Data and paid in monthly installments by the Client, with the first installment to be invoiced on the first day of the month following the execution of the Ordering Document. Each payment thereafter shall be invoiced on the first day of each calendar month, with payment due within 30 days of the invoice date. Any additional charges will be invoiced in combination with the next month's invoice, unless otherwise specified by Secure Data.

Services shall be charged against the Customer in accordance with these Conditions.

Customer will pay any and all legitimate and/or agreed upon service fees and charges due upon receipt of the relevant invoice from the Secure Data.
The Customer will, in addition to the other amounts payable under this Service Contract, pay all sales and other taxes, federal, state, or otherwise, however designated, which are levied or imposed by reason of the services provided pursuant to this Services Contract. Without limiting the foregoing, Customer will promptly pay to Secure Data an amount equal to any such taxes actually paid or required to be collected or paid by Secure Data.

When a payment under these Conditions is not on a business day (Monday to Friday), it may be paid on the next following business day.
Excluding any relevant taxes or fees withheld by law, any and all sums due under this Service Contract shall be paid in full without any set-off, counterclaim, deduction, or withholding.

Secure Data reserves the right to refuse, suspend, or even terminate service under this Service Contract in the event the Customer has failed to pay any invoice within thirty (30) days of said invoice date, whether it be an invoice for services provided under this Service Contract or any other agreement between Secure Data and Customer.

Service(s) fees are subject to change at any time. Secure Data will promptly notify Client of any such changes in pricing. Pricing changes may be required based on fees paid for by Secure Data to OEM's, Vendors, Software Rights and other such necessary items in pursuit of providing services outlined within scopes of services.

24. Out of Scope Fees

It is understood and agreed upon that any and all Services requested by the Customer that fall outside the terms of this Services Contract will be considered Service Tickets and will be billed as separate, individual Services at Secure Data's standard billing rate.

25. Terms of Service

This Service Contract shall be governed by the laws of the State of Missouri.

The parties hereto expressly assume an obligation to act in good faith toward one another in the performance of their obligations under this Service Contract. Secure Data is not responsible for failure to render services due to circumstances beyond its control including, but not limited to, acts of God.

Customer agrees that during the term of this Service Contract and for a period of one year following the termination of this Service Contract, the Customer will not recruit or hire any employee, agent, representative or subcontractor of Secure Data, nor will the Customer directly or indirectly contact or communicate with Secure Data's personnel for the purpose of soliciting or inducing such personnel (a) to accept employment with, or perform work for any person, firm, or entity other than Secure Data; or (b) to provide services to the Customer or any other person, firm or entity except as an employee or representative of the Customer. The Customer agrees that, in the event of a breach or threatened breach of this provision, in addition to any remedies at law, Secure Data, without posting any bond, shall be entitled to obtain equitable relief in the form of specific performance, a temporary restraining order, a temporary or permanent injunction or any other equitable remedy which may then be available.

Services furnished under this Service Contract are provided "as is" and, unless otherwise expressly stated, without representations or warranties of any kind, either express or implied. To the fullest extent permitted by law, Secure Data disclaims all warranties, express, implied, or statutory, including, but not limited to, implied warranties of title, non-infringement, merchantability, and fitness for a particular purpose. Secure Data does not warrant that use of software or products furnished by Secure Data will be uninterrupted, error-free, or secure, that defects will be corrected, or that products or the server(s) to which access is provided are free of viruses or other harmful components.

If any provision in this Service Contract is held by a court of competent jurisdiction to be invalid, void, or unenforceable, the remaining provisions shall nevertheless continue in full force without being impaired or invalidated in any way.

26. Limitation on Liability

Secure Data's liability with respect to any claim of any kind, including, but not limited to, claims asserting negligence or breach of warranty, resulting from, arising out of, or connected with this Service Contract, the performance or breach thereof, or the manufacture, sale, delivery, resale, repair or use of any Products or Services covered by or furnished under this Services Contract shall in no event exceed an amount equal to the gross compensation received by Secure Data under this Services Contract, and in no event shall such liability exceed the liability limit of any insurance policy in place to cover such claim.

Secure Data shall not be liable to Customer or any third party for any loss of profit or revenues, interruption of business, cost of capital, cost of cover, downtime costs, increased operation costs, claims of Customer's customers for such damages, or for any special, consequential, incidental, indirect, punitive, or exemplary damages. Secure Data shall not be liable to Customer or any third party for any losses, claims, liabilities, actions, judgments, damages, or expenses that are cause in whole or in part by acts or omissions, negligent or intentional, of Customer or any third party or their respective agents or employees.