Effective July 17, 2024. These Service Descriptions supersede and replace all prior versions.

Schedule of Services

MANAGED SERVICES

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a new Order including those Services.

ACTSCARE ENCOMPASS	**Prebuilt packages containing various solutions listed below. List is provided in the Order.**	
ACTSCARE ELEVATE	**Prebuilt packages containing various solutions listed below. List is provided in the Order.**	
ACTSCARE ESSENTIALS	**Prebuilt packages containing various solutions listed below. List is provided in the Order.**	
ACTS360 TBR	**Client is asked to participate in a quarterly review of ACTS360 and Client performance. Used to align and grow. Includes a variety of topics that vary**	
Acts 360 Onsite Helpdesk Support	Assigned End User	Onsite end user support during regular business hours. M-F 8-5 excluding federal holidays
Acts 360 Vendor Support	Assigned End User	Remote end user support during regular business hours. M-F 8-5 excluding federal holidays

Acts 360 Remote Helpdesk Support	Assigned End User	Remote end user support during regular business hours. M-F 8-5 excluding federal holidays
Acts 360 VCIO Quarterly Services	Included as an option to client	Advanced Cyber and Security services designed to deepen an organization's ability to respond and weather cyber and security incidents.
Privileged Access Management	Per system managed with the ACTS360 installed agent	On Demand event triggered by UAC events, software automates checking for known threats and ACTS360 or authorized point of contact can approve install.
3rd Party Email Backup	Per assigned Office 365 account, specifically SharePoint, OneDrive, Teams and Exchange	Daily backups of Office 365 content to a 3rd party provider. Default data retention is a rolling 1 year, optional up to 7 years.
Dark Web Monitoring and Alerting	Client owned domains	Client monitoring of domain-based email password breaches with notifications to end users on detected activity.
Basic Multi Factor Authentication	Per assigned user access to the application for verifying identity.	Remote end user support during regular business hours. M-F 8-5 excluding federal holidays
Email Threat Test	Assigned premium user and optional customer selected e-mail addresses	ThreatTest Automated Phishing Email Incident Response Service GoSecure delivers the most accurate threat intelligence with our unique hybrid approach that combines automated machine learning and human analysis to investigate and respond to phishing attacks in real-time. Triggered by end user.

© Scott & Scott, LLP

Mailbox Spam Filtering	Assigned End User and optional customer selected e-mail addresses	Rules are configured and updated based on standardized policies and best practices. Any suspicious activities are logged and will generate automatic alerts for remediation.
Enterprise Password Management	Per assigned user access to application for managing passwords and credentials.	Use of 3rd party application to install on computing devices and mobile devices for securing and accessing credentials.
Remote Monitoring Agent	Per system managed with the ACTS360 installed agent	Automated monitoring and alerting for system warnings and errors. Tickets are automatically generated and addressed based on severity.
Hosted Print Management	Assigned End User	Printix Cloud Print Management Service is a cloud-based multi-tenant subscription service especially designed and structured to provide a complete cloud-managed print infrastructure and secure printing environment, that guarantees efficiency, productivity and cost savings. No on-premise servers and databases are required. It runs with Printix Client software installed on users' computers (Windows and Mac). End user printer support during regular business hours. M-F 8-5 excluding federal holidays
Managed Detection and Response	Per system managed with the ACTS360 installed agent	The endpoint is where adversaries exploit, gain and maintain access, move laterally, and more. Identifies and detects these threats in real time so you can stop attackers before they do any damage Rules are configured and updated based on standardized policies and best practices. Any suspicious

© Scott & Scott, LLP

		activities are logged and will generate automatic alerts for remediation.
Next Generation AV	Per system managed with the ACTS360 installed agent	NGAV examines what's occurring on the endpoint to identify the symptoms of malicious behavior instead of just identifying known malware signatures. NGAV leverages ML, AI, and behavioral analytics to quickly and accurately identify known and unknown malware. Rules are configured and updated based on standardized policies and best practices. Any suspicious activities are logged and will generate automatic alerts for remediation.
Secure Access Service Edge	Assigned Client Device	Provides a secure connection from endpoint to nearest server. Is used to route data encrypted and is used to process items such as Web Content filtering, DNS requests, among other internet protocols. Rules are configured and updated based on standardized policies and best practices. Any suspicious activities are logged and will generate automatic alerts for remediation.

© Scott & Scott, LLP

SIEM & Threat Detection 30 Days	Assigned Client Device	A SIEM performs real-time analysis to detect unusual activity and generates alerts to prompt teams to take appropriate action. With it, businesses can make informed decisions to strengthen their security posture; monitor, alert, and respond to attacks; and detect a wide range of threats. SIEM aggregates data in one centralized pane of administrative glass for IT and security teams to investigate and remediate issues faster. Data is aggregated for a rolling 30 days. Rules are configured and updated based on standardized policies and best practices. Any suspicious activities are logged and will generate automatic alerts for remediation.
Lan Zero Trust	Assigned Client Device	LAN ZeroTrust (LZT) is a unique technology to segment internal networks. Built with a firewall-inspired interface, controlling internal traffic has never been easier. It leverages a deny-by-default design where devices on internal networks can no longer freely communicate without explicit policies. LZT integrates with identity, empowering you to implement multi-factor authentication (MFA) policies where users must authenticate to access sensitive resources on the internal network. Rules are configured and updated based on standardized policies and best practices. Any suspicious activities are logged and will generate automatic alerts for remediation.

© Scott & Scott, LLP

SIEM & Threat Detection 1 Year		A SIEM performs real-time analysis to detect unusual activity and generates alerts to prompt teams to take appropriate action. With it, businesses can make informed decisions to strengthen their security posture; monitor, alert, and respond to attacks; and detect a wide range of threats. SIEM aggregates data in one centralized pane of administrative glass for IT and security teams to investigate and remediate issues faster. Data is aggregated for a rolling 365 days. Rules are configured and updated based on standardized policies and best practices. Any suspicious activities are logged and will generate automatic alerts for remediation.
Acts 360 24x7 Server Support	Per server managed with the ACTS360 installed agent	Automated monitoring and alerting for system warnings and errors. Tickets are automatically generated and addressed based on severity.
Monitoring and Alerting of Existing Wireless Access Point	Assigned Client Owned Wireless Devices	Automated monitoring and alerting for system warnings and errors. Tickets are automatically generated and addressed based on severity.
Monitoring and Alerting of Existing Firewall	Assigned Client Owned Firewall Devices	Automated monitoring and alerting for system warnings and errors. Tickets are automatically generated and addressed based on severity.
Monitoring and Alerting of Existing Non-Backbone Device	Assigned Client Owned Network Devices	Automated monitoring and alerting for system warnings and errors. Tickets are automatically generated and addressed based on severity.

© Scott & Scott, LLP

Monitoring and Alerting of Existing Switch	Assigned Client Owned Switch Devices	Automated monitoring and alerting for system warnings and errors. Tickets are automatically generated and addressed based on severity.
Acts 360 IPad Management	Per system managed with the ACTS360 MDM agent	Remote end user support during regular business hours. M-F 8-5 excluding federal holidays
IPad MDM Management License	Per system managed with the ACTS360 MDM agent	IPAD MDM is a software that allows the installation of MDM Profiles or Payloads on macOS, iOS, and tvOS Devices1. It supports all MDM Configuration types, allowing the ability to import ANY MDM configuration or using the User Interface to create pre-defined payloads1. Addigy MDM software is engineered with auto-remediation measures in place2. It provides enhanced functionality on macOS devices and support for iOS and tvOS Devices
Hardware / Software Rental		ACTS360 will provide for a monthly fee a rental program of hardware or software we provide to customer. ACTS360 retains ownership of all hardware and software in this model.
Local Backup Disaster Recovery Licenses for Servers	Assigned Client Servers	Where possible, specified servers, devices or services will be at 8am and every four hours for 12 hours, and those backups held for 30 days.

© Scott & Scott, LLP

Backup Workstation Licensing with Direct to Cloud	Assigned Client Device	Where possible, specified servers, devices or services will be at 8am and every four hours for 12 hours, and those backups held for 30 days.
Microsoft Licensing	Per Microsoft SKU and quantity requested by client	N/A
Enterprise Multi Factor Authentication	Per assigned user access to the application for verifying identity.	Usage of 3rd party MFA application to provide an app for MFA verification to configured services.
Cloud Services	Local Backup Disaster Recovery Licenses for Servers	Assigned Client Servers
ACTSVoIP Coredial	Assigned VoIP User	Remote end user support during regular business hours. M-F 8-5 excluding federal holidays
ACTSVoIP Coredial	Assigned VoIP User	Includes one professional seat license associated with one device or softphone, one telephone number, E911, CNAM, as well as all standard UC and Hosted PBX features. 500 minutes included with extension. Additional minutes billed separately.

© Scott & Scott, LLP

Assigned Client PBX	ACTS360 managed PBX systems will be backup nightly once between 9pm and 1am; backups are retained for 30 days for relevant systems that replicate offsite. For systems that backup to local media, backups are not replicated and customer should have no expectation of recoverability if local physical access to recovery media is lost. ActsVOIP hosted systems are backed up per vendor standards and are not directly controlled by ACTS360 and customer should have the expectation that ACTS360 will assist in recovery but has no direct control of the backups for these hosted systems.

**Provider does not provide internet connection. Client is responsible for providing internet connection to use the Service.

THESE DESCRIPTIONS ARE SUBJECT TO CHANGE ANY TIME WITHOUT NOTICE.

© Scott & Scott, LLP