

Automated Business Technologies

Services Guide

This Services Guide contains provisions that define, clarify, and govern the scope of the services described in the Quote. If you do not agree with the terms of this Services Guide, you should not sign the Quote.

This Services Guide is governed under our Master Services Agreement ("MSA"). Capitalized terms in this Services Guide will have the same meaning as the capitalized terms in the MSA.

Initial Audit / Diagnostic Services

In most cases, we will conduct an initial audit of your IT environment to determine the readiness for, and compatibility with, our proposed ongoing managed services. This audit may include:

- Audit to determine general Environment readiness and functional capability
- Review of hardware and software configurations
- Basic security vulnerability check
- Basic backup and file recovery solution audit
- Asset inventory
- Email and website hosting audit
- IT support process audit

Onboarding Services

Onboarding is the stage during which we prepare your IT environment for the monthly managed services described in the Quote. During this phase, we will work with your Authorized Contact(s) and may:

- Uninstall any monitoring tools or other software installed by previous IT service providers
- Compile a full inventory of all protected servers, workstations, and laptops
- Uninstall any previous endpoint protection and install our managed security solutions
- Install remote support access agents on each managed device
- Configure Windows® and application patch management agents
- Optimize device performance including disk cleanup and endpoint protection scans
- Review firewall configuration and other network infrastructure devices
- Review and document current server configuration and status
- Determine existing business continuity strategy and prepare backup options

Ongoing / Recurring Managed Services

The table below describes all managed services provided or facilitated by ABT; however, only those services specifically described in the Quote will be provided to you.

Services Table (Summary)

Service	Description
Backup and File Recovery	Implementation and facilitation of a backup and file recovery solution. Includes 24/7 monitoring, troubleshooting of failed backup disks,

Service	Description
	preventive maintenance, and daily recovery verification. Data encrypted in transit and at rest (256-bit AES).
Backup Monitoring	Monitoring backup status for certain backup applications. Monitors successful completion, failure errors, and destination free space. Note: Monitoring only – not a backup and file recovery solution.
Dark Web Monitoring	Continuous human and machine-powered monitoring to determine if supplied credentials are located on the dark web. Client-supplied credentials are added to the monitoring system.
Email Threat Protection	Managed email protection from phishing, BEC, SPAM, and email-based malware. Protects against social engineering attacks.
Endpoint Antivirus & Malware Protection	AI and machine learning endpoint protection. Detects unauthorized behaviors, blocks suspicious actions, and protects against file-based and fileless malware.
Extended Detection & Response (XDR)	Automated correlation of data across multiple security layers. Includes next-generation deep learning malware detection, data loss prevention, and on-demand endpoint isolation.
End User Security Awareness Training	Online on-demand training videos, quizzes, and simulated phishing email campaigns.
Firewall as a Service	Firewall configured for your organization's needs. Prevents external hackers from accessing internal networks. Appliance provided by ABT (subject to hardware-as-a-service terms; must be returned upon termination).
Firewall Solution (Client-supplied)	Monitors, updates, and supports a Client-supplied firewall appliance.
Managed Detection & Response (MDR)	24x7 managed network detection and response, real-time threat hunting, and real-time threat response.
Password Manager	Secure password vault, password generation, financial information vault, and browser/mobile app access.
Remote Helpdesk	Remote support during normal business hours for managed devices and covered software. Onsite support included for locations within 50 miles of primary corporate location.
Remote Infrastructure Maintenance & Support	Configuration, monitoring, and preventative maintenance for managed IT infrastructure.
Remote Monitoring and Management	24x7 software agent monitoring. Includes capacity monitoring, OS inspection, and patch management.
Security Incident & Event Monitoring (SIEM)	Industry-leading SIEM solution. Detects threats from external and insider sources. Monitoring and alert-based only; remediation is not included in scope.
Server Monitoring & Maintenance	24x7 server monitoring. Includes online status, capacity, performance, and security monitoring.
Multi-Factor Authentication	MFA solution including two-factor authentication for on-premises and cloud-based applications.

Service	Description
Server Next-Generation Antivirus	Next-generation antivirus for server OS. Includes data loss prevention, exploit prevention, and malicious traffic detection.
Updates & Patching	Remote deployment of updates, patches, and security updates for all managed hardware and software.
Virtual CIO (vCIO)	Strategic IT guidance, technology planning, documentation, and participation in scheduled meetings.
Voice Over IP (VoIP) Services	Best effort VoIP telephone support. ABT will work with current VoIP provider to help troubleshoot and resolve Voice over IP issues.
AI Security Protection	Cyber-threat monitoring and enforced policy management for all AI solutions within the organization.
Workstation Next-Generation Malware Solution	Next-generation workstation malware protection. Includes data loss prevention and boot record protection. Part of ABT's Advanced Threat Protection
Workstation Monitoring & Maintenance	24x7 workstation monitoring. Includes online status, capacity, performance, and security monitoring.
Complete Help Desk Services (M–F 8am–5pm)	Comprehensive end-user technical support provided by ABT's certified help desk technicians during standard business hours (Monday–Friday, 8:00 AM–5:00 PM).
Complete Server Support (Elite Server Care) (7 days/week, 24 hours/day)	Full 24/7/365 monitoring, management, and Tier 3 remediation for Client's physical and virtual server infrastructure. Managed by ABT's certified senior engineers with guaranteed response times and rapid escalation.
Advanced Threat Protection	Enterprise-grade cybersecurity protection deployed across all 33 managed endpoints (workstations, laptops, and servers) with 24/7/365 monitoring and active threat remediation through ABT's Security Operations Center (SOC).
Premium Continuity Backup & Disaster Recovery (BDR)	Fully managed cloud-based backup and disaster recovery solution for Client's server environment.

Policies and Procedures Applicable to Services

Software Licensing: All software provided to you by or through ABT is licensed, not sold, to you.

Covered Environment: Services will be applied to the number of devices indicated in the Quote.

Physical Locations: Services will be provided remotely unless an onsite visit is required. All onsite Services will be provided at Client's primary business location unless otherwise agreed.

Minimum Requirements / Exclusions: The following minimum requirements must be maintained at all times:

- Server hardware must be under current warranty coverage
- All equipment with Windows® must be running currently supported versions with all latest critical updates installed

- All software must be genuine, licensed, and vendor-supported
- All wireless data traffic must be securely encrypted
- All servers must be connected to working UPS devices
- Client must provide exclusive administrative privileges to the Environment

Exclusions: Services not expressly described in the Quote will be out of scope. The following services are expressly excluded:

- Customization of third party applications or programming of any kind
- Support for operating systems or hardware no longer supported by the manufacturer
- Data/voice wiring or cabling services
- Battery backup replacement
- Equipment relocation
- The cost to bring the managed environment up to minimum requirements (unless noted in the Quote)

Service Levels

Response, repair, and/or remediation services will be provided during our business hours (M-F, 8 AM – 5 PM Mountain Time, excluding legal holidays), unless otherwise specifically stated in the Quote.

Trouble / Severity	Response Time
Critical / Service Not Available (all users and functions unavailable)	Response within two (2) business hours after notification
Significant Degradation (large number of users or business critical functions affected)	Response within four (4) business hours after notification
Limited Degradation (limited users affected, business process can continue)	Response within eight (8) business hours after notification
Small Service Degradation (one user affected)	Response within two (2) business days after notification
Long Term Project, Preventative Maintenance	Response within four (4) business days after
Direct ticket submission via ABT Chat function	Response within one (1) to five (5) minutes after notification (Within normal business hours)

Additional Policies

Anti-Virus; Anti-Malware

Our anti-virus / anti-malware solution will generally protect the Environment from becoming infected with new viruses and malware. We do not warrant or guarantee that all Malware will be detected, avoided, or removed.

Breach/Cyber Security Incident Recovery

Unless otherwise expressly stated in the Quote, the scope of the Services does not include the remediation and/or recovery from a Security Incident. Such services, if requested, will be provided on a time and materials basis.

Fair Usage Policy

Our Fair Usage Policy applies to all services designated as "unlimited." You agree to refrain from creating urgent support tickets for non-urgent issues or requesting excessive support services inconsistent with normal industry usage patterns.

Hosted Email

You are solely responsible for the proper use of any hosted email service provided to you.

Hosted Email solutions are subject to acceptable use policies (AUPs). You agree to refrain from uploading, posting, transmitting or distributing any prohibited content, including content that is obscene, illegal, or violates third-party intellectual property or privacy rights.

ABT reserves the right, but not the obligation, to suspend Client's access to the Hosted Email service solely (i) upon written notice to Client's Authorized Contact describing the specific AUP violation in reasonable detail, and (ii) only to the extent strictly necessary to remediate a verified AUP violation directly attributable to the Hosted Email service. ABT shall not suspend any other services or systems based on suspected Hosted Email misuse, and shall restore access promptly upon Client's remediation of the identified violation.

Backup (BDR) Services

All data transmitted over the Internet may be subject to malware and computer contaminants. BDR services require a reliable, always-connected internet solution. Data backup and recovery time will depend on the speed and reliability of your internet connection.

Procurement

Equipment and software procured by ABT on Client's behalf may be covered by manufacturer warranties, which will be passed through to Client to the greatest extent possible.

Penetration Testing; Vulnerability Scanning

You understand and agree that security devices, alarms, or other security measures may be tripped during penetration testing and/or vulnerability scanning processes. You will be solely responsible for notifying any monitoring company and all law enforcement authorities.

Obsolescence

If any portion of the managed environment becomes outdated or reaches end-of-support status from the manufacturer, we may designate the device or software as "unsupported" and require you to update the Obsolete Element within a reasonable time period.

VoIP – Dialing 911 (Emergency) Services

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

Registration: You are responsible for activating the E911 dialing feature by registering the address where you will use the VoIP service.

Location: The address you provide in the control panel is the location to which emergency services will respond.

Power Loss: If you lose power, the E911 calling service will not function until power is restored.

Internet Disruption: If your internet connection is lost, E911 calling will not function until the internet connection is restored.

Acceptable Use Policy

The following policy applies to all hosted services provided to you. ABT does not routinely monitor the activity of hosted accounts except to measure service utilization, security-related purposes, and billing-related purposes.

Violations of this AUP include:

- **Harmful or illegal uses:** Use for illegal purposes, to cause harm to minors, or to transmit material that threatens or encourages bodily harm.
- **Fraudulent activity:** Use to conduct any fraudulent activity or deceptive practices.
- **Forgery or impersonation:** Adding, removing, or modifying identifying network header information to deceive.
- **SPAM:** Use to transmit any unsolicited commercial or bulk e-mail.
- **Cryptomining:** Using any portion of Hosted Services for mining cryptocurrency.
- **Unauthorized access:** Use to access or attempt to access accounts of others or to penetrate security measures.
- **IP infringement:** Use to transmit materials that infringe intellectual property rights of any third party.
- **Distribution of malware:** Intentional distribution of software that attempts to cause damage or annoyance.

Last Updated: September 2026