

SERVICES GUIDE

This Services Guide contains provisions that define, clarify, and govern the scope of the services described in the quote that has been provided to you (the "Quote"), as well as the policies and procedures that we follow (and to which you agree) when we provide a service to you or facilitate a service for you. If you do not agree with the terms of this Services Guide, you should not sign the Quote and you must contact us for more information. This Services Guide is our "owner's manual" that generally describes all managed services provided or facilitated by Fulton May Solutions ("Fulton May," "we," "us," or "our"); however, only those services specifically described in the Quote will be facilitated and/or provided to you (collectively, the "Services").

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

Activities or items that are not specifically described in the Quote will be out of scope and will not be included unless otherwise agreed to by us in writing. Please read this Services Guide carefully and keep a copy for your records.

Function / Addendum	Description
Initial Audit / Diagnostic Services	<p>In the Initial Audit/Diagnostic phase of our services, we audit your managed information technology environment (the "Environment") to determine the readiness for, and compatibility with, ongoing managed services. Our auditing services may be comprised of some or all of the following:</p> <ul style="list-style-type: none"> • Audit to determine general Environment readiness and functional capability • Review of hardware and software configurations • Review of current vendor service / warranty agreements for Environment hardware and software • Basic security vulnerability check • Basic backup and file recovery solution audit • Speed test and ISP audit • Print output audit • Office telephone vendor service audit • Asset inventory • Email and website hosting audit • IT support process audit <p>If deficiencies are discovered during the auditing process (such as outdated equipment or unlicensed software), we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of the Services and provide you with options to correct the deficiencies. Please note, unless otherwise expressly agreed by us in writing, auditing services do not include the remediation of any issues, errors, or deficiencies ("Issues"), and we cannot guarantee that all Issues will be detected during the auditing process. Issues that are discovered in the Environment after the auditing process is completed may be addressed in one or more subsequent quotes.</p>
Onboarding Services	<p>In the Onboarding phase of our services, we will prepare your IT environment for the monthly managed services described in the Quote. During this phase, we will work with your Authorized Contact(s) to review the information we need to prepare the targeted environment, and we may also:</p> <ul style="list-style-type: none"> • Uninstall any monitoring tools or other software installed by previous IT service providers. • Compile a full inventory of all protected servers, workstations, and laptops. • Uninstall any previous endpoint protection and install our managed security solutions (as indicated in the Quote). • Install remote support access agents (i.e., software agents) on each managed device to enable remote support. • Configure Windows® and application patch management agent(s) and check for missing security updates. • Uninstall unsafe applications or applications that are no longer necessary. • Optimize device performance including disk cleanup and endpoint protection scans. • Review firewall configuration and other network infrastructure devices. • Review status of battery backup protection on all mission critical devices. • Stabilize network and assure that all devices can securely access the file server. • Review and document current server configuration and status. • Determine existing business continuity strategy and status; prepare backup file recovery and incident response option for consideration. • Review password policies and update user and device passwords. • As applicable, make recommendations for changes that should be considered to the managed environment. <p>This list is subject to change if we determine, at our discretion, that different or additional onboarding activities are required.</p> <p>If deficiencies are discovered during the onboarding process, we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of our monthly managed services. Please note, unless</p>

SERVICES GUIDE

	<p>otherwise expressly stated in the Quote, onboarding-related services do not include the remediation of any issues, errors, or deficiencies (“Issues”), and we cannot guarantee that all Issues will be detected during the onboarding process.</p> <p>The duration of the onboarding process depends on many factors, many of which may be outside of our control—such as product availability/shortages, required third party vendor input, etc. As such, we can estimate, but cannot guarantee, the timing and duration of the onboarding process. We will keep you updated as the onboarding process progresses.</p>
<p>Ongoing / Recurring Services</p>	<p>Ongoing/recurring services are services that are provided to you or facilitated for you on an ongoing basis and, unless otherwise indicated in a Quote, are billed to you monthly. Some ongoing/recurring services will begin with the commencement of onboarding services; others will begin when the onboarding process is completed. Please direct any questions about start or “go live” dates to your account manager.</p>
<p>Ongoing / Recurring Services – Backup and File Recovery</p>	<p>Implementation and facilitation of a backup and file recovery solution from our designated Third Party Provider.</p> <ul style="list-style-type: none"> • 24/7 monitoring of backup system, including offsite backup, offsite replication, and an onsite backup appliance (“Backup Appliance”). • Troubleshooting and remediation of failed backup disks. • Preventive maintenance and management of imaging software. • Firmware and software updates of backup appliance. • Problem analysis by the network operations team. • Monitoring of backup successes and failures. • Daily recovery verification. <p><u>Backup Data Security:</u> All backed up data is encrypted in transit and at rest in 256-bit AES encryption. All facilities housing backed up data implement physical security controls and logs, including security cameras, and have multiple internet connections with failover capabilities.</p> <p><u>Backup Retention:</u> Backed up data will be retained for the periods indicated below, unless a different time period is expressly stated in the Quote. This includes both on-premise and cloud backups.</p> <ul style="list-style-type: none"> • On-Premise Backups: All on-premise backups will be stored on a Network Attached Storage (NAS) device, which will be kept in a secure location with restricted access. On-premise backups will be performed daily and retained on a rolling thirty (30) day basis. • Cloud Backups: All cloud backups will be stored in a secure, off-site location that meets the organization’s security standards. Cloud backups will be performed daily and retained on a rolling thirty (30) day basis. <p><u>Backup Alerts:</u> Managed servers will be configured to inform of any backup failures.</p> <p><u>Recovery of Data:</u> If you need to recover any of your backed up data, then the following procedures will apply:</p> <ul style="list-style-type: none"> • Service Hours: Backed up data can be requested during our normal business hours, which are currently 7:00am to 7:00pm CST. • Request Method: Requests to restore backed up data should be made through one of the following methods: <ul style="list-style-type: none"> • Email: support@fultonmay.com • Web portal: https://fultonmay.com/support • Telephone: 31-207-2200 option 1 • Restoration Time: We will endeavor to restore backed up data as quickly as possible following our receipt of a request to do so; however, in all cases data restoration services are subject to (i) technician availability and (ii) confirmation that the restoration point(s) is/are available to receive the backed-up data.
<p>Ongoing / Recurring Services – Dark Web Monitoring</p>	<p>Implementation and facilitation of a Dark Web Monitoring solution from our designated Third-Party Provider.</p> <p>Credentials supplied by Client will be added into a system that continuously uses human and machine-powered monitoring to determine if the supplied credentials are located on the dark web.</p> <p>If compromised credentials are found, they are reported to Help Desk Services staff who will review the incident and notify affected end-users.</p> <p>Dark web monitoring can be a highly effective tool to reduce the risk of certain types of cybercrime; however, we do not guarantee that the dark web monitoring service will detect all actual or potential uses of your designated credentials or information.</p>

SERVICES GUIDE

<p>Ongoing / Recurring Services – Email Threat Protection</p>	<p>Implementation and facilitation of a trusted email threat protection solution from our designated Third Party Provider.</p> <ul style="list-style-type: none"> • Managed email protection from phishing, business email compromise (BEC), SPAM, and email-based malware. • Friendly Name filters to protect against social engineering impersonation attacks on managed devices. • Protection against social engineering attacks like whaling, CEO fraud, business email compromise or W-2 fraud. • Protects against newly registered and newly observed domains to catch the first email from a newly registered domain. • Protects against display name spoofing. • Protects against “looks like” and “sounds like” versions of domain names. <p>Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details. All hosted email is subject to the terms of our Hosted Email Policy and our Acceptable Use Policy.</p>
<p>Ongoing / Recurring Services – Endpoint Antivirus & Malware Protection</p>	<p>Implementation and facilitation of an endpoint malware protection solution from our designated Third Party Provider.</p> <ul style="list-style-type: none"> • Artificial intelligence and machine learning to provide a comprehensive and adaptive protection paradigm to managed endpoints. • Detection of unauthorized behaviors of users, applications, or network servers. • Blocking of suspicious actions before execution. • Analyzing suspicious app activity in isolated sandboxes. • Antivirus and malware protection for managed devices such as laptops, desktops, and servers. • Protection against file-based and fileless scripts, as well as malicious JavaScript, VBScript, PowerShell, macros and more. • Whitelisting for legitimate scripts. • Blocking of unwanted web content. • Detection of advanced phishing attacks. • Detection / prevention of content from IP addresses with low reputation. <p>* Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.</p>
<p>Ongoing / Recurring Services – End User Security Awareness Training</p>	<p>Implementation and facilitation of a security awareness training solution from an industry-leading third party solution provider.</p> <ul style="list-style-type: none"> • Online, on-demand training videos (multi-lingual). • Online, on-demand quizzes to verify employee retention of training content. • Baseline testing to assess the phish-prone percentage of users; simulated phishing email campaigns designed to educate employees about security threats. <p>Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.</p>
<p>Ongoing / Recurring Services – Firewall as a Service (firewall appliance provided by Fulton May)</p>	<ul style="list-style-type: none"> • Provide a firewall configured for your organization’s specific bandwidth, remote access, and user needs. • Helps to prevent hackers from accessing internal network(s) from outside the network(s), while providing secure and encrypted remote network access; provides antivirus scanning for all traffic entering and leaving the managed network; provides website content filtering functionality. • Firewall appliances are subject to “Hardware as a Service” terms and conditions located in this Guide. • Firewall appliance must be returned to Fulton May upon the termination of service. Client will be responsible for missing or damaged (normal wear and tear excepted) appliance.
<p>Ongoing / Recurring Services – Firewall Solution (firewall appliance provided/purchased by Client)</p>	<ul style="list-style-type: none"> • Monitors, updates (software/firmware), and supports Client-supplied firewall appliance. • Helps to prevent hackers from accessing internal network(s) from outside the network(s), while providing secure and encrypted remote network access; provides antivirus scanning for all traffic entering and leaving the managed network; provides website content filtering functionality.

SERVICES GUIDE

<p>Ongoing / Recurring Services – Labor for New / Replacement Workstations</p>	<p>Includes all labor charges for setup of new workstations, or replacement of existing workstations.</p> <ul style="list-style-type: none"> • Labor covers: <ul style="list-style-type: none"> ○ New computers / additional computers added during the term of the Quote; ○ Replacement of existing computers that are four (4) or more years old (as determined by the manufacturer's serial number records); ○ Replacement of existing computers that lost/stolen or irreparably damaged and/or out of warranty but not yet four years old; ○ Operating systems upgrades – subject to hardware compatibility. <p>The following restrictions apply:</p> <ul style="list-style-type: none"> • Upgrades or installs of new or replacement computers are limited to four (4) devices per month unless otherwise approved in advance by Fulton May; • This service is not available for used or remanufactured computers; and, • New/replacement computers must be business-grade machines (not home) from a major manufacturer like Dell, HPE, or Lenovo.
<p>Ongoing / Recurring Services – Managed Detection & Response (MDR)</p>	<p>Implementation and facilitation of a top-tier MDR solution from our designated Third Party Provider.</p> <ul style="list-style-type: none"> • 24x7 Managed network detection and response. • Real time and continuous (24x7) monitoring and threat hunting. • Real time threat response. • Alerts handled in accordance with our Service response times, below. • Security reports, such as privileged activities, security events, and network reports, are available upon request. • 24x7x365 access to a security team for incident response* <p>* Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.</p>
<p>Ongoing / Recurring Services – Managed Detection & Response (MDR Light)</p>	<p>Implementation and facilitation of a MDR with built in SIEM solution from our designated Third Party Provider.</p> <ul style="list-style-type: none"> • 24x7 Intelligent monitoring and threat hunting. • Enhanced endpoint, Microsoft 365 and Google Mail visibility. • Real time threat response. • Alerts handled in accordance with our Security team response times, below. • Security reports, such as privileged activities, security events, and network reports, are available upon request. <p>* Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.</p>
<p>Ongoing / Recurring Services – Penetration (Pen) Testing</p>	<p>Penetration testing (or “pen” testing) simulates a cyberattack against your IT infrastructure to identify exploitable vulnerabilities. Unlike ongoing vulnerability scanning services that provide a constant, static level of network scanning, pen testing may involve several stages of reconnaissance and actual attack methodologies (such as brute force attacks and/or SQL injection attacks) and may include unconventional and targeted attacks that occur during business and non-business hours. Pen testing may consist of any of the following:</p> <p>External Pen Testing: exposes vulnerabilities in your internet-facing systems, networks, firewalls, devices, and/or web applications that could lead to unauthorized access.</p> <p>Internal Pen Testing: Validates the effort required for an attacker to overcome and exploit your internal security infrastructure after access is gained.</p> <p>PCI Pen Testing: Using the goals set by the PCI Security Standards Council, this test involves both external and internal pen testing methodologies.</p> <p>Please see additional terms for Penetration Testing below.</p>
<p>Ongoing / Recurring Services – Remote Helpdesk</p>	<ul style="list-style-type: none"> • Remote support provided during normal business hours for managed devices and covered software • Tiered-level support provides a smooth escalation process and helps to ensure effective solutions.
<p>Ongoing / Recurring Services – Remote Infrastructure Maintenance & Support</p>	<ul style="list-style-type: none"> • Configuration, monitoring, and preventative maintenance services provided for the managed IT infrastructure • If remote efforts are unsuccessful, then Fulton May will dispatch a technician to the Client's premises to

SERVICES GUIDE

	<p>resolve covered incidents (timing of onsite support is subject to technician availability and scheduling).</p>																											
<p>Ongoing / Recurring Services – Remote Monitoring and Management</p>	<p>Software agents installed in Covered Equipment (defined below) report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below.</p> <ul style="list-style-type: none"> • Includes capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD partitions, not external devices such as USB or mapped drives) • Includes routine operating system inspection and cleansing to help ensure that disk space is increased before space-related issues occur. • Review and installation of updates and patches for supported software. • <p>In addition to the above, our remote monitoring and management service will be provided as follows:</p> <table border="1" data-bbox="675 606 1289 863"> <thead> <tr> <th>Event</th> <th>Server</th> <th>Workstation</th> </tr> </thead> <tbody> <tr> <td>Hardware Failures</td> <td>Yes</td> <td>No</td> </tr> <tr> <td>Device Offline</td> <td>Yes</td> <td>No</td> </tr> <tr> <td>Failed/Missing Backup</td> <td>Yes</td> <td>No</td> </tr> <tr> <td>Failed/Missing Updates</td> <td>Yes</td> <td>Yes</td> </tr> <tr> <td>Low Disk Space</td> <td>Yes</td> <td>No</td> </tr> <tr> <td>Agent missing/misconfigured</td> <td>Yes</td> <td>Yes</td> </tr> <tr> <td>Excessive Uptime</td> <td>Yes</td> <td>No</td> </tr> <tr> <td>Automatic Reboots (weekly)</td> <td>No</td> <td>Yes</td> </tr> </tbody> </table>	Event	Server	Workstation	Hardware Failures	Yes	No	Device Offline	Yes	No	Failed/Missing Backup	Yes	No	Failed/Missing Updates	Yes	Yes	Low Disk Space	Yes	No	Agent missing/misconfigured	Yes	Yes	Excessive Uptime	Yes	No	Automatic Reboots (weekly)	No	Yes
Event	Server	Workstation																										
Hardware Failures	Yes	No																										
Device Offline	Yes	No																										
Failed/Missing Backup	Yes	No																										
Failed/Missing Updates	Yes	Yes																										
Low Disk Space	Yes	No																										
Agent missing/misconfigured	Yes	Yes																										
Excessive Uptime	Yes	No																										
Automatic Reboots (weekly)	No	Yes																										
<p>Ongoing / Recurring Services – Security Incident & Event Monitoring (SIEM+)</p>	<p>Implementation and facilitation of an industry leading SIEM solution from our designated Third Party Provider.</p> <p>The SIEM+ service utilizes threat intelligence to detect threats that can exploit potential vulnerabilities against your managed network.</p> <ul style="list-style-type: none"> • Initial Assessment. Prior to implementing the SIEM service, we will perform an initial assessment of the managed network at your premises to define the scope of the devices/network to be monitored (the “Initial Assessment”). • Monitoring. The SIEM service detects threats from external facing attacks as well as potential insider threats and attacks occurring inside the monitored network. Threats are correlated against known baselines to determine the severity of the attack. • Alerts & Analysis. Threats are reviewed and analyzed by third-party human analysts to determine true/false positive dispositions and actionability. If it is determined that the threat was generated from an actual security-related or operationally deviating event (an “Event”), then you will be notified of that Event. <p>Events are triggered when conditions on the monitored system meet or exceed predefined criteria (the “Criteria”). Since the Criteria are established and optimized over time, the first thirty (30) days after deployment of the SIEM services will be used to identify a baseline of the Client’s environment and user behavior. During this initial thirty (30) day period, Client may experience some “false positives” or, alternatively, during this period not all anomalous activities may be detected.</p> <p>Note: The SIEM service is a monitoring and alert-based system only; remediation of detected or actual threats are not within the scope of this service and may require Client to retain Fulton May’s services on a time and materials basis.</p>																											

SERVICES GUIDE

<p>Ongoing / Recurring Services – Server Monitoring & Maintenance</p>	<p>As part of our RMM service, we will monitor and maintain managed servers as follows:</p> <ul style="list-style-type: none"> • Software agents installed in covered servers report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below. • Online status monitoring, alerting us to potential failures or outages • Capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD and SSD partitions, not external devices such as USB or mapped network drives) • Performance monitoring, alerting us to unusual processor or memory usage • Server essential service monitoring, alerting us to server role-based service failures • Endpoint protection agent monitoring, alerting us to potential security vulnerabilities • Routine operating system inspection and cleansing • Secure remote connectivity to the server and collaborative screen sharing • Review and installation of updates and patches for Windows and supported software • Asset inventory and server information collection
<p>Ongoing / Recurring Services – Two Factor Authentication</p>	<p>Implementation and facilitation of a two-factor authentication solution from our designated Third-Party Provider.</p> <ul style="list-style-type: none"> • Advanced two factor authentication with advanced admin features. • Secures on-premises and cloud-based applications. • Permits custom access policies based on role, device, location. • Identifies and verifies device health to detect “risky” devices
<p>Ongoing / Recurring Services – Server Next-Generation Antivirus</p>	<p>Implementation and facilitation of a top-tier, next generation antivirus protection solution from our designated Third Party Provider.</p> <p>Software agents installed in covered server devices protect against malware and prevents intruder access. Used in coordination with other endpoint security layers and security solutions to form a comprehensive defense strategy.</p> <ul style="list-style-type: none"> • Next-generation deep learning malware detection, file scanning, and live protection for Server OS • Web access security and control, application security and control, intrusion prevention system • Data loss prevention, exploit prevention, malicious traffic detection, disk and boot record protection
<p>Ongoing / Recurring Services – Software Licensing (applies to all software licensed by or through Fulton May)</p>	<p>All software provided to you by or through Fulton May is licensed, not sold, to you (“Software”). In addition to any Software-related requirements described in Fulton May’s Master Services Agreement, Software may also be subject to end user license agreements (EULAs), acceptable use policies (AUPs), and other restrictions all of which must be strictly followed by you and any of your authorized users.</p> <p>When installing/implementing software licenses in the managed environment or as part of the Services, we may accept (and you agree that we may accept) any required EULAs or AUPs on your behalf. You should assume that all Software has an applicable EULA and/or AUP to which your authorized users and you must adhere. If you have any questions or require a copy of the EULA or AUP, please contact us.</p>
<p>Ongoing / Recurring Services – Updates & Patching</p>	<ul style="list-style-type: none"> • Remotely deploy updates (e.g., x.1 to x.2), as well as bug fixes, minor enhancements, and security updates as deemed necessary on all managed hardware. • Perform minor hardware and software installations and upgrades of managed hardware. • Perform minor installations (i.e., tasks that can be performed remotely and typically take less than thirty (30) minutes to complete). • Deploy, manage, and monitor the installation of approved service packs, security updates and firmware updates as deemed necessary on all applicable managed hardware. <p><u>Please note:</u> We will keep all managed hardware and managed software current with critical patches and updates (“Patches”) as those Patches are released generally by the applicable manufacturers. Patches are developed by third party vendors and, on rare occasions, may make the Environment, or portions of the Environment, unstable or cause the managed equipment or software to fail to function properly even when the Patches are installed correctly. We will not be responsible for any downtime or losses arising from or related to the installation or use of any Patch. We reserve the right, but not the obligation, to refrain from installing a Patch if we are aware of technical problems caused by a Patch, or we believe that a Patch may render the Environment, or any portion of the Environment, unstable.</p>

SERVICES GUIDE

<p>Ongoing / Recurring Services – Vulnerability Scanning</p>	<p>Implementation and facilitation of an industry-recognized vulnerability scanning solution from our designated Third Party Provider.</p> <p>Vulnerability scanning identifies holes in the managed network that could be exploited. External vulnerability scans (which pertain to the IP address assigned to each customer location through the Client's ISP) are run monthly. Internal vulnerability scans (which pertain to all systems inside the managed network) are run at least annually.</p> <p>Vulnerability results will be discussed during business review meetings with Client. Vulnerability reports will be made available on request.</p> <p>Please see additional terms for vulnerability scanning below.</p>
<p>Ongoing / Recurring Services – Website Hosting</p>	<p>Our designated Third Party Provider will provide sufficient space and bandwidth to host your designated website ("Website") which, except for scheduled downtime or force majeure events, will be available on a 24x7 basis. The Website will be hosted on a server that may be shared between many customers; however, the Website will be given a unique address.</p> <ul style="list-style-type: none"> • Migration of Servers. As a normal course of business, we or our Third Party Provider, as applicable, may migrate the servers on which the Website is hosted. This process will not interfere with the Hosting Services, however, due to the potential for migration, you are not guaranteed a permanent or dedicated IP address. • Administration. You will be provided with access to a dashboard through which you may make configuration adjustments to the hosted environment; however, we strongly advise you to refrain from making changes to the hosted environment without our guidance or direction. We will not be responsible for remediating issues caused by your adjustments to the hosted environment unless those adjustments were made pursuant to our written directions or under our supervision. • Resource/Load Balancing. The bandwidth made available to your website is shared and allocated among all of our customers. You must comply with all bandwidth and Fulton May-imposed limitations on the hosting services as established by Fulton May from time to time. We reserve the right to load-balance applicable bandwidth to ensure that your activity will not restrict, inhibit, or diminish any other user's use of the bandwidth or create an unusually large burden on the bandwidth. We reserve the right to restrict your access to your hosted website in the event that your activities create a disproportionate burden on our network or our third party providers' networks (if applicable), or any other crucial resources reasonably needed to ensure the functionality, integrity, and/or security of the hosting services. • Backup. Data in the hosted environment will be backed up daily ("Standard Backup Service"); however, the Standard Backup Service is not, and should not be regarded as, a backup and disaster recovery solution. Although the Standard Backup Service is a part of the hosting services, it is only a basic backup service, and it does not provide data integrity verification services or other advanced backup or recovery options. We strongly recommend that you implement a separate backup and disaster recovery solution to protect the security and integrity of, and accessibility to, the data in the hosted environment. • Storage and Security. We and/or our third party providers will take reasonable steps to prevent unauthorized access to the Website and the hosted environment; however, you understand and agree that no security solution is 100% effective, and we do not warrant or guarantee that the hosted environment will be free from unauthorized access or malware at all times. <p>Client, as well as any visitors to the Website, must comply with our Acceptable Use Policy which is located at the end of this Services Guide.</p>
<p>Ongoing / Recurring Services – Workstation Monitoring & Maintenance</p>	<p>Software agents installed in covered workstations report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below.</p> <ul style="list-style-type: none"> • Online status monitoring, alerting us to potential failures or outages. • Capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD and SSD partitions, not external devices such as USB or mapped network drives). • Performance monitoring, alerting us to unusual processor or memory usage. • Endpoint protection agent monitoring, alerting us to potential security vulnerabilities. • Routine operating system inspection and cleansing. • Secure remote connectivity to the workstation and collaborative screen sharing. • Review and installation of updates and patches for Windows and supported software. • Asset inventory and workstation information collection.

SERVICES GUIDE

Ongoing / Recurring Services –
Secure Destruction of Client
Hardware

Recommended that all client hardware must be securely destroyed when it is no longer needed, has reached an end-of-life, or is returned for disposal. Destruction must ensure that data is irrecoverable and that physical components are rendered unusable.

- Destruction Service
 - Obtain written authorization from the client before proceeding with and scheduling destruction of hardware and provide current pricing per item at time of request to be charged to Client.
 - Facilitate destruction through a Third-Party Provider certified to follow secure destruction standards and receive the Certificate of Destruction that will be retained and provided to Client upon request.
 - Record the following:
 - Serial numbers and asset tags
 - Date and method of destruction
- Declining Destruction Service
 - Client will be responsible for arranging to have their hardware removed or providing approval for their hardware to be shipped to them at their expense, from our facility upon end of life if our Destruction Service is declined.
 - Delays in removing hardware may result in storage fees after 60 days of storage.

SERVICES GUIDE

Covered Environment

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

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

If the Quote indicates that the Services are billed on a "per user" basis, then the Services will be provided for up to two (2) Business Devices used by the number of users indicated in the Quote. A "Business Device" is a device that (i) is owned or leased by Client and used primarily for business, (ii) is regularly connected to Client's managed network, and (iii) has installed on it a software agent through which we (or our designated Third-Party Providers) can monitor the device.

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

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

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

Physical Locations Covered by Services

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

Minimum Requirements / Exclusions

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

- Server hardware must be under current warranty coverage.
- All equipment with Microsoft Windows® operating systems must be running then-currently supported versions of such software and have all the latest Microsoft service packs and critical updates installed.
- All software must be genuine, licensed, and vendor- or OEM-supported.
- Server file systems and email systems (if applicable) must be protected by licensed and up-to-date virus protection software.
- The managed environment must have a currently licensed, vendor-supported server-based backup solution that can be monitored.
- All wireless data traffic in the managed environment must be securely encrypted.
- All servers must be connected to working UPS devices.
- Recovery coverage assumes data integrity of the backups or the data stored on the backup devices. We do not guarantee the integrity of the backups or the data stored on the backup devices. Server restoration will be to the point of the last successful backup.
- Client must provide all software installation media and key codes in the event of a failure.
- Any costs required to bring the Environment up to these minimum standards are not included in this Services Guide.
- Client must provide us with exclusive administrative privileges to the Environment.
- Client must not affix or install any accessory, addition, upgrade, equipment, or device on to the firewall, server, or NAS appliances (other than electronic data) unless expressly approved in writing by us.

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

- Customization of third party applications, or programming of any kind.
- Support for operating systems, applications, or hardware no longer supported by the manufacturer.
- Data/voice wiring or cabling services of any kind.
- Battery backup replacement.
- Equipment relocation.

SERVICES GUIDE

Exclusions Cont'd:

- SharePoint, Automation and AI Development and Customization. The design, development, configuration, or customization of environments, sites, pages, workflows, or integrations of any kind are expressly excluded from the scope of the Services. Day-to-day administration and end-user support of an existing, previously configured SharePoint environment may be provided on a best-effort basis; however, any build-out, migration, redesign, or custom development work requires a separate written quote and, if applicable, a Statement of Work agreed upon by Fulton May in writing prior to commencement.
- The cost to bring the managed environment up to these minimum requirements (unless otherwise noted in the Quote).
- The cost of repairs to hardware or any supported equipment or software, or the costs to acquire parts or equipment, or shipping charges of any kind.

Fees

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

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

Changes to Environment. Initially, you will be charged the monthly fees indicated in the Quote. Thereafter, if the managed environment changes, or if the number of authorized users accessing the managed environment changes, then you agree that the fees will be automatically and immediately modified to accommodate those changes. Project Threshold; Statement of Work Requirement. Any service request or engagement that is anticipated to require more than four (4) cumulative hours of labor to complete will be considered a project-level engagement and will not be performed under the standard managed services agreement. Prior to commencing any such engagement, Fulton May will provide Client with a separate written project quote and, where applicable, a Statement of Work ("SOW") outlining the scope, estimated labor, timeline, and applicable fees. Work will not begin until the project quote and/or SOW has been reviewed and approved by Client in writing. Fulton May reserves the right to determine, in its reasonable discretion, whether a request meets the project threshold based on estimated scope.

Travel Time. If onsite services are provided, we will travel up to 45 minutes from our office to your location at no charge. Time spent traveling beyond 45 minutes (e.g., locations that are beyond 45 minutes from our office, occasions on which traffic conditions extend our drive time beyond 45 minutes one-way, etc.) will be billed to you at our then current hourly rates. In addition, you will be billed for all tolls, parking fees, and related expenses that we incur if we provide onsite services to you.

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

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

Term; Termination

The Services will commence, and billing will begin, on the date indicated in the Quote ("Commencement Date") and will continue through the initial term listed in the Quote ("Initial Term"). We reserve the right to delay the Commencement Date until all onboarding/transition services (if any) are completed, and all deficiencies / revisions identified in the onboarding process (if any) are addressed or remediated to Fulton May's satisfaction.

The Services will continue through the Initial Term until terminated as provided in the Agreement, the Quote, or as indicated in this Service Guide (the "Service Term").

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

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

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

SERVICES GUIDE

Offboarding

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

- Removal / disabling of monitoring agents in the Environment.
- Removal / disabling of endpoint software from the Environment.
- Removal / disabling of Microsoft 365 from the Environment (unless the licenses for Microsoft 365 are being transferred to your incoming provider; please speak to your technician for details.)
- Termination of SQL or Remote Desktop licenses provided by Fulton May.
- Removal of credentials from the Environment.
- Removal of backup software from the Environment.

Additional Policies

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

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

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

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

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

Anti-Virus; Anti-Malware. Our anti-virus / anti-malware solution will generally protect the Environment from becoming infected with new viruses and malware ("Malware"); however, Malware that exists in the Environment at the time that the security solution is implemented may not be capable of being removed without additional services, for which a charge may be incurred. We do not warrant or guarantee that all Malware will be detected, avoided, or removed, or that any data erased, corrupted, or encrypted by Malware will be recoverable. To improve security awareness, you agree that Fulton May or its designated third party affiliate may transfer information about the results of processed files, information used for URL reputation determination, security risk tracking, and statistics for protection against spam and malware. Any information obtained in this manner does not and will not contain any personal or confidential information.

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

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

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



SERVICES GUIDE

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

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

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

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

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

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

VTCTO or VCIO or Technical Account Manager Services. The advice and suggestions provided by us in our capacity as a virtual chief technology or information officer (if applicable) will be for your informational and/or educational purposes only. Fulton May will not hold an actual director or officer position in Client’s company, and we will neither hold nor maintain any fiduciary relationship with Client. Under no circumstances shall Client list or place Fulton May on Client’s corporate records or accounts.

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

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

No Third Party Scanning. Unless we authorize such activity in writing, you will not conduct any test, nor request or allow any third party to conduct any test (diagnostic or otherwise), of the security system, protocols, processes, or solutions that we implement in the managed environment (“Testing Activity”). Any services required to diagnose or remediate errors, issues, or problems arising from unauthorized Testing Activity are not covered under the Quote, and if you request us (and we elect) to perform those services, those services will be billed to you at our then-current hourly rates.

SERVICES GUIDE

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

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

Acceptable Use Policy

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

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

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

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

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

SERVICES GUIDE

shared network resources by one customer may have a negative impact on all other customers. Misuse of network resources in a manner which impairs network performance is prohibited. You are prohibited from excessive consumption of resources, including CPU time, memory, and session time. You may not use resource-intensive programs which negatively impact other customers or the performances of our systems or networks.

- *Allowing the misuse of your account:* You are responsible for any misuse of your account, even if the inappropriate activity was committed by an employee or independent contractor. You shall not permit your hosted network, through action or inaction, to be configured in such a way that gives a third party the capability to use your hosted network in an illegal or inappropriate manner. You must take adequate security measures to prevent or minimize unauthorized use of your account. It is your responsibility to keep your account credentials secure.

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

Revisions to this AUP: We reserve the right to revise or modify this AUP at any time. Changes to this AUP shall not be grounds for early contract termination or non-payment.