1856 North Nob Hill Rd, #213
Plantation, FL 33322
(954)441-6211
www.otmgm.com

SERVICE GUIDE

This Service Guide defines the scope of services described in the quote (the "**Quote**") that has been provided to you, as well as policies and support standards applicable to services provided by Online Technology Management, Inc. ("**OTM**"). Only services expressly included in the Quote are provided. If you do not agree with the terms of this Service Guide, please contact us for more information before signing the Quote.

Introduction

This Services Guide outlines the managed services available through Online Technology Management, Inc. ("**OTM**," "**we**," "**us**," or "**our**"). Your engagement includes only those services specifically listed in your Quote, which together constitute the services ("**Services**") provided and/or facilitated by OTM.

OTM provides services in accordance with the applicable Master Services Agreement ("**MSA**"). The MSA may be located through the link on the Quote provided to you or we can send you a copy by email upon request.

This Service Guide does not replace the MSA but incorporates all the provisions and obligations set forth in the MSA. In the event of any conflict among the governing documents, the order of precedence shall be: (i) the applicable Quote, (ii) the applicable Service Guide, (iii) this Master Services Agreement, and (iv) applicable Third-Party Provider terms. The Requested Services to be provided by OTM shall be limited to those Services described below pursuant to the terms and conditions stated in the MSA and/or your Quote.

Services may include monitoring, maintenance, support, reporting, remediation assistance, vendor coordination, and strategic technology guidance. Customers are responsible for maintaining supported systems, licensing, and cooperation with OTM personnel.

OTM may utilize third-party solutions and other approved platforms when applicable to the purchased services. OTM may change Third-Party Providers without notice provided the replacement offers substantially similar functionality.

Any services, activities, or deliverables not expressly identified in the applicable Quote are excluded from the Services and will be considered out of scope unless mutually agreed upon in writing by the parties.

Please review this Service Guide carefully and retain a copy for your records.

1856 North Nob Hill Rd, #213
Plantation, FL 33322
(954)441-6211
www.otmgm.com

Recurring Services

Ongoing or recurring services are provided or facilitated on a continuing basis and, unless otherwise specified in the applicable Quote, are billed monthly. Certain recurring services may commence during the onboarding process, while others may begin upon completion of onboarding. For questions regarding service commencement or go-live dates, please contact your account manager.

DynamiCare

Managed Service offering from Dynamic Network Support, LLC (DynamiCare Complete)

- Monitoring and alerting of computers and servers.
- Automated and manual maintenance of computers and servers (including software updates and patch management).
- Helpdesk Services
- Project Services – design, quoting, implementation, and management.
- Cyber-Security Training.
- Server Backup & Disaster Recovery Services.
- Dark Web Monitoring
- Employee Cyber Training
- Multi-Factor Authentication Support
- Remote/Onsite Support

Backup and File Recovery

OTM will implement, manage, and facilitate a backup and file recovery solution through its designated third-party backup provider.

Service Features

The Managed Backup & Recovery Service includes:

- Monitoring of backup operations, including onsite backups, offsite backups, and offsite replication.
- Monitoring and management of the onsite backup appliance ("Backup Appliance"), where applicable.
- Troubleshooting and remediation of backup failures and storage-related issues.
- Preventive maintenance and administration of backup and imaging software.
- Firmware and software updates for the Backup Appliance.
- Problem identification, analysis, and escalation by OTM Support Team.
- Monitoring and reporting of backup successes and failures.

1856 North Nob Hill Rd, #213
Plantation, FL 33322
(954)441-6211
www.otmgm.com

- Bi-monthly verification testing of backup recovery capabilities.

Backup Data Security
All backup data is encrypted both in transit and at rest using AES-256 encryption. Backup data is stored in facilities that maintain industry-standard physical security controls, including access controls, monitoring systems, audit logging, and redundant network connectivity with failover capabilities.

Backup Retention
Unless otherwise specified in the applicable Quote, backup data will be retained according to the following schedule:

On-Premises Backups
- Stored on a Network Attached Storage (NAS) device located on your premises.
- The NAS device must be maintained in a secure location with restricted physical access.
- Backups are performed daily.
- Backup data is retained on a rolling thirty (30) day basis with no fewer than 10 versions.

Cloud Backups
- Stored in a secure offsite environment maintained by our designated backup provider.
- Backups are performed daily.
- Backup data is retained on a rolling thirty (30) day basis with no fewer than 10 versions.

Backup Failure Notifications
Managed servers will be configured to generate alerts for backup failures, allowing for timely investigation and remediation.

Data Restoration Services
If recovery of backed-up data is required, the following provisions will apply:

Service Hours
- Requests for data restoration may be submitted during OTM's standard business hours, currently Monday through Friday, 8:30 a.m. to 5:30 p.m., excluding recognized holidays.

Request Method
- Requests for the restoration of backup data must be submitted through one of the following methods:
- Email: support@otmgm.com
- Phone: (954)441-6211 Option: 2

1856 North Nob Hill Rd, #213
Plantation, FL 33322
(954)441-6211
www.otmgm.com

Restoration Timing

OTM will use commercially reasonable efforts to restore requested data as promptly as possible after receiving a valid restoration request. Restoration services are subject to:

- Technician availability
- Availability and integrity of the requested recovery point
- Verification that the target environment is capable of receiving the restored data.

Unless expressly stated otherwise in the applicable Quote, no specific Recovery Time Objective (RTO) or Recovery Point Objective (RPO) is guaranteed.

Service Limitations

OTM is not responsible for the loss of data resulting from:

- Corrupted, incomplete, or failed backups caused by third-party hardware, software, or connectivity issues
- Unauthorized modification or deletion of backup data by the client or its agents
- Failure by the client to maintain required power, internet connectivity, environmental conditions, or physical security for onsite backup equipment
- Circumstances beyond OTM's reasonable control, including events affecting third-party backup providers

This service is intended to support business continuity and data recovery efforts but does not constitute a guarantee against all forms of data loss. No security solution, product, monitoring service, EDR, MDR, firewall, email security service, or other cybersecurity technology can prevent or detect all threats. Security logs, event data, backup records, monitoring records, and system telemetry may be retained only for the period made available by OTM or the applicable Third-Party Provider and are not guaranteed to be retained for any specific duration unless expressly stated in a Quote.

Email Threat Protection

OTM will implement, configure, and manage a cloud-based email security solution designed to protect client email environments from phishing, spam, malware, ransomware, business email compromise (BEC), account compromise, domain spoofing, and other email-borne threats.

Service Features

- Advanced threat detection
- Impersonation protection
- Display name spoofing prevention
- Malicious link and attachment analysis
- Protection from newly observed domains
- Incident response and remediation capabilities
- Mail security reporting

online
technology management, inc

1856 North Nob Hill Rd, #213
Plantation, FL 33322
(954)441-6211
www.otmgm.com

Features may vary based on the Client's selected licensing level and the capabilities of the Third-Party Provider. Security telemetry, threat intelligence, and aggregated analytics produced by Third-Party Providers remain subject to the licensing and ownership rights of the applicable provider. Security logs, event data, backup records, monitoring records, and system telemetry may be retained only for the period made available by OTM or the applicable Third-Party Provider and are not guaranteed to be retained for any specific duration unless expressly stated in a Quote. No security solution, product, monitoring service, EDR, MDR, firewall, email security service, or other cybersecurity technology can prevent or detect all threats.

Endpoint Protection and Detection/Response

Implementation, configuration, and ongoing management of an advanced Endpoint Protection (EPP) and Endpoint Detection and Response (EDR) solution utilizing related security technologies provided through our designated Third-Party Provider.

Service Features

- AI-driven threat prevention using behavioral analysis, machine learning, and autonomous protection technologies to identify and stop known and unknown threats.
- Continuous monitoring and detection of malicious, suspicious, or unauthorized activity across managed endpoints.
- Real-time prevention of malicious actions, including ransomware, malware, exploits, and other cyber threats before they can execute or spread.
- Advanced threat analysis through automated investigation and threat intelligence correlation to identify potential security incidents.
- Antivirus, anti-malware, and endpoint protection for managed laptops, desktops, servers, and supported endpoint devices.
- Protection against both file-based and fileless attacks, including malicious PowerShell, JavaScript, VBScript, macros, living-off-the-land techniques, and other advanced attack methods.
- Detection and mitigation of ransomware activity, including encryption attempts and lateral movement behaviors.
- Application control capabilities, including allow-listing and policy-based management of approved applications and scripts.
- Centralized security event visibility, alerting, and reporting through the Third-Party management platform.
- Support for automated response actions, including process termination, network isolation, and threat remediation where supported by the platform.

This service is designed to strengthen endpoint security, reduce the risk of successful cyberattacks, and provide enhanced visibility into threats affecting managed systems. Security telemetry, threat intelligence, and aggregated analytics produced by Third-Party Providers remain

1856 North Nob Hill Rd, #213
Plantation, FL 33322
(954)441-6211
www.otmgm.com

subject to the licensing and ownership rights of the applicable provider. Security logs, event data, backup records, monitoring records, and system telemetry may be retained only for the period made available by OTM or the applicable Third-Party Provider and are not guaranteed to be retained for any specific duration unless expressly stated in a Quote. No security solution, product, monitoring service, EDR, MDR, firewall, email security service, or other cybersecurity technology can prevent or detect all threats.

Managed Detection & Response

Implementation, configuration, monitoring, and management of a Managed Detection and Response (MDR) service supported by a dedicated Security Operations Center (SOC) provided through our designated Third-Party Provider. MDR combines advanced AI-driven security technology, continuous threat monitoring, proactive threat hunting, and expert security analyst oversight to detect, investigate, contain, and remediate cyber threats impacting managed systems. MDR that combines advanced technology with human expertise to provide continuous monitoring, threat hunting, incident investigation, and rapid response capabilities.

Service Features

- Deployment, configuration, and ongoing management of agents on supported workstations, servers, and other managed endpoints.
- Continuous 24x7x365 monitoring of managed endpoints by a Security Operations Center (SOC) to identify suspicious, malicious, or unauthorized activity.
- Proactive threat hunting is performed by security analysts to identify threats that may evade traditional security controls.
- AI-driven and behavioral-based threat detection designed to identify known and unknown malware, ransomware, exploits, fileless attacks, and other advanced threats.
- Real-time alert triage, investigation, validation, and classification by trained security personnel.
- Ongoing creation, maintenance, and optimization of endpoint security policies, exclusions, and protection settings.
- Continuous monitoring of endpoint, user, process, and system activity for indicators of compromise and suspicious behavior.
- Detection and prevention of malware, ransomware, credential theft attempts, unauthorized access attempts, and malicious application activity.
- Protection against file-based and fileless attacks, including malicious PowerShell, JavaScript, VBScript, macros, and living-off-the-land techniques.
- Monitoring and investigation of advanced phishing-related activity, command-and-control communications, and malicious network behaviors.
- Support for threat containment actions, including process termination, endpoint isolation, and other remediation measures supported by the platform. MDR services are designed to investigate, contain, and remediate threats as part of the response process.

1856 North Nob Hill Rd, #213
Plantation, FL 33322
(954)441-6211
www.otmgm.com

- Utilization of remediation and rollback capabilities (where supported) to assist with the recovery of systems affected by ransomware or other malicious activity. Availability and effectiveness of rollback, recovery, restoration, or remediation features are dependent upon the capabilities of the Third-Party Provider and the condition of affected systems and are not guaranteed.
- Escalation of significant security events and incidents to specialized security engineers for advanced investigation and response activities.
- Integration with supported log management, SIEM, and security monitoring platforms where applicable to provide centralized visibility into security events.
- Regular reporting, security reviews, and environment health assessments to help maintain operational effectiveness and visibility into threats, incidents, and endpoint security status.

This service is intended to provide enterprise-grade endpoint security capabilities without requiring the Customer to maintain a dedicated in-house security operations center. By combining Third-Party Provider's autonomous protection platform with 24x7 security monitoring, threat hunting, incident response, and expert analyst oversight, the service helps reduce risk, improve threat visibility, accelerate threat response, and strengthen the overall security posture of managed systems. Security telemetry, threat intelligence, and aggregated analytics produced by Third-Party Providers remain subject to the licensing and ownership rights of the applicable provider. Security logs, event data, backup records, monitoring records, and system telemetry may be retained only for the period made available by OTM or the applicable Third-Party Provider and are not guaranteed to be retained for any specific duration unless expressly stated in a Quote. No security solution, product, monitoring service, EDR, MDR, firewall, email security service, or other cybersecurity technology can prevent or detect all threats.

Managed Zero Trust/Application Allow Listing

OTM will implement, configure, monitor, and manage an application allow-listing and zero-trust security platform designed to prevent unauthorized applications, scripts, and processes from executing on managed endpoints.

Service Features

- Application allow-listing
- Ring-fencing
- Privilege management
- USB/device control
- Storage control
- Application control
- Zero trust enforcement

1856 North Nob Hill Rd, #213
Plantation, FL 33322
(954)441-6211
www.otmgm.com

This service is intended to supplement endpoint protection technologies by preventing unauthorized software, scripts, executables, and system activities from running through application allow-listing, privilege management, and zero-trust controls. Security telemetry, threat intelligence, and aggregated analytics produced by Third-Party Providers remain subject to the licensing and ownership rights of the applicable provider. Security logs, event data, backup records, monitoring records, and system telemetry may be retained only for the period made available by OTM or the applicable Third-Party Provider and are not guaranteed to be retained for any specific duration unless expressly stated in a Quote. No security solution, product, monitoring service, EDR, MDR, firewall, email security service, or other cybersecurity technology can prevent or detect all threats.

Firewall Management

Implementation, monitoring, management, and maintenance of firewall infrastructure. Acting as a critical layer of network security, firewalls help inspect and control inbound and outbound traffic, enforce security policies, and reduce the risk of cyberattacks across on-premises, cloud, and hybrid environments.

Service Features

- **Monitoring & Alerting**
  Monitoring of firewall health, network traffic, security events, and service availability.
- **Firmware & Security Update Management**
  Deployment and management of vendor-released firmware updates, security patches, and threat intelligence signature updates to help maintain system security and stability.
- **Firewall Policy Administration**
  Configuration, modification, and maintenance of firewall rules, access control policies, network objects, and related security settings in accordance with approved change requests.
- **Threat Prevention Services**
  Management and oversight of available Next-Generation Firewall (NGFW) security features, including intrusion prevention, malware protection, application control, web filtering, and encrypted traffic inspection capabilities, where supported by the deployed solution.
- **VPN & Secure Connectivity Management**
  Configuration and maintenance of site-to-site VPN connections, remote access VPN services, and other secure connectivity technologies supported by the firewall platform.
- **Security Review & Optimization**
  Periodic review of firewall configurations and security policies to identify opportunities for improved protection, performance, and policy alignment.
- **Compliance & Audit Support**
  Assistance with firewall-related reporting and documentation that may support regulatory

1856 North Nob Hill Rd, #213
Plantation, FL 33322
(954)441-6211
www.otmgm.com

or cybersecurity framework requirements, such as HIPAA, PCI DSS, or other applicable standards. Compliance-related reporting or technical assistance does not constitute legal, regulatory, audit, or certification services and should not be relied upon as evidence of regulatory compliance.

Service Delivery Models
Depending on the deployed environment, firewall management services may include:

- **On-Premises Firewall Management**
  Management of physical firewall appliances installed at customer locations.
- **Cloud Firewall Management**
  Management of virtual or cloud-native firewall solutions protecting cloud workloads, applications, and remote-access environments.
- **Co-Managed Firewall Services**
  A collaborative model in which the Client's internal IT team and OTM share management responsibilities, with OTM providing advanced administration, security monitoring, and escalation support.

Exclusions
Unless expressly included in the Quote, services do not include the procurement, licensing, replacement, or warranty coverage of firewall hardware, software subscriptions, internet connectivity services, or after-hours project work. Major firewall redesigns, network architecture changes, or migrations are subject to separate scoping and fees. Security telemetry, threat intelligence, and aggregated analytics produced by Third-Party Providers remain subject to the licensing and ownership rights of the applicable provider. Security logs, event data, backup records, monitoring records, and system telemetry may be retained only for the period made available by OTM or the applicable Third-Party Provider and are not guaranteed to be retained for any specific duration unless expressly stated in a Quote. No security solution, product, monitoring service, EDR, MDR, firewall, email security service, or other cybersecurity technology can prevent or detect all threats.

Helpdesk Services

Centralized point of contact for technology support and service requests. Through remote assistance channels, our technicians work to resolve day-to-day IT issues, restore productivity, and provide guidance on supported systems, applications, and services.
Support requests may be submitted through approved communication channels, including telephone, email, and customer portal. Service availability and coverage hours are provided as specified in the applicable Quote or MSA.

Service Features
User & Identity Management

1856 North Nob Hill Rd, #213
Plantation, FL 33322
(954)441-6211
www.otmgm.com

- Password reset assistance and account recovery support.
- Assistance with multi-factor authentication (MFA) enrollment, synchronization, and lockout issues.
- User onboarding and offboarding activities, including account creation, modification, and deactivation.
- Assignment and management of approved software licenses and user access permissions.

Workstation & Endpoint Support

- Troubleshooting of supported desktop and laptop operating systems.
- Diagnosis and resolution of performance issues, application errors, and device configuration problems.
- Remote support sessions to investigate and remediate end-user issues.
- Installation and configuration of approved business applications and updates.

Microsoft 365 & Cloud Services Support

- Support for Microsoft 365 services, including Outlook, Teams, OneDrive, SharePoint, and related applications.
- Assistance with email access, mailbox configuration, collaboration tools, and file synchronization issues.
- Basic troubleshooting of approved cloud-based business applications and services.

Network Connectivity & Remote Access Support

- Troubleshooting of end-user connectivity issues involving local networks, wireless networks, and internet access.
- Support for approved VPN and remote access solutions.
- Assistance with access to network resources and business applications.

Service Delivery

Ticket Management

All service requests, incidents, and support activities are documented and tracked through our service management platform. Tickets are prioritized, assigned, and managed according to established service procedures and applicable service level objectives.

Remote Monitoring & Management

Where applicable, support services may be supplemented by Remote Monitoring and Management (RMM) tools to facilitate proactive issue identification, device health monitoring, automated maintenance activities, and remote remediation efforts.

Escalation Management

Issues requiring advanced expertise may be escalated to specialized engineering, infrastructure, cloud, cybersecurity, or vendor support resources. Escalations are managed in accordance with established operational procedures.

Service Levels

Response and resolution objectives may vary based on incident priority, service impact, and the support plan selected by the Client. Applicable service levels are defined within the Quote, MSA, or related service documentation.

1856 North Nob Hill Rd, #213
Plantation, FL 33322
(954)441-6211
www.otmgm.com

Exclusions
Unless otherwise specified in a Quote, Help Desk Services do not include:

- Custom software development or application programming.
- OTM reserves the right to deny support for hardware, operating systems, applications, firmware, or cloud services that have reached end-of-life, end-of-support, or end-of-security-support status.
- Vendor-specific support beyond commercially reasonable troubleshooting and coordination efforts.
- On-site support visits.
- Project-based services, migrations, deployments, or major configuration changes.
- Training services or end-user education beyond reasonable issue resolution assistance.

Support for third-party applications, devices, and services may be provided on a commercially reasonable effort basis and are subject to vendor limitations, additional fees, or separate scoping requirements.

Software Licensing and Acceptable Use

Certain software applications, cloud services, subscriptions, platforms, and related technologies provided, managed, supported, or facilitated by OTM ("**Software**") are licensed to the Client and are not sold. Use of all Software is subject to the terms, conditions, licensing requirements, End User License Agreements ("**EULAs**"), Acceptable Use Policies ("**AUPs**"), subscription agreements, and other requirements established by the applicable software publisher, vendor, or service provider ("**Third-Party Provider**").
As part of delivering the Services, OTM may procure, install, configure, deploy, manage, or administer Software and related subscriptions on the Client's behalf. The Client authorizes OTM to accept, acknowledge, or agree to applicable EULAs, AUPs, subscription terms, and other licensing agreements as the Client's authorized agent when such acceptance is necessary to provision, implement, maintain, or support the Software.

Certain Services may require the purchase of software subscriptions or licenses on a per-user, per-device, per-mailbox, per-asset, or similar basis ("**Access Licenses**"). Examples include Microsoft New Commerce Experience (NCE) subscriptions, and other third-party software or cloud service subscriptions. Access Licenses are often non-cancelable, non-refundable, and non-transferable once ordered or committed. Accordingly, the Client remains responsible for all fees associated with Access Licenses and other committed software subscriptions for the full applicable subscription, licensing, or contract term, regardless of whether the associated Services are terminated, suspended, reduced, or otherwise discontinued prior to the end of such term.

The Client is responsible for ensuring that its employees, contractors, agents, and authorized users comply with all applicable Software licensing requirements, usage restrictions, and

1856 North Nob Hill Rd, #213
Plantation, FL 33322
(954)441-6211
www.otmgm.com

acceptable use standards. The Client shall not permit any unauthorized use, copying, sharing, transfer, sublicensing, circumvention of licensing controls, or other activity that violates the terms established by the applicable Third-Party Provider. Any penalties, fees, claims, damages, or liabilities arising from the Client's failure to comply with applicable licensing or acceptable use requirements shall be the sole responsibility of the Client.

Failure to comply with applicable licensing or acceptable use requirements may result in the suspension, restriction, or termination of Software access by the Third-Party Provider and may adversely affect OTM's ability to provide related Services.

Unless otherwise stated, all Software provided, supported, or facilitated under the Services should be presumed to be subject to one or more EULAs, AUPs, subscription agreements, or similar contractual requirements. Copies of applicable licensing terms may be available directly from the Third-Party Provider or through OTM upon request.

OTM shall not be responsible for any licensing restrictions, feature changes, service interruptions, subscription limitations, pricing changes, compliance obligations, or other actions imposed by Third-Party Providers. Provided that all applicable licensing fees have been paid in full, the Client may continue to use any Access Licenses through the end of their applicable subscription or licensing term, subject to the terms and conditions of the applicable Third-Party Provider.

Breach/Cyber Security Incident Recovery

Unless expressly included in a Quote, Statement of Work, or other written agreement, the Services do not include incident response, forensic investigation, remediation, restoration, recovery, or any other services related to a cybersecurity event, data breach, ransomware attack, malware infection, business email compromise, unauthorized access incident, or other security-related event (collectively, a "**Security Incident**").

If requested by the Client, OTM may provide assistance with the investigation, containment, remediation, recovery, restoration, or coordination of a Security Incident on a time-and-materials basis at OTM's then-current rates and subject to resource availability. Such services may require the involvement of third-party vendors, security specialists, manufacturers, software providers, cyber insurance carriers, legal counsel, or other external resources, the costs of which shall be the Client's responsibility unless otherwise agreed in writing.

Due to the unique nature and severity of Security Incidents, OTM does not warrant, guarantee, or represent that any Security Incident can be fully remediated, that recovery efforts will be successful, or that all affected systems, applications, configurations, data, or services can be restored to their pre-incident condition. OTM further makes no guarantee regarding the time

1856 North Nob Hill Rd, #213
Plantation, FL 33322
(954)441-6211
www.otmgm.com

required to investigate, remediate, recover from, or restore operations following a Security Incident.

For purposes of this Agreement, a "Security Incident" includes any actual, suspected, attempted, or successful unauthorized access to, use of, disclosure of, alteration of, destruction of, encryption of, or interference with the Client's systems, network, applications, accounts, data, credentials, or technology environment. A Security Incident also includes any event that compromises, or is reasonably believed to compromise, the confidentiality, integrity, availability, or security of the Client's information or technology environment, or that disrupts normal business operations or access to systems and services.

The Client acknowledges that cybersecurity risk cannot be completely eliminated and that no security product, monitoring service, or managed service can guarantee protection against all Security Incidents, cyber threats, or data loss events. The Client remains responsible for maintaining appropriate cyber liability insurance, security policies, user awareness training, and compliance with applicable security requirements unless such services are expressly included within the Services. Security Incident response services are excluded unless expressly included in a Quote, Statement of Work, or Incident Response Agreement. No security solution, product, monitoring service, EDR, MDR, firewall, email security service, or other cybersecurity technology can prevent or detect all threats.

Service Levels

Response
OTM will use commercially reasonable efforts that OTM will provide the Requested Services, and reasonably respond to any notification received by OTM of any error, outage, alarm or alert pertaining to the System, in the manner defined in the applicable MSA except for (i) periods of delay caused by Client

Downtime (defined below), Vendor-Side Downtime (defined below) or (ii) periods in which OTM is required to suspend the Services to protect the security or integrity of Client System or OTM's equipment or network, or (iii) delays caused by a force majeure event. Any response times stated herein are goals and not guarantees unless expressly identified as service credits in an applicable Quote.

Scheduled Downtime
For the purposes of this Service Guide, Scheduled Downtime will mean those hours, as determined by OTM which will not occur between the OTM's normal business hours of 8:30 AM and 5:30 PM (Eastern) Monday through Friday without Client authorization or unless exigent circumstances exist, during which time OTM will perform scheduled maintenance or adjustments to Client System. OTM will use its commercially reasonable efforts to provide Client with at least twenty-four (24) hours of notice prior to scheduling Scheduled Downtime.

1856 North Nob Hill Rd, #213
Plantation, FL 33322
(954)441-6211
www.otmgm.com

Client Downtime
OTM will not be responsible under any circumstances for any delays or deficiencies in the provision of, or access to, the Requested Services to the extent that such delays or deficiencies are caused in whole or in part by Client acts or omissions ("**Client Downtime**").

Vendor-Side Downtime
OTM will not be responsible under any circumstances for any delays or deficiencies in the provision of, or access to, the Requested Services to the extent that such delays or deficiencies are caused by Third-Party Service Providers, Third-Party Product Providers, third-party licensors, or "upstream" service or Product vendors. Client and OTM expressly agree that this Section of the Service Guide is intended to be interpreted as broadly as possible under applicable law.

Availability & Hours of Operation

"Business Hours" means Monday through Friday, 8:30 a.m. through 5:30 p.m. Eastern Time, excluding OTM-observed holidays.

Day	Time	Availability
Monday – Friday	8:30 AM – 5:30 PM	Unlimited remote service.

Support During Off-Hours/Non-Business Hours
Technical support provided outside of our normal business hours is offered on a case-by-case basis and is subject to technician availability. Non-Business Hour Support will be provided on a time and materials basis (which is not covered under any Service plan), and will be billed to Client at 1.5x our then-current hourly rate.

All hourly services are billed in 15-minute increments, and partial increments are rounded to the next highest increment. A one (1) hour minimum applies to all Non-Business Hour Support.

Observed Holidays

- New Year's Day
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving Day
- The day following Thanksgiving Day
- Christmas Eve – Half Day

1856 North Nob Hill Rd, #213
Plantation, FL 33322
(954)441-6211
www.otmgm.com

- Christmas Day
- New Year's Eve – Half Day

Priority Levels for Support

Automated monitoring is provided on an ongoing (*i.e.*, 24x7x365) basis. Response, repair, and/or remediation services (as applicable) will be provided only during our business hours (currently M-F, 8:30 AM to 5:30 PM Eastern Time, excluding legal holidays and OTM-observed holidays as listed above), unless otherwise specifically stated in the Quote or as otherwise described below.

OTM will respond to problems, errors, or interruptions in the provision of the Services during business hours in the timeframe(s) described below. Severity levels will be determined by OTM discretion after consulting with the Client. All remediation services will initially be attempted remotely; onsite service only if remote remediation is ineffective and, under all circumstances, only if covered under the Service plan selected by Client.

Description	Priority	Response
All users and functions unavailable.	Critical	Within two (2) business hours after notification
Large number of users or business critical functions.	Significant Degradation	Response within four (4) business hours after notification.
Limited number of users or functions affected, business process can continue.	Limited Degradation	Response within eight (8) business hours after notification.
Business process can continue one user affected	Small Service Degradation	Response within two (2) business days after notification.

* All time frames are calculated as of the time that we are notified of the applicable issue / problem by Client through our designated support methods:

- Email: support@otmgm.com
- Phone: (954)441-6211 Option: 2

Notifications received in any manner other than described herein may result in a delay in the provision of remediation efforts.