MANAGED IT AND SECURITY SERVICES CATALOG

TABLE OF CONTENTS

General Services 3

Part I. Managed IT Services 4

Service Management 4

MIT-01 Service Desk and Ticket Management 4
MIT-02 Account Management and Service Reviews 4
MIT-03 Asset and Inventory Management 5
MIT-04 Procurement, Vendor, and Third-Party Management 5
MIT-05 General Support Requests 6

Workstation and End User Services 6

MIT-06 Workstation and End User Support 6
MIT-07 Workstation Configuration and Deployment 7
MIT-08 Workstation Hardware Support 7
MIT-09 Workstation Operating System Management 7
MIT-10 Software Deployment Management 8
MIT-11 Remote Monitoring, Access, and Platform 8
MIT-12 Peripheral Support 9
MIT-13 Tablet Support 9
MIT-14 Line-of-Business Application Support 9
MIT-15 Microsoft 365 Administration 10
MIT-16 Endpoint Antivirus and Anti-Malware 10
MIT-17 DNS and Web Filtering 11

Identity and Access Services 11

MIT-18 User Lifecycle Administration 11
MIT-19 Access and Group Administration 12
MIT-20 Privileged Access Administration 12

Server and Cloud Services 12

MIT-21 Server Monitoring and Alerting 12
MIT-22 Server Operating System Maintenance 13
MIT-23 Server Incident Support 13
MIT-24 Server Configuration Management 14
MIT-25 Server Backup Monitoring and Routine Restoration 14
MIT-26 Cloud Infrastructure Management 14
MIT-27 Directory and Core Infrastructure Services 15

Network Services 15

MIT-28 Network Monitoring and Alerting 15
MIT-29 Network Device Maintenance 15
MIT-30 Network and Circuit Incident Support 16
MIT-31 Network Configuration Management 16

Communications Services 16

MIT-34 Cloud VoIP System Support 16
MIT-35 Call Flow Administration 17
MIT-36 Contact Center Support 17
MIT-37 E-Fax and Analog Adapter Support 17

Print Services 18

MIT-38 Printer Connectivity Support 18
MIT-39 Print Management Platform Administration 18
MIT-40 Printer Supply Monitoring 18
Onsite Services 18
MIT-41 Onsite Dispatch Support 18
MIT-42 Scheduled Onsite Technical Resource 19
Specialized Healthcare Technology Services 19
MIT-43 Biomedical Device Connectivity Support 19
MIT-44 Medical Imaging Systems Support 20
MIT-45 Security System Connectivity Support 20
Part II. Managed Security Services 21
Identify 21
MSS-01 Vulnerability Management 21
MSS-02 Attack Surface Management 21
Protect 22
MSS-03 End User Protection 22
MSS-04 Endpoint Protection Platform (EPP) 22
MSS-05 Identity Protection and Conditional Access 23
Detect and Respond 23
MSS-06 Managed Detection and Response (MDR) 23
MSS-07 Security Incident Response 24
Govern 24
MSS-08 Security Governance, Risk, and Compliance (GRC) 24
MSS-09 Security Policy Management 25
MSS-10 Third-Party Risk Management 25
Part III. Fractional Executive Services 27
FXS-01 Fractional Executive Services (CIO, CTO, CISO) 27
Glossary 30

GENERAL SERVICES

The following apply to every service in this Catalog unless the service or the SOW states otherwise.

Delivery. Services are delivered remotely during Business Hours.

Customer Responsibilities

- Maintain the hardware, software, licensing, subscriptions, warranties, and manufacturer, vendor, carrier, and lease agreements that covered services require, other than those provided by Focus

Exclusions from Focus' Scope of Work

- Work on unsupported or uncovered systems, devices, operating systems, services, or locations
- Project Services and project management, including new implementations, deployments, builds, migrations, major upgrades, redesigns, and large-scale refreshes
- Hardware, parts, consumables, and replacement devices, and physical or component-level repair
- Custom software development, application packaging, and custom integrations
- Full system or environment rebuilds and disaster recovery execution
- Digital forensics, breach counsel, and regulatory or individual breach notification
- Legal, regulatory, compliance, HR, and employment advice or decisions, and independent audits, attestations, or certifications
- Carrier, vendor, and other third-party charges, and negotiation of Customer's third-party contracts
- Construction, electrical, and cabling work
- Guarantees of availability, performance, security, compliance, or business outcomes
- Non-IT duties

PART I. MANAGED IT SERVICES

Managed IT Services keep your workforce productive and your environment stable, maintained, and documented. Services are grouped by area.

SERVICE MANAGEMENT

MIT-01 Service Desk and Ticket Management

Service Description. Centralized intake, prioritization, escalation, tracking, communication, and closure of covered Incidents and Requests.

Standard Inclusions

- Customer-accessible support portal for submitting and tracking tickets
- Intake through approved phone, email, chat, and portal channels
- Prioritization of Incidents using the priority definitions in the SLA
- Ticket routing, escalation, status updates, documentation, and closure
- After-hours emergency intake through the designated after-hours method

Delivery. Remote, during Business Hours. After-hours emergencies are reported through the designated after-hours method; after-hours work is billed at the rates stated in the SOW.

Service Boundaries. Requests are handled under the applicable support schedule. After-hours emergencies must be reported through the designated after-hours method (by phone). Requests sent by email or portal outside Business Hours are handled on the next Business Day. Response and resolution targets are stated only in the SLA.

Customer Responsibilities

- Submit requests through approved channels rather than contacting individual Focus personnel directly
- Include the affected User, device, symptoms, and business impact so the request can be prioritized correctly
- Use the phone channel for urgent issues and after-hours emergencies

Exclusions

- Business-process consulting
- Use of a Customer-specific or other third-party ticketing platform

MIT-02 Account Management and Service Reviews

Service Description. Operational oversight of service performance, support trends, technology lifecycle, risks, and recommendations.

Standard Inclusions

- Designated Client Success contact
- Business reviews at the cadence stated in the SOW, typically a Quarterly Business Review (QBR) covering ticket trends, SLA performance, patch compliance, asset lifecycle, and open recommendations, and an Annual Business Review (ABR) covering the year's performance and planned technology priorities
- Coordination of material escalations

Delivery. Remote or onsite as agreed, on the cadence stated in the SOW.

Service Boundaries. Review cadence and standard reporting are defined in the SOW. Recommendations are advisory, and Customer decides whether to adopt and fund them.

Customer Responsibilities

- Make a decision-maker available for scheduled reviews
- Share business plans that affect technology needs, such as new sites, new service lines, staffing changes, or new applications
- Respond to recommendations with a decision or a documented deferral

Exclusions

- Virtual CIO services unless stated in the SOW
- Fractional Executive Services (FXS-01)
- Custom reporting outside the standard review package

MIT-03 Asset and Inventory Management

Service Description. Collection and maintenance of inventory information for covered hardware and software.

Standard Inclusions

- Automated hardware and software inventory through Focus's standard remote monitoring and management (RMM) platform
- Device details such as model, serial number, operating system, and installed software, as reported by the management agent
- Warranty and lifecycle information when available from the manufacturer
- Inventory reporting as part of service reviews

Delivery. Automated collection; reporting during Business Hours.

Service Boundaries. Inventory depends on installed agents and device connectivity. It is not a physical audit, and devices without an agent are not inventoried.

Customer Responsibilities

- Tell Focus about devices purchased outside Focus so they can be enrolled
- Report lost, stolen, or retired devices promptly

Exclusions

- Financial or fixed-asset accounting
- Use of a Customer-specific or third-party RMM solution

MIT-04 Procurement, Vendor, and Third-Party Management

Service Description. Assistance with sourcing, quoting, ordering, tracking, and warranty coordination, plus coordination with covered third-party vendors. This service is subject to Section 2, "Procurement, Vendor Management, and Third-Party Products," of the Managed IT – Supplemental Terms and Conditions.

Standard Inclusions

- Product recommendations aligned to Focus technology standards
- Quote preparation
- Order placement and tracking
- Vendor and warranty coordination for products/services per Focus agreement

Service Boundaries. Ordering does not include setup, deployment, or installation. Those are covered by the applicable service or as Project Services. Items Focus purchases on Customer's behalf are subject to the pricing methodology and fees in Section 2.5, "Procurement and Administrative Fees," of the Managed IT – Supplemental Terms and Conditions and Section 5, "Procurement and Vendor Management Pricing," of the SOW.

Customer Responsibilities

- Approve quotes and purchases in writing through an authorized approver
- Talk to Focus before buying technology elsewhere. Products bought outside Focus may need onboarding or validation, or may have support limits.

Exclusions

- Product, freight, tax, licensing, and warranty costs
- Deployment unless stated

MIT-05 General Support Requests

Service Description. Routine, Customer-authorized support requests related to the covered environment that are not otherwise classified under a specific service in this Catalog.

Standard Inclusions

- Routine requests related to covered Users, devices, and systems, each requiring no more than 120 minutes of labor
- Guidance on supported technology questions

Service Boundaries. Limited to routine requests that do not introduce new capability, change the environment materially, or need planning (see the project thresholds in the SOW). Focus determines classification and may treat a request as T&M or as Project Services. Work that meets the Project Services definition is scoped separately.

Customer Responsibilities

- Submit requests through the service desk with enough detail to assess the scope

WORKSTATION AND END USER SERVICES

MIT-06 Workstation and End User Support

Service Description. Remote support for covered Users, Workstations, standard configurations, supported operating systems, and approved applications.

Standard Inclusions

- Remote troubleshooting of supported operating system issues
- Sign-in, profile, settings, performance, printing, and connectivity support
- Routine troubleshooting of approved applications
- Answers to routine how-to questions about supported technology

Service Boundaries. Services are primarily remote and limited to covered Users and supported devices. Issues caused by unsupported software or hardware are handled on a reasonable-efforts basis and may require remediation first.

Customer Responsibilities

- Make the affected User and device available during troubleshooting

- Keep devices powered on and connected so they can receive support and updates

Exclusions

- Formal training
- Personal devices unless covered
- Data recovery

MIT-07 Workstation Configuration and Deployment

Service Description. Remote configuration and deployment of approved standard Workstations.

Standard Inclusions

- Standard operating system configuration
- Domain or Microsoft Entra ID enrollment
- Deployment of approved standard software
- Application of standard security and management policies
- Enrollment in Focus management and security platforms

Service Boundaries. Quantities, staging, shipping, data transfer, and onsite work must be stated in the SOW. Large or coordinated refreshes are Project Services.

Customer Responsibilities

- Give advance notice of new hires and device needs
- Confirm the software and access each new device needs

Exclusions

- Custom images

MIT-08 Workstation Hardware Support

Service Description. Remote diagnosis and coordination related to covered Workstation hardware failures.

Standard Inclusions

- Hardware diagnostics
- Failure assessment
- Warranty claim coordination with the manufacturer
- Repair-or-replace recommendations

Delivery. Remote, during Business Hours. Onsite work as described in MIT-41.

Service Boundaries. Physical repair and replacement depend on warranties, parts, location, and onsite coverage. Replacement parts and hardware are billed separately.

Customer Responsibilities

- When asked, provide simple onsite help such as checking cables or power

Exclusions

- Accidental damage

MIT-09 Workstation Operating System Management

Service Description. Administration, support, security patching, and approved feature updates for covered Workstation operating systems.

Standard Inclusions

- Automated security patch deployment within Customer-approved maintenance windows
- Approved feature updates
- Patch compliance monitoring and reporting
- Operating system troubleshooting

Delivery. Automated deployment within approved windows; remediation during Business Hours.

Service Boundaries. Updates follow approved maintenance policies and may require a restart or vendor validation. Devices must be powered on and connected to receive updates. Operating system upgrades that require hardware replacement are Project Services.

Customer Responsibilities

- Approve maintenance windows and restart policies
- Have application vendors confirm compatibility with operating system updates when needed
- Retire or upgrade devices running unsupported operating systems

Exclusions

- Compatibility remediation

MIT-10 Software Deployment Management

Service Description. Administration of automated deployment policies for approved software through RMM catalog for applications agreed upon contractually referred to as “supported packages” throughout.

Standard Inclusions

- Standard deployment policy maintenance
- Deployment monitoring
- Troubleshooting of supported packages

Service Boundaries. Only supported and approved applications are eligible. Packaging new or custom applications is Project Services.

Customer Responsibilities

- Approve software for deployment
- Provide installation media and vendor guidance for line-of-business software

Exclusions

- Custom application packaging (available as Project Services)

MIT-11 Remote Monitoring, Access, and Platform

Service Description. Administration of Focus's remote monitoring and management capabilities.

Standard Inclusions

- Management agent deployment
- Secure remote support access
- Standard alert and policy administration

Delivery. Automated; administration during Business Hours.

Service Boundaries. The platform is a delivery tool and does not expand any other service. It is included when the RMM platform is licensed through Focus.

Customer Responsibilities

- Allow agent installation on covered devices
- Do not remove or disable Focus agents

MIT-12 Peripheral Support

Service Description. Connectivity, driver, software, and routine support for covered Peripherals.

Standard Inclusions

- Support for printers, scanners, webcams, card readers, signature pads, label printers, barcode readers, and similar peripherals connected to a Workstation that are not regulated medical devices
- Driver configuration
- Connectivity troubleshooting
- Vendor coordination

Service Boundaries. Support for vendor-maintained and specialized devices, such as leased copiers and medical devices, is limited to connectivity triage.

Customer Responsibilities

- Use models that are supported on current operating systems

Exclusions

- Biomedical servicing

MIT-13 Tablet Support

Service Description. Configuration, connectivity, management-platform, and routine support for covered Tablets.

Standard Inclusions

- Management platform enrollment
- Connectivity support
- Approved mobile app support
- Standard policy administration, including remote lock and wipe where the platform supports it

Service Boundaries. Support is limited to approved models, operating system versions, ownership models, and applications, and requires a covered mobile device management platform such as Microsoft Intune.

Customer Responsibilities

- Report lost or stolen Tablets immediately

Exclusions

- Consumer-account recovery

MIT-14 Line-of-Business Application Support

Service Description. First-line troubleshooting and vendor coordination for designated applications, such as EHR, document, and dictation software.

Standard Inclusions

- Initial triage
- Access validation
- Client-side troubleshooting
- Vendor ticket coordination

Service Boundaries. Designated applications are identified in the SOW or onboarding documentation. Resolution may depend on the vendor and an active third-party support agreement.

Customer Responsibilities

- Authorize Focus to act as a technical contact with application vendors
- Designate application administrators for configuration and workflow decisions

Exclusions

- Database administration

MIT-15 Microsoft 365 Administration

Service Description. Routine administration and user support for covered Microsoft 365 workloads.

Standard Inclusions

- Exchange Online administration
- Teams administration
- OneDrive support
- SharePoint access and permissions
- Intune administration when covered
- License assignment

Service Boundaries. What Focus can do depends on Customer licensing and on the workloads identified in the SOW. Tenant security policies such as multi-factor authentication and conditional access are covered under MSS-05.

Customer Responsibilities

- Approve access to shared mailboxes, sites, and data

Exclusions

- SharePoint design

MIT-16 Endpoint Antivirus and Anti-Malware

Service Description. Deployment, policy management, and alert handling for Focus-provided endpoint antivirus and anti-malware on covered Workstations and Servers.

Standard Inclusions

- Agent deployment to covered devices
- Standard protection policy administration
- Alert review and routine remediation
- Protection status reporting

Delivery. Automated protection; alert handling during Business Hours unless MSS-06 is purchased.

Service Boundaries. Included when the endpoint protection platform is licensed through Focus. Investigation beyond routine alert handling is covered under MSS-06 and MSS-07 when purchased. Otherwise it is billed on a T&M basis.

Customer Responsibilities

- Do not disable or uninstall protection agents
- Report suspicious activity to the service desk

Exclusions

- Incident response and forensic investigation
- Recovery of data lost to malware

MIT-17 DNS and Web Filtering

Service Description. Administration of Focus-provided DNS-layer web filtering policies for covered Users and devices.

Standard Inclusions

- Filtering agent or network deployment
- Standard security and content category policy administration
- Allow and block list changes on authorized request
- Filtering reports

Delivery. Automated filtering; administration during Business Hours.

Service Boundaries. Included when the filtering platform is licensed through Focus. Filtering reduces exposure to known malicious destinations. It does not block every malicious or inappropriate site.

Customer Responsibilities

- Approve content-category policies and exceptions
- Ask for allow-list changes through the service desk

Exclusions

- Monitoring of individual browsing for HR purposes

IDENTITY AND ACCESS SERVICES

MIT-18 User Lifecycle Administration

Service Description. Administration of authorized user accounts in covered identity platforms.

Standard Inclusions

- Onboarding, modification, disablement, and offboarding
- User account administration in Active Directory and Microsoft Entra ID
- Standard license assignment
- Mailbox and file handling at offboarding according to Customer instructions

Delivery. Remote, during Business Hours. Urgent terminations should be phoned in.

Service Boundaries. Requests must come from authorized requesters. Focus does not determine employment status.

Customer Responsibilities

- Submit onboarding requests in advance, with role and access requirements
- Notify Focus of terminations promptly, and immediately for involuntary terminations
- Decide how a departing User's data and mailbox are handled

MIT-19 Access and Group Administration

Service Description. Administration of approved password resets, groups, and permissions, and support for User enrollment in multi-factor authentication.

Standard Inclusions

- Password resets with identity verification
- Group membership changes
- Routine permission changes
- Multi-factor authentication (MFA) enrollment support

Service Boundaries. Access is granted only on valid Customer authorization. Conditional access policy design is covered under MSS-05.

Customer Responsibilities

- Define who may approve access to each system
- Review access periodically and request removals

Exclusions

- Entitlement engineering

MIT-20 Privileged Access Administration

Service Description. Administration of designated privileged accounts, roles, and approved access assignments.

Standard Inclusions

- Privileged account maintenance
- Approved role assignment and removal
- Scheduled access review support

Service Boundaries. Customer retains privileged-access approval and risk-acceptance authority. In Co-Managed engagements, privileged-account responsibilities follow Appendix A of the SOW.

Customer Responsibilities

- Approve each privileged account and role
- Identify vendors and contractors who hold administrative access

Exclusions

- Unapproved emergency access
- Security governance

SERVER AND CLOUD SERVICES

MIT-21 Server Monitoring and Alerting

Service Description. Automated monitoring and alerting for covered on-premises and cloud-hosted Servers.

Standard Inclusions

- 24x7x365 automated monitoring
- Availability, performance, capacity, and drive-space monitoring
- Alert and ticket generation

Delivery. Automated monitoring 24x7x365. Human response during the coverage hours stated in the SLA.

Service Boundaries. Monitoring and alerting are automated 24x7x365. Human response occurs during the alert-response hours stated in the SLA, and remediation outside Business Hours is billed at the rates stated in the SOW unless the SOW includes it. Only onboarded and reachable Servers are covered.

Customer Responsibilities

- Notify Focus of planned shutdowns and maintenance
- Maintain power protection and connectivity for on-premises Servers

Exclusions

- Application performance management unless stated

MIT-22 Server Operating System Maintenance

Service Description. Security patching and routine operating system maintenance for covered Servers.

Standard Inclusions

- Automated security patching within Customer-approved maintenance windows
- Patch compliance monitoring
- Routine operating system maintenance

Delivery. Automated within approved windows; remediation during Business Hours.

Service Boundaries. Application compatibility testing and vendor certification remain Customer or vendor responsibilities.

Customer Responsibilities

- Approve maintenance windows
- Ask application vendors to confirm patch compatibility when needed

Exclusions

- Application remediation

MIT-23 Server Incident Support

Service Description. Diagnosis and restoration of failed covered Servers and server services.

Standard Inclusions

- Incident diagnosis
- Service restoration during covered hours
- Vendor escalation
- Routine operating system recovery actions

Delivery. Remote, during Business Hours. After-hours work is billed at the rates stated in the SOW.

Service Boundaries. Recovery depends on available backups, licenses, hardware, documentation, and vendor support. Charges from Microsoft or other vendor support are billed to Customer.

Customer Responsibilities

- Provide decision-makers for restoration priorities during a major outage

Exclusions

- Data-center relocation

MIT-24 Server Configuration Management

Service Description. Approved configuration changes to covered Servers and standard server roles.

Standard Inclusions

- Routine Active Directory, Group Policy, DNS, DHCP, file, and print changes
- Configuration of existing supported roles

Service Boundaries. New builds, migrations, upgrades, and material redesigns are Project Services.

Customer Responsibilities

- Authorize changes and confirm business requirements

MIT-25 Server Backup Monitoring and Routine Restoration

Service Description. Monitoring and verification of covered backup jobs, and routine restore support.

Standard Inclusions

- Backup-job monitoring
- Failed-job remediation
- Routine verification of backup completion
- File-level restoration on authorized request
- Recommend backup retention scope and durations

Delivery. Automated monitoring; remediation and restores during Business Hours.

Service Boundaries. A successful job status does not guarantee that every item can be recovered. Backup licensing and storage are separate. Full-system recovery and disaster recovery execution are billed on a T&M basis unless included in the SOW.

Customer Responsibilities

- Approve Focus's recommendations for what data must be protected and for how long
- Notify Focus of new systems or data locations that need backup
- Maintain backup storage

Exclusions

- Business continuity planning

MIT-26 Cloud Infrastructure Management

Service Description. Administration and support of covered cloud compute, storage, networking, platform, and serverless resources.

Standard Inclusions

- Administration of identified cloud resources
- Monitoring and routine configuration
- Virtual machine, storage, and cloud-network support

Service Boundaries. The SOW must identify covered subscriptions, tenants, resource types, and responsibilities. Cloud consumption charges are billed as described in the SOW.

Customer Responsibilities

- Maintain cloud subscriptions and approve consumption-affecting changes, unless purchased through Focus.

Exclusions

- Application modernization

MIT-27 Directory and Core Infrastructure Services

Service Description. Routine administration of covered directory and core network services.

Standard Inclusions

- Active Directory and Group Policy administration
- DNS and DHCP administration
- File and print role administration

Service Boundaries. Material restructuring or legacy remediation may require Project Services.

Customer Responsibilities

- Authorize changes to directory structure and policies

Exclusions

- Application-specific engineering

NETWORK SERVICES

MIT-28 Network Monitoring and Alerting

Service Description. Automated monitoring and alerting for covered Network Devices and circuits.

Standard Inclusions

- 24x7x365 automated availability and health monitoring
- Alert and ticket generation
- Monitoring of covered devices and circuits

Delivery. Automated monitoring 24x7x365. Human response during the coverage hours stated in the SLA.

Service Boundaries. Human remediation occurs during covered hours and requires supported devices and credentials.

Customer Responsibilities

- Provide administrative credentials

MIT-29 Network Device Maintenance

Service Description. Routine firmware, configuration-backup, and health management for covered Network Devices.

Standard Inclusions

- Firmware maintenance
- Configuration backup where supported
- Health checks
- Lifecycle recommendations

Delivery. Remote, within maintenance windows.

Service Boundaries. Devices must be under active manufacturer support. Maintenance windows apply.

Customer Responsibilities

- Approve maintenance windows

MIT-30 Network and Circuit Incident Support

Service Description. Troubleshooting network connectivity, failed devices, and internet service provider circuit issues.

Standard Inclusions

- Network connectivity diagnosis
- Failed-device troubleshooting
- Carrier escalation
- Restoration of existing configurations

Delivery. Remote, during Business Hours. Onsite as described in MIT-41.

Service Boundaries. Carrier and vendor repair times are outside Focus's control. Signal levels for wireless coverage not guaranteed; physical conditions may need an onsite assessment.

Customer Responsibilities

- Give carriers site access when needed
- Authorize Focus as a technical contact with each carrier, including a letter of authorization where the carrier requires one
- Report wireless coverage issues

MIT-31 Network Configuration Management

Service Description. Approved changes to existing firewall, routing, switching, VLAN, and wireless configurations.

Standard Inclusions

- Firewall rule changes
- VLAN and switch changes
- Routing updates
- Wireless setting changes

Delivery. Remote, during Business Hours or within approved windows.

Service Boundaries. New sites, major segmentation, redesign, and large-scale replacements are Project Services.

Customer Responsibilities

- Authorize changes and identify the business purpose of each rule

COMMUNICATIONS SERVICES

MIT-34 Cloud VoIP System Support

Service Description. Routine support for covered cloud VoIP systems.

Standard Inclusions

- Platform and handset troubleshooting
- Extension and user support
- Call-quality triage
- Vendor coordination

Service Boundaries. Platform and carrier outages may require vendor resolution.

MIT-35 Call Flow Administration

Service Description. Routine changes to existing call-routing configurations.

Standard Inclusions

- Auto-attendant, hunt group, queue, extension, and schedule changes
- Holiday routing updates

Service Boundaries. Complex redesigns, integrations, and mass changes may be Project Services.

Customer Responsibilities

- Submit holiday and schedule changes in advance
- Provide recorded greetings or approve scripts

MIT-36 Contact Center Support

Service Description. Routine operational support for covered contact-center platforms.

Standard Inclusions

- Agent and supervisor support
- Existing queue and configuration support
- Routine reporting assistance
- Vendor coordination

Service Boundaries. The SOW must identify the platform, features, user groups, and responsibilities.

Customer Responsibilities

- Designate a platform owner

Exclusions

- Process redesign

MIT-37 E-Fax and Analog Adapter Support

Service Description. Routine support for covered e-fax platforms and analog telephone adapters (ATAs).

Standard Inclusions

- User and connectivity troubleshooting
- ATA configuration support
- Vendor and carrier coordination

Service Boundaries. Transmission success may depend on third parties and device compatibility.

PRINT SERVICES

MIT-38 Printer Connectivity Support

Service Description. Network, driver, queue, and user-connectivity support for covered printers.

Standard Inclusions

- Printer configuration
- Driver deployment
- Queue support
- User printing troubleshooting

Service Boundaries. Mechanical repair is not included. Leased devices are limited to connectivity triage.

MIT-39 Print Management Platform Administration

Service Description. Administration of covered print-management software.

Standard Inclusions

- Platform administration
- Automated driver deployment
- Queue administration
- Routine troubleshooting

Service Boundaries. What the platform can do depends on licensing, compatibility, and connectivity.

Customer Responsibilities

- Maintain platform licensing unless purchased from Focus.

MIT-40 Printer Supply Monitoring

Service Description. Automated monitoring and notification of toner or ink status where supported.

Standard Inclusions

- Supply-level monitoring
- Standard notifications
- Platform troubleshooting

Delivery. Automated.

Service Boundaries. Accuracy depends on printer telemetry. Fulfillment is not included unless stated.

Customer Responsibilities

- Order and stock supplies unless fulfillment is included

Exclusions

- Toner, ink, shipping, and fulfillment unless stated

ONSITE SERVICES

MIT-41 Onsite Dispatch Support

Service Description. Dispatch of Focus personnel when a covered Incident cannot reasonably be

resolved remotely.

Standard Inclusions

- Incident-based onsite troubleshooting
- Physical connectivity troubleshooting
- Device and infrastructure diagnostics

Delivery. Onsite, during Business Hours, when Focus determines that remote resolution is not reasonable.

Service Boundaries. Onsite labor is covered according to the designation of the underlying service. Travel time, travel expenses, geographic limits, minimum charges, and after-hours rates are governed by the SOW.

Customer Responsibilities

- Give site access and an onsite contact
- Provide safe working conditions, power, and workspace

Exclusions

- Travel unless included

MIT-42 Scheduled Onsite Technical Resource

Service Description. Recurring onsite technical presence as defined in the SOW.

Standard Inclusions

- Scheduled onsite visits
- Local support for covered services
- Coordination with remote Focus teams

Delivery. Onsite, on the schedule stated in the SOW.

Service Boundaries. Hours, frequency, locations, duties, substitutions, and travel are stated in the SOW.

Customer Responsibilities

- Provide workspace, network access, and a site contact

Exclusions

- Work outside the schedule

SPECIALIZED HEALTHCARE TECHNOLOGY SERVICES

MIT-43 Biomedical Device Connectivity Support

Service Description. Network-connectivity triage and vendor coordination for covered Biomedical Devices.

Standard Inclusions

- Connectivity troubleshooting
- IP, DNS, VLAN, and interface triage
- Vendor and biomedical-team coordination

Service Boundaries. Focus supports the IT connection, not clinical function, calibration, safety, or

efficacy.

Customer Responsibilities

- Maintain biomedical maintenance programs
- Designate a clinical or biomedical contact for each device type

Exclusions

- Clinical maintenance
- Calibration

MIT-44 Medical Imaging Systems Support

Service Description. Infrastructure, connectivity, storage, interface, and vendor support for covered Medical Imaging Systems.

Standard Inclusions

- PACS, RIS, and VNA infrastructure support
- Storage and network support
- Vendor coordination
- User-access triage

Service Boundaries. The SOW must identify covered applications, modalities, storage, and vendor responsibilities.

Exclusions

- Modality maintenance
- Image interpretation
- Clinical workflow consulting

MIT-45 Security System Connectivity Support

Service Description. Network and IT-infrastructure support for covered physical Security Systems.

Standard Inclusions

- Camera, badge, controller, and sensor connectivity support
- Vendor coordination
- Management-software access support

Service Boundaries. Focus does not provide monitoring, guard services, alarm dispatch, or life-safety assurance.

Exclusions

- Physical installation unless included
- Monitoring or dispatch
- Locksmith work
- Life-safety certification

PART II. MANAGED SECURITY SERVICES

Managed Security Services are organized around the NIST Cybersecurity Framework 2.0 functions of Govern, Identify, Protect, Detect, Respond, and Recover. Recovery is supported through MIT-25 and MSS-07. They are designed to reduce the likelihood and impact of security events and to support the Customer's security program. They do not guarantee uninterrupted operation, prevention or detection of every security event, or compliance with any law or framework. Customer remains responsible for its own compliance obligations, including its obligations as a covered entity or business associate under HIPAA.

IDENTIFY

MSS-01 Vulnerability Management

Service Description. Ongoing identification, prioritization, tracking, and supported remediation of vulnerabilities affecting covered assets.

Standard Inclusions

- Recurring automated vulnerability scanning of covered assets
- Risk-based prioritization using the Exploit Prediction Scoring System (EPSS) and severity data
- Remediations executed for Critical and High-priority vulnerabilities via automated patch orchestration (operating systems and supported standard third-party desktop applications).
- Asset and vulnerability reporting for service reviews

Delivery. Automated scanning; remediation during Business Hours.

Service Boundaries. Scanning covers assets where the scanning agent or credentials are in place. Remediation that requires hardware replacement, major application upgrades, vendor services, or material change is Project Services. Some vulnerabilities cannot be remediated until a vendor releases a fix, and Focus will document compensating recommendations where practical. Where Managed Security is procured without Managed IT services, Focus's scope is strictly limited to scanning, prioritization, and providing remediation guidance to Customer.

Customer Responsibilities

- Authorize scanning of covered assets and networks
- Approve remediation that requires downtime or vendor involvement
- Document risk acceptance for vulnerabilities Customer chooses not to remediate

Exclusions

- Penetration testing
- Custom application remediation

MSS-02 Attack Surface Management

Service Description. Ongoing monitoring of covered internet-facing assets, external exposures, and identified credential risks.

Standard Inclusions

- Internet-facing asset and exposure monitoring for covered domains and IP ranges
- Dark web monitoring for leaked credentials and data associated with covered domains
- Remediation and risk-tracking workflows where supported
- Asset and risk dashboard

Delivery. Automated monitoring; review and notification during Business Hours.

Service Boundaries. Monitoring is limited to covered domains, assets, brands, and identities. Finding an exposure does not mean it will be remediated or removed. Credential exposures are reported to Customer, and password resets follow MIT-19.

Customer Responsibilities

- Identify all domains and public IP ranges to be monitored
- Act on exposure notifications, including password resets and decommissioning

Exclusions

- Penetration testing
- Red-team exercises
- Takedown or removal of exposed data

PROTECT

MSS-03 End User Protection

Service Description. Safeguards designed to protect covered Users, email, web activity, and data.

Standard Inclusions

- Advanced email threat protection against phishing, business email compromise, malware, and impersonation
- Email data loss prevention and encryption, as available through Focus-provided email security and Customer's Microsoft licensing

Delivery. Automated protection; administration during Business Hours.

Service Boundaries. What is available depends on Customer licensing and on the covered Users, devices, domains, and tenants. Protective controls reduce risk and will not stop every malicious message or action. Endpoint anti-malware and DNS filtering are provided under MIT-16 and MIT-17.

Customer Responsibilities

- Approve data loss prevention rules and encryption triggers
- Train Users to report suspicious email, and confirm payment-change requests by a second channel
- Release or deny quarantined messages through the approved process

Exclusions

- Security awareness training unless included elsewhere

MSS-04 Endpoint Protection Platform (EPP)

Service Description. Policy-based endpoint controls intended to restrict unauthorized software and contain risky activity on covered endpoints.

Standard Inclusions

- Application allowlisting and execution control
- Behavioral containment and application ringfencing
- Endpoint network traffic control
- Storage and removable-media control

- Exception request handling through the service desk

Delivery. Automated enforcement; exception handling during Business Hours.

Service Boundaries. Controls apply only to supported covered endpoints. Customer-approved exceptions may reduce protection.

Customer Responsibilities

- Approve allowlisting policies and exception workflows
- Plan new software with Focus so it can be approved before rollout

MSS-05 Identity Protection and Conditional Access

Service Description. Management of multi-factor authentication (MFA) and conditional access policies in covered identity platforms.

Standard Inclusions

- MFA policy configuration and administration
- Conditional access policy design and administration
- Review of risky sign-in reports where licensing supports it
- Exception handling on authorized request

Delivery. Automated enforcement; administration during Business Hours.

Service Boundaries. Requires Microsoft Entra ID P1 or equivalent licensing. Exceptions approved by Customer reduce protection.

Customer Responsibilities

- Approve policies and exceptions
- Require User enrollment in MFA

DETECT AND RESPOND

MSS-06 Managed Detection and Response (MDR)

Service Description. Ongoing security monitoring, detection, analysis, escalation, containment, and supported response for covered assets and data sources.

Standard Inclusions

- 24x7x365 security operations center (SOC) monitoring of covered data sources
- Behavioral and signature-based threat detection
- User and entity behavior analytics (UEBA)
- Automated and analyst-driven containment using supported security orchestration (SOAR) capabilities, according to Customer-approved containment policies
- Alert investigation, escalation to Customer's designated contacts, and documentation

Delivery. SOC monitoring and automated containment 24x7x365. Focus engineer response occurs during Business Hours, or as described in MSS-07.

Service Boundaries. SOC monitoring, analyst triage, and automated or pre-approved containment operate 24x7x365. Investigation beyond initial triage, engineer-led eradication, and restoration are provided under MSS-07 up to its stated limits. Work beyond those limits, forensics, and after-hours engineering are billed at the rates stated in the SOW. Detection depends on the data sources connected to the platform.

Customer Responsibilities

- Maintain a current after-hours emergency contact with authority to approve containment
- Approve containment policies, such as automatic isolation of devices or disabling of accounts
- Notify Focus of planned activity that may look like an attack, such as penetration tests or administrative scripts
- Notify your cyber insurer and engage breach counsel when required by your policy or the situation

MSS-07 Security Incident Response

Service Description. Coordinated technical response to confirmed security incidents affecting covered assets.

Standard Inclusions

- Containment, eradication, and restoration of affected covered systems, up to the included hours per incident stated in the SOW.
- Coordination with Customer's designated contacts, insurer, breach counsel, and third-party forensic firms
- Written incident summary, prepared at the direction of Customer's breach counsel where counsel is engaged

Delivery. During Business Hours. After-hours engineering is billed at the rates stated in the SOW.

Service Boundaries. If the SOW states no included hours, none are included and all hours are billed on a T&M basis. Hours beyond the included limit, digital forensics, legal and regulatory work, and full environment rebuilds are billed as described in the SOW. Decisions on ransom payment, law-enforcement involvement, and notification belong to Customer.

Customer Responsibilities

- Engage breach counsel and notify the cyber insurer as the policy requires
- Make decision-makers available during the incident
- Preserve evidence as directed by counsel or forensic providers

Exclusions

- Ransom negotiation or payment

GOVERN

MSS-08 Security Governance, Risk, and Compliance (GRC)

Service Description. Strategic security leadership, risk oversight, compliance support, workforce training, testing, and reporting.

Standard Inclusions

- Virtual CISO (vCISO) advisory leadership supporting the Customer's designated security official
- Annual security risk assessment of covered systems with a documented findings report, designed to support Customer's HIPAA risk analysis
- Risk register maintenance and tracking
- Monthly executive security and compliance reporting
- Periodic simulated phishing assessments
- Security awareness training for the workforce, with participation reporting

Delivery. Remote advisory and reporting; scheduled meetings during Business Hours.

Service Boundaries. vCISO services are advisory. The vCISO is a virtual service delivered by Focus's team on a defined cadence. It is not a named individual filling the role of Customer's CISO. Focus personnel are not officers, employees, or fiduciaries of Customer and have no authority to bind Customer. Customer retains accountability for compliance, legal interpretation, risk acceptance, policy adoption, workforce management, and sanctions. Customer remains responsible for the completeness of its enterprise-wide HIPAA risk analysis. Remediation of findings is scoped separately unless covered by another purchased service.

Customer Responsibilities

- Designate a security official and make that person available for scheduled meetings
- Provide information and access needed for the risk analysis
- Require workforce participation in training and enforce the sanction policy
- Decide on and document risk treatment for each finding

Exclusions

- Fractional CISO services (FXS-01)

MSS-09 Security Policy Management

Service Description. Development, lifecycle administration, review, and supported technical enforcement of Customer security policies.

Standard Inclusions

- Security policy development from Focus templates tailored to the Customer
- Periodic policy review and updates
- Mapping of policies to supported technical controls
- Policy status reporting

Service Boundaries. Customer is responsible for policy approval, adoption, communication, and enforcement. Focus templates and methodologies remain Focus property. Customer-specific policies belong to Customer as described in the MSA.

Customer Responsibilities

- Review and approve policies
- Communicate policies to the workforce and enforce them

MSS-10 Third-Party Risk Management

Service Description. Assessment, monitoring, and reporting of cybersecurity risks associated with Customer-designated third parties.

Standard Inclusions

- Vendor security and risk assessments, up to the annual limit stated in the SOW (default: 25 per year)
- Ongoing third-party risk monitoring of assessed vendors
- Findings documentation and remediation recommendations

Service Boundaries. Focus does not control vendor participation, remediation, or contract terms. Assessments beyond the annual limit are billed on a T&M basis.

Customer Responsibilities

- Identify vendors for assessment and provide vendor contacts
- Make decisions on vendor risk and contract terms

Exclusions

- Onsite vendor audits
- Execution of business associate agreements

PART III. FRACTIONAL EXECUTIVE SERVICES

Fractional Executive Services give Customer a named Focus consultant who fills a technology leadership role part-time. They are distinct from the virtual advisory services in this Catalog, such as the vCISO in MSS-08. Virtual services are a defined set of deliverables and meetings on a cadence, delivered by a Focus team. Fractional services provide an individual who participates in Customer's leadership, within the time allocation and decision authority stated in the SOW.

FXS-01 Fractional Executive Services (CIO, CTO, CISO)

Service Description. Provision of a named Focus consultant to serve part-time in one of the technology leadership roles below. The consultant works within the time allocation, scope, and decision authority stated in the SOW.

Role Profiles. The SOW identifies the role selected.

Role	Accountable for
Fractional Chief Information Officer (fCIO)	Overall operational delivery of IT. Sets IT strategy in service of the business, develops and manages the IT budget, oversees IT vendors and service providers, and reports to Customer's executive team on how technology operates.
Fractional Chief Technology Officer (fCTO)	Technical direction. Evaluates and recommends the technology platforms, architecture, and standards the organization builds on, and guides technology for product, research, or innovation initiatives.
Fractional Chief Information Security Officer (fCISO)	Leadership of Customer's security and risk program: security strategy, policy, risk management, HIPAA security compliance support, incident readiness, and security reporting to executives and the board.

Standard Inclusions

- A named individual, or a role profile when the SOW so states, assigned to the selected role
- Participation in Customer leadership meetings, planning sessions, and board or committee meetings at the cadence stated in the SOW
- Strategy, roadmap, budget, and policy development within the selected role
- Exercise of the decision authority expressly delegated in the SOW
- Coordination with Focus managed service teams and Customer's vendors
- Periodic written status reporting to Customer's designated executive sponsor
- Quarterly site visits in conjunction with Quarterly and Annual Business Reviews

Delivery. Onsite or remote, as stated in the SOW, during Business Hours. Time outside Business Hours is scheduled by mutual agreement.

Allocation and Allocation Cap. The SOW states the time allocation as hours per month. Allocation for one Customer may not exceed 65% of a full-time schedule. That means no more than 26 hours per week, averaged over each calendar month, based on a 40-hour week. A requirement above this cap is not Fractional Executive Services and must be addressed through a separate staffing or employee transition engagement. Unused hours do not roll over to later months. Additional hours within the cap require a Change Order.

Service Boundaries. Status. The consultant is a Focus employee or contractor. The consultant is not an employee, officer, director, or fiduciary of Customer, even if Customer uses the role's title internally, unless Customer separately appoints the consultant to an office in writing with Focus's prior written consent. If Customer makes such an appointment, Customer must name the consultant as an insured under its directors and officers liability insurance and indemnify the consultant and Focus as it does its

own officers. This service is primarily delivered remotely.

Decision Authority and Delegated Authority. Unless otherwise stated in the applicable SOW, a Fractional Executive may:

- Direct and prioritize the activities of Focus personnel assigned to the Customer;
- Coordinate with Customer personnel, vendors, contractors, carriers, software providers, and service providers;
- Develop and recommend technology strategies, budgets, standards, roadmaps, policies, priorities, and operational procedures;
- Participate in leadership, planning, budgeting, vendor-selection, and operational-review meetings;
- Approve routine operational decisions required to maintain and operate the covered technology environment;
- Escalate operational issues and make recommendations regarding technology investments, risk treatment, staffing needs, vendor selection, and project prioritization; and
- Serve as Customer's primary technology leadership representative for matters involving information technology operations.

Unless otherwise stated in the applicable SOW, a Fractional Executive may not:

- Execute contracts on Customer's behalf;
- Commit Customer to expenditures, purchases, financing arrangements, subscriptions, or contractual obligations;
- Approve expenditures exceeding previously approved budgets;
- Hire, terminate, evaluate, discipline, compensate, or otherwise make employment decisions regarding Customer personnel;
- Make legal, regulatory, tax, accounting, compliance, clinical, or risk-acceptance decisions on behalf of Customer;
- Make representations to regulators, auditors, insurers, lenders, investors, or governmental agencies on Customer's behalf; or
- Bind Customer to any commitment, agreement, policy, or obligation not previously approved by Customer.

Customer retains final authority and accountability for all business, financial, employment, legal, compliance, clinical, security, and risk-management decisions.

Vendor Recommendations. When a recommendation involves products or services that Focus resells or provides, the consultant will disclose that.

Substitution. Focus may substitute the named individual with notice to Customer, for example because of illness, departure, or a conflict. Focus will provide a replacement with comparable qualifications. Customer may request a replacement for reasonable cause.

Customer Responsibilities

- Designate an executive sponsor to whom the consultant reports
- Document delegated decision authority in the SOW, and update it in writing when it changes
- Include the consultant in the meetings, information, and systems the role requires
- Make final decisions on recommendations, and record risk acceptance where recommendations are declined

Exclusions

- Allocation above 65% of a full-time schedule

- Travel time & expense is not included and subject to the travel policy as defined in the SOW
- Hands-on technical work, which is provided under the applicable managed services or as Project Services
- Hands-on IT director or IT manager duties
- Service as an officer of record, except as described in Service boundaries

GLOSSARY

The Glossary is informational. Capitalized terms defined in the MSA, SOW, SLA, or Managed IT – Supplemental Terms and Conditions have the meanings given there.

Term	Meaning
Add-on	An optional service or enhancement that applies only when expressly selected in the SOW.
Business Day / Business Hours	As defined in the Managed IT – Supplemental Terms and Conditions, or as stated in the SOW.
Co-Managed / Fully Managed	The delivery models defined in the Managed IT – Supplemental Terms and Conditions and designated in the SOW.
EPSS	Exploit Prediction Scoring System, a public model that estimates the likelihood a vulnerability will be exploited.
Incident / Request	As defined in the Managed IT – Supplemental Terms and Conditions. An Incident is something that isn't working as expected. A Request is something new or changed.
Fractional executive	A named Focus consultant who fills a technology leadership role part-time under FXS-01. Distinct from a virtual service.
MDR / SOC	Managed detection and response, delivered through a security operations center that monitors for threats 24x7.
MFA / Conditional access	Sign-in protections that require a second factor, or that evaluate the sign-in context, before granting access.
PHI / ePHI	Protected health information and electronic protected health information, as defined under HIPAA.
Primary / Secondary	The organization with overall operational accountability, and the organization assisting it, as defined in the Managed IT – Supplemental Terms and Conditions and designated in the SOW.
Project Services	Work that meets the project thresholds in the SOW, scoped and billed separately.
RMM	Remote monitoring and management platform used to support, patch, and inventory devices.
SOAR / UEBA	Security orchestration, automation, and response; user and entity behavior analytics. Capabilities of the MDR platform.
User, Workstation, Tablet, Server, Network Device, Peripheral, Biomedical Device, Medical Imaging System, Security System, Low Voltage Wiring	As defined in the Managed IT – Supplemental Terms and Conditions.
CIS / ITIL / NIST CSF	Widely used frameworks: CIS Critical Security Controls, the IT Infrastructure Library for service management, and the NIST Cybersecurity Framework.
PACS / RIS / VNA	Picture archiving and communication system; radiology information system; vendor-neutral archive. Medical imaging platforms.
ATA	Analog telephone adapter, which connects fax machines and analog phones to a VoIP network.
vCISO	Virtual Chief Information Security Officer, an advisory security leadership role provided under MSS-08. The vCISO is not an officer of the Customer.
Virtual service	A defined set of advisory deliverables and meetings delivered by a Focus team on a cadence, such as the vCISO. Distinct from a fractional executive. Distinct from a fractional CISO (FXS-01).