DESCRIPTION OF SERVICES

SERVICE STATEMENT

Companion Document to the Master Service Agreement

Westshore Technologies, LLC d/b/a predictiveIT

PRIVATE & CONFIDENTIAL

Version 3.0 | 2026

1. ABOUT THIS DOCUMENT

This Service Statement contains provisions that define, clarify, and govern the services described in the Quote to which it is attached. If you do not agree with the terms of this Service Statement, you should not sign the Quote and you must contact us for more information.

This Service Statement is the comprehensive reference that describes all managed services provided or facilitated by Westshore Technologies, LLC d/b/a predictiveIT; however, only those services specifically described in the Quote will be provided. Activities not described in the Quote are out of scope unless agreed to in writing.

> *This Service Statement contains important provisions pertaining to auto-renewal, fee increases, and scope boundaries. Please read carefully and keep a copy for your records.*

Key Definitions

- **Covered User:** A computer user with an assigned or dedicated workstation, point-of-sale station, or shared computer station. Each includes a single user license and single endpoint license entitlement.
- **Covered Device:** A desktop, laptop, workstation, or other supported endpoint managed under the agreement.
- **Additional Endpoint:** A device not assigned to a specific Covered User (shared workstations, kiosks, conference room PCs, medical devices) receiving basic maintenance and cybersecurity protection.
- **Cloud User:** An additional cloud-based user account not covered by a Covered User entitlement, including email-only, service, and administrative accounts.
- **Authorized Contact:** Your designated personnel authorized to provide direction, consent, and approval for services.
- **Environment:** The managed portion of your technology infrastructure as defined in the Quote.

2. YOUR PREDICTIVEIT SERVICE TEAM

Every predictiveIT client is supported by a structured service delivery team built around five distinct layers, each with a defined purpose. This enforces segregation of duties, governance oversight, controlled change management, and proactive incident reduction.

Technology Alignment Manager (TAM) — Your technical steward. Through structured standards-based assessments, your TAM identifies technical risk, documents misalignment, and ensures your infrastructure conforms to our standards library.

Virtual Chief Information Officer (vCIO) — Your strategic technology advisor. Develops technology roadmaps, manages IT budgets, conducts Technology Business Reviews, assesses workflows, and ensures investments align with business goals.

Service Desk — Unlimited remote technical support through phone, email, chat, and portal. Every interaction is tracked and governed by our escalation policies.

Centralized Operations (NOC/SOC) — 24x7x365 monitoring, alerting, maintenance, and threat detection and response across your entire managed environment.

Professional Services — Project implementation, infrastructure deployments, system migrations, and escalated technical work outside day-to-day managed services.

3. SERVICE PLANS

predictiveIT offers tiered service plans with modular add-ons (Compliance, Evergreen, Momentum, Penetration Testing) attachable to any base plan.

3.1 Essential

Comprehensive remote-only managed IT and cybersecurity services.

- All Centralized IT Operations (NOC) services (Section 4)
- Unlimited Remote Help Desk (8AM–5PM ET, M–F)
- Remote Tier 1–3 Service Desk Support
- Dedicated TAM (remote reviews only)
- Dedicated vCIO with Technology Business Reviews
- All Cybersecurity Services (Section 8)
- Monthly Reporting

Essential Does Not Include:

- Onsite visits, block hours, or after-hours coverage (available billable)

3.2 ProCare

Everything in Essential plus onsite services and billable after-hours support.

- Monthly Block Hours based on Managed IT & Cyber MRR (see Section 12)
- Onsite TAM reviews, Wellness Visits, Escalated Onsite Support
- Mini-Project eligibility (block-hour-eligible work)
- After-hours support at published extended-hours rates

> *Block Hours are calculated on Managed IT & Cybersecurity fees only. M365 licensing, cloud resale, and third-party subscriptions are excluded.*

3.3 EliteCare

Highest coverage: 24x7x365 support and unlimited escalated onsite.

- 24x7x365 Support Coverage (after-hours on-call)
- Unlimited Escalated Onsite Support dispatched by predictiveIT
- Priority Professional Services scheduling

- Enhanced SLA commitments (Exhibit A)

3.4 + Momentum (Prepaid Professional Services)

Momentum converts unpredictable project costs into a fixed annual technology investment. Available as an add-on to ProCare or EliteCare.

> *Instead of approving every project individually, you have an annual technology investment fund managed by your vCIO. We plan the work, you get preferred pricing, and your technology evolves predictably.*

- Annual Professional Services pool calculated as a percentage of your annual Managed IT & Cyber spend
- Work billed at a discounted rate reflecting the value of prepaid, committed investment
- Your vCIO manages planning, prioritization, and scheduling across the year
- Emergency or short-notice requests (less than 5 business days' notice) are subject to scheduling surcharges and billed at standard (non-discounted) rates
- Momentum is designed for planned, scheduled work; your vCIO will collaboratively plan the annual project calendar
- Annual pool is non-rollover; unused allocation expires at end of contract period
- Large-scope projects (>2x remaining pool) may be quoted separately

3.5 + Compliance

Executive-level cybersecurity governance, compliance assessment, and security program oversight. Attachable to any base plan. See Section 9 for full scope.

> *Available as Essential + Compliance, ProCare + Compliance, or EliteCare + Compliance.*

3.6 + Evergreen (Hardware as a Service)

Eliminates capital hardware expenses with predictable monthly investment from predictiveIT's approved catalog. 36-month workstation lifecycle with automatic refresh. predictiveIT retains ownership. See Exhibit E for terms.

4. CENTRALIZED IT OPERATIONS (NOC)

24x7x365 monitoring, maintenance, and proactive management of your technology environment.

4.1 Site Documentation

Comprehensive documentation including asset inventory, backup schedules, ISP information, credential management references, patch policies, and monitoring escalation policies.

4.2 Infrastructure Monitoring

Servers

Online/offline status, CPU/memory performance, disk space and health, critical Windows services (AD, DNS, Netlogon, time sync), application services, antivirus/EDR status, patch compliance, SQL health, backup completion.

Workstations & Endpoints

Online/offline status, disk space, performance, antivirus/EDR, encryption compliance, local admin changes, patch status, security event auditing.

Network Infrastructure

Device reachability (ICMP/SNMP), switch port status, bandwidth utilization, VLAN/subnet discovery, topology mapping, configuration backup and change detection, DHCP health.

Firewalls

Reachability, configuration/rule changes, VPN tunnel status, admin sign-in auditing, IDS/IPS detection, wireless intrusion detection. Logs correlated through SOC.

Wireless

AP status, client connections, signal quality, channel utilization, rogue AP detection, configuration changes.

Power & Environmental

UPS battery state, temperature, self-test results via vendor platforms.

4.3 Preventative Maintenance

Patch management (whitelisted critical security patches), performance reviews, temp file cleanup, disk integrity checks, service packs, spyware/malware remediation.

4.4 Managed Backup & Disaster Recovery

Backup completion monitoring, failure alerting, remediation, quarterly restore verification. Client provides backup media and cloud storage.

4.5 Managed Endpoint Protection (EDR/MDR)

Next-gen endpoint detection and response on all covered devices. Continuous monitoring of protection status, signatures, scans, detections, quarantine, and unauthorized software.

4.6 Monthly Reports

Executive Summary, Uptime, SLA, and System Health reports delivered monthly.

5. REACTIVE SUPPORT SERVICES (SERVICE DESK)

Your single point of contact for technical support, vendor coordination, and issue resolution.

5.1 Unlimited Remote Help Desk

Phone, chat, email, and portal support. Issues that cannot be resolved remotely are dispatched onsite with Authorized Contact approval.

5.2 Remote Tier 2 & 3 Support

Advanced technical expertise for server, router, and firewall issues.

5.3 Server Administration

User account management, password resets, security group management, directory share management.

5.4 Single Point of Contact

Vendor and LOB coordination: web/email hosting, ISP, copier/printer, and software vendor liaison.

5.5 Escalated Onsite Support

Dispatched at predictiveIT's discretion. ProCare: billed to block hours. EliteCare: included. Essential: billed at PS rate.

5.6 Escalation & Priority Model

Severity	Definition	Response Target
P1 — Critical	Entire client impacted; business stopped	Immediate; escalation within 15 min
P2 — High	Department or multiple users	Within 1 hour
P3 — Medium	Single user degraded	Within 4 hours
P4 — Low	Minor / service requests	Within 24 hours

6. PROACTIVE MANAGEMENT (TECHNOLOGY ALIGNMENT)

> *Technology Alignment sets predictiveIT apart. Our TAM process identifies technical risk before it impacts your business — reducing downtime, lowering costs, and keeping technology aligned with best practices.*

6.1 What Technology Alignment Is

Proactive assessment and alignment of your IT environment against predictiveIT's Standards Library — covering security, infrastructure, cloud, backup, networking, and endpoints. Monthly reviews on a rotating frequency schedule.

6.2 What Technology Alignment Is Not

Not reactive support, on-demand service, or project implementation. Break/fix, hardware installs, MACs, and accumulated issue lists go through Service Desk or Professional Services.

> *If an issue requires immediate attention during a TAM review, the TAM reports it to the Service Desk. Proactive work is never displaced by reactive demand.*

6.3 Remote-First Model

Monthly reviews performed remotely. Onsite visits coordinated when physical inspection is required, billed to Block Hours.

6.4 Onsite Wellness Visits

Periodic onsite check-ins for relationship maintenance, feedback, and physical inspection. Not a support session. Issues reported to Service Desk.

6.5 Action Plan Management

Documented alignment findings tracked through remediation. Low/medium items discussed in TBRs; high/critical items reported immediately.

6.6 In-Scope Remediation

Minor items (<1 hour, no user impact) may be performed within Block Hours. Larger items scoped through vCIO.

7. STRATEGIC MANAGEMENT (VCIO)

> *Your vCIO is a strategic business partner who understands your goals, translates technical risk into business impact, and builds roadmaps tied to your priorities and outcomes.*

7.1 Engagement Framework

- **Discover —** Business goals, challenges, priorities. Identify top rocks for the quarter and year.
- **Assess —** Leverage TAM data and workflow assessments to identify gaps, risks, opportunities.
- **Plan —** Technology Roadmap and Budget Forecast aligned to business objectives.
- **Execute —** Coordinate delivery, track progress, ensure changes support outcomes.
- **Review —** Technology Business Reviews to measure progress and adjust priorities.

7.2 Technology Business Reviews (TBR)

Scheduled reviews with decision-makers covering service activity, alignment items, project status, roadmap progress, and service satisfaction. Frequency based on service plan and organizational profile.

7.3 Technology Roadmap

Prioritized, budgeted quarterly plan tied to business objectives. Updated at each TBR.

7.4 Budget Forecasting

IT investment guidance aligned to your roadmap and financial planning cycle.

7.5 Workflow Assessment & Optimization

Identify manual processes, key-person dependencies, system fragmentation, and automation opportunities. Recommendations incorporated into the roadmap.

> *Technology exists to support how your business operates — not the other way around.*

7.6 Virtual Purchasing Agent

Hardware/software research, warranty tracking, lifecycle replacement planning.

7.7 Baseline DR Planning

Basic disaster recovery plan. Comprehensive BCP available as Professional Services.

7.8 Baseline Security & Risk Analysis

Security risk review with mitigation recommendations. Comprehensive assessments via Compliance add-on.

7.9 IT Policy Development

IT-related policy development for employee manuals.

7.10 IT Project Management

Project Size	PM Approach	PM Billing
Under 4 hours	No formal PM	vCIO oversight included
4–8 hours	vCIO light PM	Minimum 1hr PM fee
8–40 hours	Dedicated PM	10% of project hours, min 2hrs
40+ hours	Full PM engagement	10–15% with milestones

8. CYBERSECURITY SERVICES

Continuous detection, response, and mitigation powered by the NIST Cybersecurity Framework and MITRE ATT&CK methodology.

8.1 24x7x365 SOC

SIEM-based event correlation across all security tools. Real-time detection, response, and mitigation.

Monitoring Scope:

- Endpoint telemetry (malware, quarantine, unauthorized software, policy violations)

- Network/firewall (config changes, unauthorized access, VPN, IDS/IPS)
- SaaS Application Security (M365/Azure AD/Google: sign-in anomalies, privilege escalation, OAuth, file activity)
- Email threats (phishing, forwarding rules, BEC indicators)
- Identity/MFA (geo-fence, impossible travel, enrollment events)
- Dark web credential monitoring

8.2 SaaS Application Security Monitoring

Dedicated cloud environment visibility: suspicious behavior, insider threats, BEC detection, activity logging, security posture management.

8.3 Managed EDR/MDR

24x7x365 endpoint monitoring, detection, containment, and response.

8.4 Email Security & Phishing Protection

Anti-virus, anti-spam, anti-phishing, and executive targeting protection.

8.5 Security Awareness Training & Phishing Simulation

Recurring training and monthly simulated phishing campaigns.

8.6 Dark Web Monitoring

Continuous credential exposure monitoring with SOC investigation.

8.7 Vulnerability Management

Monthly scanning with severity-prioritized remediation reporting.

8.8 DNS Security & Web Content Filtering

DNS-layer blocking of malicious domains and policy-violating content.

8.9 Managed MFA

MFA management, enrollment support, policy management, anomaly detection.

8.10 Penetration Testing

- **Engagement-Based:** Annual internal/external pentest per SOW. Executive and technical reports with remediation roadmap.
- **Continuous (Monthly):** Recurring automated pentesting with monthly findings reports feeding TAM Action Plans.

8.11 Incident Response

Detection, containment, analysis, mitigation, recovery coordination, and post-incident reporting.

8.12 Cadence & SLA

Service	Cadence	SLA
SOC Monitoring	24x7x365	Triage within 15 min
Incident Notification	On confirmation	Within 2 hours
Containment	On confirmed threat	Within 1 hour
Remediation Plan	Post-incident	Within 24 hours
SAT Delivery	Quarterly min	New users within 14 days
Phishing Sim	Monthly	Results within 5 days
Vuln Scanning	Monthly	Crit/High: 72hrs; Med: 14 days
Dark Web	Continuous	Investigated within 24hrs

8.13 Cybersecurity Exclusions

- Full forensic investigation and evidence collection
- Legal/regulatory notification on client's behalf
- Breach counsel or legal representation
- Data recovery beyond backup restoration
- Pre-existing vulnerability remediation
- Compliance certification or attestation

9. COMPLIANCE & SECURITY GOVERNANCE (+ COMPLIANCE)

Attachable to any base plan. Provides security program governance, compliance assessment, risk management, policy development, cyber insurance support, training oversight, IR planning, and vendor risk management.

> *Bridges cybersecurity operations and business strategy. Ensures your security program meets regulatory requirements, insurance mandates, and business objectives.*

- Security Program Governance aligned to NIST CSF, CIS, CMMC, or industry frameworks
- Compliance Gap Analysis (HIPAA, PCI, SOC 2, CMMC, state privacy, cyber insurance)
- Formal Risk Assessment translated into business impact for the technology roadmap
- Security Policy Development (acceptable use, data classification, IR, access control, vendor risk)
- Cyber Insurance Support (applications, renewals, evidence, coverage gaps)
- Security Awareness Program Oversight
- Incident Response Planning, tabletop exercises, and executive oversight
- Vendor & Third-Party Risk Management

Compliance add-on does not certify, attest, or replace legal counsel. Remediation labor is scoped as Professional Services or Momentum projects. See Exhibit F.

10. PROFESSIONAL SERVICES & PROJECTS

10.1 Project Definition

Work requiring scoping/planning beyond a service request, estimated >2 hours, involving deployment/reconfiguration, or requiring multi-visit scheduling. Requires formal scope, quote, and approval.

10.2 Anti-Fragmentation

> *Related service requests that constitute a single project will be consolidated, scoped, and quoted as a Project.*

10.3 Emergency & Unscheduled Work

Scheduled at predictiveIT's discretion. Emergency requests (<5 business days' notice) billed at standard rates with scheduling surcharges.

> *Momentum is designed for planned work. Emergency requests against a Momentum pool are charged at standard (non-discounted) rates with surcharges. Plan with your vCIO to maximize value.*

10.4 Mini-Projects (Block-Hour Eligible)

Single PC, printer, app, or network device setup — only when block hours remain after TAM activities.

11. AI, AUTOMATION & BUSINESS INTELLIGENCE

11.1 Automated Onboarding & Offboarding

Form-triggered workflows for new hires and terminations: account creation/suspension, permissions, device provisioning/return, compliance documentation.

11.2 API Integrations & RPA

System integration, duplicate data elimination, automated connections between disconnected platforms.

11.3 Business Intelligence & Reporting

Automated dashboards replacing manual spreadsheets. API-driven consolidated reporting from multiple business systems.

> *Quoted as Professional Services or included in Momentum allocations.*

12. MONTHLY BLOCK HOURS

ProCare and EliteCare plans include a Monthly Block Hour allocation for onsite and remote services beyond the proactive TAM review. Your TAM's monthly alignment review time is accounted for separately and does not consume your Block Hours. Block Hour allocation is based on your Managed IT & Cybersecurity Services monthly spend (ORR excluded) and is specified in your Quote.

Block Hour Priority of Use:

Block Hours are consumed in the following priority order to protect high-value activities:

- 1st — In-Scope Remediation: Minor items (<1 hour, no user impact) discovered during TAM review
- 2nd — Onsite Wellness Visits: Periodic check-ins, feedback, and physical environment inspection
- 3rd — Escalated Onsite Support: Issues requiring onsite dispatch at predictiveIT's discretion
- 4th — Mini-Projects: Approved single-unit setups, only when hours remain after higher-priority activities

Block Hours are non-rollover. Overages billed at applicable rates. Trip and travel fees are billed separately from Block Hours.

13. PRICING & BILLING MODEL

Per User / Per Device structure. Additional Endpoints and Cloud Users at reduced rates. Rate categories: Standard PS, Senior PS, Project Management, Extended Hours, Momentum discounted, New User Setup, MACs, and trip/travel fees. All rates defined in your Quote.

14. ITEMS NOT COVERED

- Onsite PS not covered by Block Hours or EliteCare
- New hardware/software installation (Professional Services)
- Major system upgrades (Projects)
- Hardware/software procurement costs
- After-hours for Essential/ProCare (extended rates)
- Non-supported software/equipment
- Office/network relocation (Projects)
- Custom DR/BCP beyond baseline
- Forensic investigation and legal services
- LOB application development

- Cabling and physical infrastructure

15. ONBOARDING SERVICES

Deploys management and cybersecurity tools, documents environment, performs initial alignment assessment, develops initial technology roadmap and budget forecast. Includes minor remediation (<15 min, no user impact). Does not include system upgrades, procurement, migrations, or pre-existing vulnerability remediation. Fees in Quote.

EXHIBIT A — SERVICE LEVEL AGREEMENT

A.1 Response Time Targets

Channel	Business Hours (M–F 8–5 ET)	Extended Hours
Phone / Chat	Average <3 minutes	Within 2 hours (EliteCare); billable otherwise
Email / Portal	2–24 hours by severity	Next business day (unless EliteCare)

A.2 Severity Response & Resolution

Severity	Response	Resolution Plan	Resolution
P1 Critical	15 min	1 hour	4 hours
P2 High	1 hour	4 hours	8 hours
P3 Medium	4 hours	8 hours	24 hours
P4 Low	24 hours	48 hours	Best effort

A.3 Service Credits

Target: 90% measured monthly. Pro-rated credit of 1/30 of monthly recurring fees per day missed. Maximum 30% of monthly fees. 45-day transition exception applies.

EXHIBIT B — SOC SERVICES SCOPE & SLA

B.1 Methodology

Based on NIST Cybersecurity Framework and MITRE ATT&CK. Combined automated detection and analyst investigation.

B.2 Responsibility Matrix

NIST Function	Responsible	Activities
IDENTIFY	Client / predictiveIT	Asset mgmt, risk assessment, governance
PROTECT	Client / predictiveIT	Access control, training, data security
DETECT	predictiveIT SOC	Anomaly detection, continuous monitoring
RESPOND	predictiveIT SOC	Response, analysis, mitigation, comms
RECOVER	Client / predictiveIT	Recovery planning, improvements

B.3 Monitoring Scope

Servers: online/offline, CPU/memory/disk, services, AV/EDR, patches, backups, SQL, local admin changes. Workstations: online/offline, disk, performance, AV/EDR, encryption, admin changes, patching, security auditing. Network: reachability, port status, bandwidth, VLAN/subnet, topology, config backups/changes. Firewalls: reachability, config/rule changes, VPN, admin auth, IDS/IPS. Wireless: AP status, clients, signal, rogue AP. M365/Identity: sign-in anomalies, privilege activity, MFA, account lifecycle, mailbox permissions, forwarding rules, group changes, OAuth, file activity. Email: phishing, spam, forwarding manipulation, mail flow. EDR: malware, quarantine, unauthorized software, policy violations, anti-forensics. Backup: completion, failures, restore tests. Vulnerability: external/internal scans, EPSS scoring. Dark Web: credential exposure. UPS: battery, temperature.

B.4 Incident Severity

Severity	Criteria	Response
SEV1	Ransomware, data exfil, identity compromise, multi-client	War Room, executive notification, incident commander
SEV2	Confirmed malware, compromised account, unauthorized admin	Immediate containment, analyst investigation
SEV3	Suspicious activity, policy violation, failed exploitation	Investigation, documented findings
SEV4	Informational, known false positives	Logged, monthly reporting

EXHIBIT C — SUPPORTED SOFTWARE & EQUIPMENT

Supported: Windows Server/Desktop (current and N-1 with active support), macOS (current and N-1), Microsoft 365, Google Workspace, standard browsers (Edge, Chrome, Firefox), network equipment from Cisco Meraki, SonicWall, Sophos, Ubiquiti, WatchGuard, VMware/Hyper-V. Non-supported: EOL operating systems, out-of-warranty hardware, consumer-grade networking. Issues caused by non-supported equipment billed at standard PS rates.

EXHIBIT D — MONTHLY BLOCK HOUR ALLOCATION

Monthly Block Hour allocations are determined by your Managed IT & Cybersecurity Services monthly recurring spend and are specified in your Quote. Allocations are based on Managed IT & Cybersecurity fees only; Other Recurring Revenue (M365 licensing, cloud resale, third-party subscriptions) is excluded from the calculation.

Clients below the minimum Managed IT & Cybersecurity MRR threshold for ProCare are on the Essential plan and do not receive Block Hour allocations. The detailed Block Hour allocation schedule is available from your vCIO upon request.

Block Hour Priority of Use:

Block Hours are consumed in the following priority order. Your TAM's monthly alignment review time is accounted for separately and does not consume Block Hours.

Priority	Activity	Description
1st	In-Scope Remediation	Minor items (<1hr, no user impact) discovered during TAM review.
2nd	Wellness Visits	Periodic onsite check-ins, feedback, and physical inspection.
3rd	Escalated Onsite Support	Issues requiring onsite dispatch at predictiveIT's discretion.
4th	Mini-Projects	Approved single-unit setups, only when hours remain.

Monthly Block Hours are non-rollover. Unused hours expire at the end of each billing period. All onsite visits incur trip and travel fees billed separately from Block Hours.

EXHIBIT E — EVERGREEN HARDWARE AS A SERVICE

predictiveIT-owned hardware from approved catalog. 36-month workstation lifecycle, 60-month infrastructure lifecycle. Auto-refresh at end of lifecycle. Client responsible for physical care. Early termination = remaining balance. Custom requests at additional cost.

Category	Specification	Lifecycle
Standard Laptop	Business-class, i5, 16GB, 512GB SSD	36 months
Standard Desktop	Business-class, i5, 16GB, 512GB SSD	36 months
Managed Switch	48-port PoE+ managed	60 months
Firewall/UTM	Business-grade UTM	60 months
Wireless AP	Enterprise-grade	60 months

EXHIBIT F — COMPLIANCE ADD-ON SCOPE

Attachable to any base plan. Does not replace legal counsel or external auditors.

Service	Description
Security Program	Establish and maintain security program (NIST CSF, CIS, CMMC, industry)
Gap Analysis	Periodic compliance assessment with remediation roadmap (HIPAA, PCI, SOC 2, CMMC, cyber insurance)
Risk Assessment	Formal risk identification and prioritization for technology roadmap
Policy Development	Acceptable use, data classification, IR, access control, vendor risk policies
Insurance Support	Application/renewal, control documentation, evidence, coverage gaps
SAT Oversight	Training program strategy, results analysis, program adjustments
IR Planning	IR Plan development, tabletop exercises, executive oversight, insurer coordination
Vendor Risk	Vendor security evaluation, requirements, ongoing assessments

Typical cadence: annual risk assessment and gap analysis, semi-annual policy review, quarterly compliance reporting in TBRs, annual tabletop exercise. Excludes certification/attestation, legal counsel, remediation labor (scoped as PS/Momentum).

— End of Description of Services —