OCEAN COMPUTER GROUP, INC.

OceanWATCH IT Managed Services SOW

Prepared for:

John Karpinski | Director, Professional Services
E: jkarpinski@oceancomputer.com
P: 732.242.0264

Table of Contents

Section Page

OceanWATCH IT Managed Services Program Details

Services Agreement Letter

May 24, 2021

Borough and Police Department of South Tomes River
19 Double Trouble Road
South Toms River, New Jersey 08757
ATTN: Joseph Kostecki

Re. Information Technology (IT) Managed Services SOW

Dear, Mr. Kostecki,

Ocean Computer Group, Inc. is prepared to begin IT Managed Services for **BOROUGH AND PD OF SOUTH TOMS RIVER May 1, 2021,** through our OceanWATCH program. This managed services agreement/SOW contains:

The services to be covered in a standard monthly service cost as requested in the initial Proposal for Information Technology Managed Services for **BOROUGH AND PD OF SOUTH TOMS RIVER**.

- On Page 4, the monthly pricing agreement for the duration of the contract (as stated in the original proposal details presented by Ocean Computer Group, Inc. on July 2nd, 2021.)

- Ocean Computer Group, Inc. specifics on the OceanWATCH IT Managed Services program that was presented to **BOROUGH AND PD OF SOUTH TOMS RIVER** (specifically the IT Managed Services that will be performed during the agreement starting on Page 6).

Once the agreement is signed, we will reach out to establish a date/time to begin the initial onboarding process. This process is designed to level set and update all your crucial computing equipment and operating systems to provide the best possible user experience.

Please contact me if you have any further questions. We are looking forward to servicing the IT needs of **BOROUGH AND PD OF SOUTH TOMS RIVER.**

John Karpinski
Director of Professional Services
(P): 732.242.0264
(E): jkarpinski@oceancomputer.com

OceanWATCH Pricing Summary

Proposed Solution:

Ocean Computer Group, Inc. is proposing our OceanWATCH fully managed service agreement. Our managed services agreements work towards these **'8' major goals:**

❶ Proactively address issues and risks before they happen	❺ Cost-effective access to enterprise-level support and skills
❷ Provide a high level of service to your organization	❻ Minimize downtime
❸ Increase operational efficiencies and up-time	❼ Plan budgets, upgrades, and improvements
❹ Reduce costs	❽ Total peace of mind as your network is monitored 24/7/365

Location(s) of Services / Cost Proposal:

Ocean Computer Group, Inc. is prepared to provide IT services as required by the Client for following facilities:

9:00am – 5:00pm Monday through Friday monitoring for administrative offices

START DATE: May 1, 2021

INFORMATION TECHNOLOGY (IT MANAGED SERVICES)	
DESCRIPTION / AGREEMENT DURATION	**MONTHLY RECURRING CHARGE (All-inclusive)***
Current Device Inventory	**27 total***
Total Monthly Recurring Charge** *NOTE: Any devices added will be billed at $50.00 per device.**	**$1,350.00 / per month charge***
Initial On-boarding fee	**N/A**
Dark Web Scanning/Bullphish ID	**Included in monthly charge**
***NOTE: Management of servers, switches and firewalls are included at no extra charge.**	

ADDITIONAL IT SERVICES	
Backup Services	**Available upon request**
Anti-virus / Malware / Endpoint Detection and Response	**Available upon request**
Microsoft Office 365	**Available upon request**
Security Services (i.e. firewalls, multi-factor authentication, SOC-SIEM)	**Available upon request**

***NOTE: All-inclusive charge includes onsite service when necessary/required, travel charges, mileage, and tolls.**
****Pricing will be locked-in for the term of the contract.**

OUT-OF-SCOPE WORK (PROJECT-BASED SERVICES AS NEEDED)	
DESCRIPTION	**HOURLY CHARGE**
Hourly Rate for Project-based Services *(handled during normal business hours)*	**$165.00/per hr.** *(Hourly Rate is the same for both Police Dept. and Town Hall)*

It is understood that all services requested by the Borough & PD of South Toms River that fall outside of the terms of this Agreement will be considered projects, and will be quoted and billed as separate, individual services. Ocean Computer Group will not perform any out-of-scope services without prior approval from CLIENT.

This Statement of Work ("SOW") is entered into pursuant to and adopts and incorporates by reference the terms and conditions of the Master Services Agreement (MSA) dated _____, between the undersigned parties.

Signature: _____ Title:_____ Date:_____

CLIENT: Borough & PD of South Toms River

Signature: _____ Title:_____ Date:_____

MSP: OCEAN COMPUTER GROUP, INC.

OCEANWATCH IT MANAGED SERVICES DETAILS

A crucial step in our OceanWATCH IT Managed Service offering is the initial onboarding process. This process is designed to level set and update all your crucial computing equipment and operating systems to provide the best possible user experience. The onboarding process sets the stage for a successful managed service offering.

The following pages provide in detail the IT Managed Service process performed by the technological staff at Ocean Computer Group, Inc. which correlates with the request for IT Managed Services to be provided to the Borough and PD of South Toms River.

OCG Technical Staff

Ocean Computer Group Inc. has a staff of 36 W2 employees. The IT staff has over 200 years of collective experience which includes a host of various technological disciplines and expertise. Several of the IT staff members have been employed for over 30 years. The following staff will be available to work directly with the **CLIENT** including a designated vCIO / Account Manager.

Ocean Computer Group Technical Personnel	Job Classification / Title	Technical Education	Certifications
Director, Professional Services			
John Karpinski	Director, Professional Service	DeVry Technical Institute 30+ yrs. IT industry experience	VMWare, VSP, VTSP
vCIO / Sr. Account Manager*			
Ken Dominguez	vCIO / Sr. Account Manager (MAIN CONTACT)*	30+ yrs. IT industry experience	Dell, SonicWALL, Cisco, VMware, Microsoft, Quest, Veeam, IBM, Trumethods vCIO, Project Management
OceanWATCH Managed IT Services Team Members			
David Bates	Sr. Systems Engineer / MSP Lead	University of South Carolina, Brick Computer Science Institute 30+ yrs. IT industry experience	Dell, Barracuda, CISCO: CCA, CCNA, CCEA, VCP, VMWare, Perch, Quest
Eric Parker	MSP System Administrator	20+ yrs. IT industry experience	Comptia A+, Comptia Network+, Microsoft
Steven Boytis	MSP System Administrator	Mercer County Community College 30 yrs. IT industry experience	AS in Computer Systems / Network Administration, Dell, Xerox, Cisco
Robert Karpinski	MSP System Administrator	Lincoln Technical Institute Network Communication & Information Systems Program	CompTIA A+, EC-Council Certified Ethical Hacker (CEH) Certified
Ryan Caravella	MSP System Administrator	Brookdale Community College AS, Computer Networking 2011	
Anthony Loiacono	MSP System Administrator	Keller Grad. School of Mgmt. Masters, Info. Sys. Management DeVry University, B.S. Comp. Sys. 25+ yrs. IT industry experience	
OceanWATCH Managed IT Services Systems Engineers			
Werner Philipp	Sr. Systems Engineer	Global Knowledge New Horizons Computer Learning Computer Insight Learning Ctr. 30+ yrs. IT industry experience	Dell, Server Storage, VMWare VCP, IBM, Veeam, Sophos
Chris Lehmann	Sr. Systems Engineer	Brick Computer Science Institute, Cittone Institute 20+ yrs. IT industry experience	MCSE, MCDBA, SonicWALL CCS Barracuda, Microsoft, Sophos
Larry Desmond	Sr. Systems Engineer	Dover Business College 30+ yrs. IT industry experience	MCSA, Microsoft, Comptia A+, Comptia Network+
Robert E. Wasiewicz	Sr. Systems Engineer	University Maryland, Maryland (2022) MS: Cloud Computing Architecture, BS: Computer Sciences / IT, Kean University, NJ	MCSE, CCNA, Watchguard Firewall Professional, Barracuda Essentials Engineer
Isaac Matara	Sr. Systems Engineer	NJIT, B.S, Engineering Computer Technology. Passaic County Community College, A.A.S, Computer Info. Systems	MCITP, MCTS, MCSA, MCSE

The Virtual CIO (vCIO)

The **CLIENT** will have the support of a Virtual CIO (vCIO) leveraging the myITprocess tools and methodology to deliver a continual plan of success. The role of the vCIO is to work with the **CLIENT** Business Administrator and/or stakeholders to continually deliver value, high level of service and support while assisting to recommend standards, best practices, and long-term planning.

The vCIO's responsibility is to:

- Work with **CLIENT** Business Administrator / Staff / Director
- Ongoing Consultation with the Site Manager
- Assist in developing standards and best practices
- Assist in technology recommendations
- Strategic IT planning
- Technology roadmaps
- Assist in budget creation
- Assist in acquiring additional resources, if needed

The myITprocess methodology provides:

- Comprehensive library of IT standards
- Industry compliance guidelines such as CJIS and HIPPA
- Complete impact assessments
- Helps to identify areas of concern
- Deliver a strategic roadmap

Your assigned Ocean Computer Group vCIO | Sr. Account Manager will be your first point of contact in all matters related to the IT services.

Hardware and Software Partnerships

Ocean Computer Group's strategic alliances and partnerships enable is to offer the top technologies in the industry.

After completing a project, we continue to provide post-sales support and consulting services as needed with our team of experienced senior consultants, architects, and engineers.

Clients count on us to stay up to date on the newest technology trends as they come on the market, and we are constantly exploring and evaluating new solutions to expand our portfolio of best-in-class solutions. Regulatory compliance is important to us, and our clients and we ensure that our teams trained in regulations affecting government, municipalities, education, higher education, and commercial businesses.

OCG recognizes that to support rapid growth, we must provide consistent, high quality, and responsive services while maximizing resource utilization and managing costs. OCG accomplishes this, in part, through a formal set of robust Operational Practices aligned with the Information Technology Infrastructure Library (ITIL) Service Management processes. These practices consist of a set of guides, tools, roles, and measurements that enable OCG to effectively manage the delivery of consistent and reliable infrastructure service.

OceanWATCH Managed IT and Networking Services	INCLUDED
OceanWATCH Benefits	
FIPS 140-2 Compliant Platform	✓
24x7 System Support Services, Security and Network Monitoring	✓
24x7 Onsite for Critical Failures	✓
Critical and Emergency Notifications	✓
Alert client to critical conditions, failures, and patches	✓
Secure Password Management	✓
Change Management	✓
Servers & Workstations, Laptops and Mobile Devices	
Proactively Monitor & Manage Servers for uptime and availability	✓
Operating System Patching (supported systems)	✓
Monitor critical Windows Server Services	✓
Reboot servers if needed	✓
Update Server Hardware Firmware	✓
Scheduled off time server maintenance	✓
Monitor Memory Usage to maintain uptime and performance	✓
Monitor Hard drives for failures that can cause outages	✓
Monitor and manage Hard drive disk space	✓
Resolve daily user issues such as printing application access and error conditions	✓
Data Protection	
Monitor and confirm that backup has been performed daily and replicated	✓
Check and validate status of backups procedures	✓
Document and validate retention time	✓
Perform bi-yearly targeted restores to assure valid backup data	✓
VCIO	
Conduct a full audit of the client's environment	✓
Understand the business goals	✓
Identify the challenges they are facing in their key drivers	✓
Develop a dynamic technology roadmap	✓
Conduct quarterly technology and security reviews	✓
WAN / LAN Network	
Automated inventory, that creates a profile for every device on a network	✓
Network documentation and Topology	✓
IP address management and which devices are using them	✓
Real-time mapping of network (instant notification to changes/problems that occur; quick remediation)	✓
Active Directory / Workgroup Administration	
Manage Active Directory / Workgroup account policies	✓
Manage Server Permissions and file system management	✓
Set up new users, including login restrictions, passwords, security, applications	✓
Set up and change security for users and applications	✓
Create: new directories, shares/security groups, new/disable/delete accounts, manage account policies	✓
Firewall Security	
Check, Manage and Monitor firewall logs for errors or critical issues	✓
Intelligent reporting and activity visualization	✓
Centralized logging	✓
Real-time and historic next generation syslog reporting	✓
Application traffic analytics for better insight into network activity and threats	✓
Real-time and historic data flow reporting	✓
Dark Web Monitoring	
Monitor the dark web for stolen corporate credentials of your users	✓
Protect against a breach with early detection of compromised user credentials	✓
Be alerted as soon as compromised user credentials are discovered on the dark web	✓
Email Security Awareness Training	
Simulated Phishing Attacks & End User Training	✓
Measured detail reports and analytics	✓

Response and Resolution: Trouble Ticketing Process

The following table shows the targets of response and resolution times for each priority level:

Trouble	Priority	Response time (in hours)	Resolution time (in hours)	Escalation threshold (in hours)
Services Not Available (all users and functions unavailable)	As needed	Within 2 hours	ASAP - Best Effort	2 hours
Significant degradation of service (Large number of users or business critical functions affected)	As needed	Within 4 hours	ASAP - Best Effort	8 hours
Limited degradation of service (limited number of users or functions affected, business process can continue)	Ongoing	Within 24 hours	ASAP - Best Effort	48 hours
Small service degradation (business process can continue, one user affected)	Ongoing	Within 48 hours	ASAP - Best Effort	96 hours
Service not available (all users and functions unavailable) – After Hours	As needed	Within 4 hours	ASAP - Best Effort	8 hours

The response, resolution and escalation times are provided to demonstrate a framework to bring different severity problems to resolution within the least amount of time. It is not intended to show the amount of time before a problem is addressed or escalated.

OceanWATCH Support Tiers - The following details and describes our Support Tier levels:	
Tier 1 Support	All support incidents begin in Tier 1, where the initial trouble ticket is created, the issue is identified, and clearly documented, and basic hardware/software troubleshooting is initiated.
Tier 2 Support	All support incidents that cannot be resolved with Tier 1 Support are escalated to Tier 2, where more complex support on hardware/software issues can be provided by more experienced Engineers.
Tier 3 Support	Support Incidents that cannot be resolved by Tier 2 Support are escalated to Tier 3, where support is provided by the most qualified and experienced Engineers who have the ability to collaborate with 3rd Party (Vendor) Support Engineers to resolve the most complex issues.

OceanWATCH Support Flow Process	
INITIAL PROCESS	1. Support Request is received 2. Trouble Ticket is created 3. Issue is identified and documented in Help Desk system 4. Issue is qualified to determine if it can be resolved through Tier 1 Support
Support Level	**Description**
Tier 1 Level: issue being resolved through Tier 1 Support	1. Level 1 Resolution - issue is worked to successful resolution 2. Quality Control –Issue is verified to be resolved 3. Trouble Ticket is closed, after complete problem resolution details updated in Help Desk system 4. If issue cannot be resolved through Tier 1 Support, escalated to Tier 2
Tier 2 Support: issue being resolved through Tier 2 Support	1. Level 2 Resolution - issue is worked to successful resolution 2. Quality Control –Issue is verified to be resolved 3. Trouble Ticket is closed, after complete problem resolution details updated in Help Desk system 4. If issue cannot be resolved through Tier 1 Support, escalated to Tier 3
Tier 3 Support: issue being resolved through Tier 3 Support	1. Level 3 Resolution - issue is worked to successful resolution 2. Quality Control –Issue is verified to be resolved 3. Trouble Ticket is closed, after complete problem resolution details updated in Help Desk system 4. If issue cannot be resolved through Tier 3 Support, escalated to Onsite Support
Onsite Support: issue being resolved through Tier 3 Support	1. Onsite Resolution - issue is worked to successful resolution 2. Quality Control –Issue is verified to be resolved 3. Trouble Ticket is closed, after complete problem resolution details updated in Help Desk system

NOTE: Support will determine and escalate to subsequent Tiers as the situation merits.
For example, Tier 1 support will escalate directly to Tier 3 or onsite.

OceanWATCH
MSP Automation / Support Tools

The foundation of a successful service strategy are the tools used to manage, collect, and disseminate information to our internal team. Ocean Computer Group, Inc. is focused on providing an array of systems engineering tools and associated techniques for designing, controlling, and improving the overall IT health of our customers. Here are some of the best in breed products we use in our portfolio:

- 24x7 System, Security and Network Monitoring
- 24x7 Onsite for Critical Failures
- Critical and Emergency Notifications
- Alert client to critical conditions, failures, patches
- Secure Password Management
- Change Management
- Help Desk and Ticketing
- Infrastructure Management
- Remote support
- Faster time to resolution
- Project planning and management
- Automation
- Patching
- Reporting

ConnectWise is a Professional Services Automation tool (PSA). It allows our MSP customers to receive better, faster service including resource scheduling and on-time project delivery. The ticketing system documents all details of projects, requests, and issue resolutions through the automated helpdesk and customer portal which maintains collaboration and communication across departments and teams.

Kaseya is a market leader in remote monitoring and management (RMM). Kaseya integrates tightly with ConnectWise and provides remote access to devices allowing issues to be remediated quickly, reducing travel to each location. The tool provides automated audit reports at the push of a button, keeping auditors satisfied and systems in compliance. Streamlined IT efficiency enables the entire IT infrastructure to be managed through a single-pane-of-glass view.

Auvik allows Ocean Computer Group to efficiently and effectively manage ethernet networks. Networks are incredibly complex and managing them has traditionally involved many time-intensive manual tasks Auvik provides real-time mapping of your network, includes automated inventory that creates a profile for every device on a network. We build out your network documentation, showing how everything on the network is connected, provide a list of all the IP addresses in use, and the devices using them.

Dark Web ID helps identify, analyze, and proactively monitor compromised or stolen user credentials and data. It proactively performs identity monitoring for employees and monitors the dark web for compromised credentials and sensitive data notifying you when problems arise.

Rapid Fire is an overall IT assessment tool to discover Domain controllers, applications and operating systems, AD health, server and PC aging, security permissions, etc. It provides complete awareness of the state of the network at any given time.

Passportal provides simple yet secure password and documentation management. The platform is cloud-based and offers automated password protection and makes storing, managing, and retrieving passwords & client knowledge quick and easy from virtually any connected device.

TruMethods' software, myITprocess, is the industry's first technology success platform that manages your IT standards library, and helps you easily perform alignment reviews and builds an IT roadmap, strategy, and budget.

The SonicWall Capture Cloud Platform tightly integrates security, management, analytics and real-time threat intelligence across the company's portfolio of network, email, mobile and cloud security products. This approach enables our complete portfolio of high-performance hardware, virtual appliances, and clients to harness the power, agility and scalability of the cloud.

Our Framework is a Dedicated MSP Process

Ocean Computer Group has adopted a set of standard principles guidelines for onboarding new customers. As part of our onboarding process, we execute an assessment of your current IT environment and compare it with industry and sector best practices.

The assessment is a mix of tools and a proven standards library that will focus on **'6 critical areas'** of your IT environment covering over **250 questions** in the following areas:

- Cyber Security (15-point & NIST Cyber Security Framework)
- Core Infrastructure
- Server Infrastructure
- Business Continuity
- Software
- Hardware

The results of the assessment will help to identify critical issues that should be addressed right away and assist in creating a long-term strategic IT roadmap with the **CLIENT NAME**.

Listed below is a sample of the standards library utilized by Ocean Computer Group, Inc. during our onboarding phase:

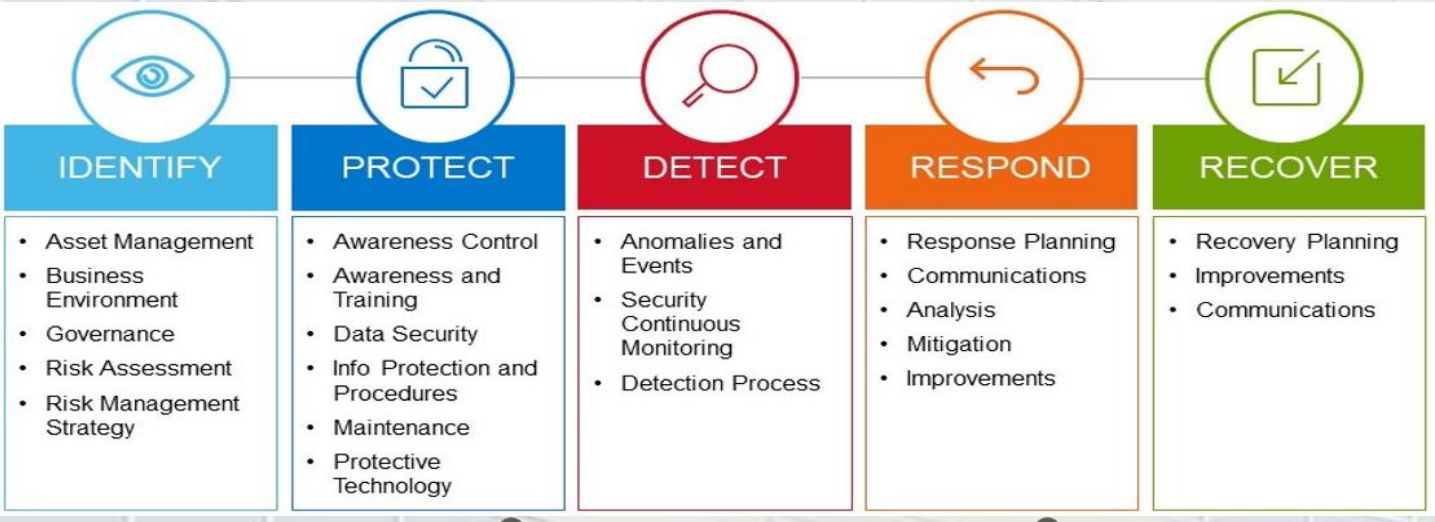
Type	Name	Question Priority	Question
SECTION - SECURITY			
Category: Physical Security			
Question	Dedicated Room	High	The server room is isolated and not used for any other business-related functions (files, employee office space, etc.)?
Question	Server Room Access	High	Access to the server room is limited to personnel who require such permissions?
Question	Physical Security Protection Mechanisms	High	The appropriate physical security protection mechanisms are in place for the server and its networking components such as locks, card reader access, security guards, or physical intrusion detection systems (cameras, motion sensors)?
Question	Physical Access Availability	High	The door to the server room is locked at all times?
Question	Server Hardware Locking Mechanism	Medium	Servers are physically located in a lockable server rack or cabinet?
Question	Elevated Equipment	High	Equipment is elevated off of the floor?
Category: Password Policy & Procedures			
Question	Organizational Password Policy	High	Is a secure password policy in place?
Question	Password Length	High	Does the password policy require a minimum length of 8 or more characters?
Question	Password Complexity	High	Does the password policy require minimum complexity (capital letters, numbers, symbols)?
Question	Password Aging	High	Does the password policy require passwords be changed after a specified number of days?
Question	Password Reuse	High	Does the password policy prevent passwords to be reused?
Question	Password Security	High	Does the password policy have unencrypted passwords or reversible encryption disabled?
Question	Password Expiration	High	User passwords are set to expire after a specified amount of time?
Question	Password Authority	High	The password policy designates who is allowed to change or reset passwords AND if proof is required before initiating any changes?
Question	Password Lockout Policy	High	The password policy denies future logins for a set period of time after a specific number of failed attempts?
Question	Last Logon	Medium	Last Login is enabled in Group Policy?
Question	Single Sign On	Medium	Single Sign On is enabled with any Active Directory integrated software?
Question	Inactive Session Timeout	High	Inactive user sessions are automatically locked after a designated period of time?
Question	Inactive User Accounts	High	User accounts not used in the last 90 days have been disabled?
Category: Other Policies & Procedures			
Question	Access Controls	High	File access controls are implemented to enforce separation of duty and unauthorized user access?
Question	Data Accessibility	High	A policy is in place to periodically examine the services and information accessible on the server and to determine necessary security requirements?
Category: Antivirus			
Question	Antivirus / Antimalware Management	High	Antivirus and antimalware software is centrally managed?
Question	Antivirus Updates	High	Software updates antivirus definitions every 24 hours?
Question	Active Scanning	High	An active scan is performed at least once per week?
Question	EDR	High	Is there an Endpoint Detection and Response Solution in place

15-POINT NIST Cyber Security Approach

The Framework provided by NIST assists in determining which areas are most important to focus on to manage and minimize cyber security risk, protect critical infrastructure, and protect your assets. This framework also helps prioritize investments and maximize the impact of each dollar spent on cybersecurity.

OceanWATCH uses a risk-based approach to protecting our clients from a cyberattack to help you determine what cybersecurity investments are adding value to your organization.

The NIST framework is broken down into 15 core areas that if not correctly addressed, present a risk or vulnerability to your organization. We leverage leading processes and solutions which will increase your protection and reduce your risk.



1 Advanced Endpoint Detection & Response
Protect your computers data from malware, viruses, and cyber-attacks with advanced endpoint security. Today's latest technology (which replaces your outdated anti-virus solution) protects against file-less and script-based threats and can even rollback a ransomware attack.

2 Backup
Backup local. Backup to the cloud. Have an affine backup for each month of the year. Test your backups often.

3 Dark Web Research
Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach. We scan the Dark Web and take action to protect your business from stolen credentials that have been posted for sale.

4 Encryption
Whenever possible, the goal is to encrypt files at rest, in motion (think email) and especially on mobile devices.

5 Firewall (Edge Security)
Leverage cloud sandboxing, DPI/SSL Inspection and IDS/IPS features. Turn on Intrusion Detection and Intrusion Prevention features. Send the log files to a managed SIEM.

6 Mobile Device Security
Today's cyber criminals attempt to steal data or access your network by way of your employees' phones and tablets. They are counting on you to neglect this piece of the puzzle. Mobile device security closes this gap.

7 Multi-Factor Authentication
It adds an additional layer of protection to ensure that even if your password does get stolen, your data stays protected.

8 Passwords
Apply security policies on your network. Examples: Deny or limit USB file storage access, enable enhanced password policies, set user screen timeouts, and limit user access.

9 Security Assessment
It is important to establish a baseline and close existing vulnerabilities.

10 Security Awareness
Train your users - often! Teach them about data security, email attacks, and your policies and procedures. We offer a web-based training solution and "done for you" security policies.

11 SIEM/Log Management
(Security Incident & Event Management)
Uses big data engines to review all event and security logs from all covered devices to protect against advanced threats and to meet compliance requirements.

12 Spam & Malware Protection
Secure your email. Leverage next generation anti-virus tools to secure your email. Most attacks originate in your email.

13 Updates & Patching
Keep Microsoft, Adobe, and Java products updated for better security. We provide a "critical update" service via automation to protect your computers from the latest known attacks.

14 Web Gateway Security
Internet security is a race against time. Cloud based security detects web and email threats as they emerge on the internet and blocks them on your network.

15 Cyber Security Insurance Used to protect your business and individual users from Internet-based risks, and more generally from risks relating to information technology infrastructure and activities.

OceanWATCH Deliverables

DESCRIPTION	FREQUENCY	INCLUDED
Help Desk and Remote Management		
Access to ConnectWise Ticketing System	Ongoing	Yes
Assign dedicated account manager	Ongoing	Yes
Create, manage, and update technical documentation	Ongoing	Yes
Remote network management	24x7	Yes
Remote server management	24x7	Yes
24x7x365 network monitoring		Yes
Quarterly Review		
Provide Quarterly Service History Reports	Quarterly	Yes
Provide and review technology consulting & Planning services	Quarterly	Yes
Provide Quarterly Trending Reports	Quarterly	Yes
Recommend areas of improvement for better user experience	Quarterly	Yes
Servers & Workstations		
Proactively Monitor & Manage Servers for uptime and availability	Ongoing	Yes
Help Desk Support (8:00am – 5:00pm / Monday – Friday)	As needed	Yes
Support Microsoft Supported operating systems	As needed	Yes
Support Microsoft supported office applications	As needed	Yes
Onsite support for issues that cannot be resolved remotely	As needed	Yes
24x7 On-site Emergency Support – Critical Issues	As needed	Yes
Manage Server and Workstation Anti-virus updates	Ongoing	Yes
Manage Active Directory account policies	Ongoing	Yes
Monitor Active Directory replication	Ongoing	Yes
Monitor critical Windows Server Services	Ongoing	Yes
Reboot servers if needed	As needed	Yes
Update Server Hardware Firmware	As needed	Yes
Scheduled off time server maintenance	As needed	Yes
Install supported Operating System Service Packs and Patches – Workstations	Monthly	Yes
Install supported Operating System Service Packs and Patches – Servers	Quarterly	Yes
Install Critical Operating System Service Packs and Patches	Ongoing	Yes
Set up/maintain Active Directory groups (accounting, admin, printers, sales, warehouse, etc.)	As needed	Yes
Alert Client to critical conditions, failures, patches	Ongoing	Yes
Monitor Memory Usage to maintain uptime and performance	Ongoing	Yes
Monitor Hard drives for failures that can cause outages	Ongoing	Yes
Monitor and manage Hard drive disk space	Ongoing	Yes
Monitor Server resources for failures or outages	Ongoing	Yes
Mobile Phone Support for email and Microsoft Authenticator	As needed	Yes

OceanWATCH Deliverables (con't)

DESCRIPTION	FREQUENCY	INCLUDED
Backup & Disaster Recovery		
Monitoring success of daily backup	Ongoing	Yes
Check and validate status of backups procedures	Ongoing	Yes
Manage, optimize and maintain replication	Ongoing	Yes
Targeted test restores of backup data	Bi-Yearly	Yes
Security		
Performance monitoring/capacity planning	As needed	Yes
Monitor Internet availability	Ongoing	Yes
Check and Manage firewall logs for errors, critical issues, or threats	If applicable	Yes
Remote Firewall Management and updates	Ongoing	Yes
Create new directories, shares and security groups, new accounts, disable/delete old accounts, manage account policies	As needed	Yes
Manage Server Permissions and file system management	Ongoing	Yes
Set up new users, including login restrictions, passwords, security, applications	As needed	Yes
Assist with on-boarding and off-boarding users	As needed	Yes
Self Service Password Reset Service	Ongoing	Yes
Automated Password rotation, identify management and account unlocks.	Ongoing	Yes
Manage, maintain, and remediate SSO and MFA	Ongoing	Yes
DarkWeb Monitoring Monitoring at no extra cost. This service will help identify, analyze and proactively monitor for compromised or stolen user credentials and data.	Ongoing	Yes
End User Email Security and Awareness Training Guards against social-engineering threats with quarterly simulation and training for employees. Exposing them to the latest attack techniques and teach them to recognize the subtle clues and help stop email fraud, data loss, and brand damage.	Ongoing	Yes
Set up and change security for users	As needed	Yes
Remediation of Viruses and Malware Encryption	As needed	No
Core Network		
WAN / LAN Network Monitoring (Auvik) The software provides instant visual insight into the infrastructure networks and automates complex and time-consuming network management tasks.	Ongoing	Yes
Manage network connectivity to firewalls, wireless and related services	Ongoing	Yes
Maintain network connectivity, manage vlans, QoS and manage VPNs.	Ongoing	Yes
vCIO Services		
Conduct a full audit of the client's environment	Ongoing	Yes
Understand business goals and align with IT services	Ongoing	Yes
Identify the challenges they are facing in their key drivers	Ongoing	Yes
Develop a dynamic technology roadmap	Ongoing	Yes
Conduct yearly and quarterly technology and security reviews	Ongoing	Yes

Onboarding Milestones: Onboarding & Assessment

The Initial onboarding of BOROUGH AND PD OF SOUTH TOMS RIVERwill start with the deployment of tools and assessments that will allow Ocean Computer Group, Inc. to assess the present state of the network, create baseline documentation and lay the groundwork for the first 90 days.

Below are the management tools that will be deployed during the onboarding process of our OceanWATCH program:

CONNECTWISE

ConnectWise is used as our ticketing system to document all details of projects, requests, and issue resolution.

- Automates helpdesk
- Maintains Collaboration and Communication Across Departments and Teams
- Powerful reporting for all your projects

KASEYA

Kaseya is used by our team to perform Remote Management and Monitoring that allows them to perform many tasks as if they were on-site. Some of these may include:

- Access to diagnose and remediate issues
- Install software and administer upgrades
- Patch management for workstations and servers
- Proactively alert impending events

AUVIK

Through Auvik we have a real-time map of your network that proactively notifies us and allows us to remediate items quickly. Capabilities of this application are:

- Automated inventory, that creates a profile for every device on a network.
- Network documentation, showing how everything on a network is connected.
- IP address management, providing a list of all the IP addresses currently in use and which devices are using them.

RAPIDFIRE

A complete set of IT assessment, documentation, and reporting tools. Tools for IT compliance process automation. Tools for insider Cyber threat detection and alerting.

- Network Detective
  - IT Assessments Made Fast & Easy.
  - Run Non-Intrusive IT Assessments On-Site, in less than an hour.
  - Capture Threat Assessment (CTA)
    - The CTA will identify any internet traffic or potential threats that are evading the current firewall implementation. The CTA will also identify internet user behavior that should be addressed.

LIVE OPTICS

- Live Optics is an online software utilized to collect, visualize, and share data about your IT environment and workloads. Live Optics provides data analysis to help us understand our workload performance, so that we can simplify discovery and have a mutual understanding of project requirements.

Onboarding Milestones: First 90 Days / First 12 Months

FIRST 90 DAYS
Meet with the Township of Plumsted Stakeholders
Evaluate and Document current Backup strategy
Lock down / change administrative usernames and passwords
Create and implement patch strategies and schedules
Create up to date network diagram
Setup secure password database using Ocular
Implement Help Desk and ticket resolution escalation
Setup and Communicate help desk process
Review and document Antivirus
Active Directory • Determine health • Remove or disable inactive accounts • Review password policy • Review Group policies • Validate Admin access
Equipment labeling and inventory
Document manufacturer support contracts
Perimeter Security • Capture threat assessment (CTA) • Document remote access • Document topology and implementation
Email • Evaluate effectiveness of Spam and malware protection • Evaluate effectiveness of Advanced threat protection • Backup Status • Archiving Status
Meeting with the Township of Plumsted to review the findings and discuss recommendations.

FIRST 12 MONTHS
The main objective of the first 12 Months is to work with the CLIENT Stakeholders to:
Successfully complete onboarding and assessments
Successfully define lines of communication between the Township of Plumsted and Ocean Computer Group
Meet with the Township of Plumsted Stakeholders to understand needs and business initiatives.
Work with and educate the Township of Plumsted endusers on how to obtain service.
Plan and implement patching schedule
Identify any areas where the Township of Plumsted IT infrastructure does not meet standards.
Work with the Township of Plumsted Stakeholders to remediate these areas
Perform quarterly vCIO reviews
Work with the Township of Plumsted Stakeholders to define any planned projects
Work with the Township of Plumsted Stakeholders to define projects / business initiatives for the next 12 months