MSP Scope of Services

Version: 2020.1
Last updated: 7-17-2020
Website: https://www.uscomputer.com/descriptions/

Managed Service Plans

Proactive Care Plan Executive (PCPE)

PCPE is our fully managed solution. PCPE provides unlimited IT service, helpdesk, and on-site support during business hours for a flat monthly rate per device. PCPE is designed for the company that needs a complete IT department experience, without having to hire anyone. We provide full IT management of your existing network and full IT support during and after installation and migration of a new or upgraded network.

Included in the PCPE plan:

- Unlimited IT Helpdesk and on-site support during normal business hours (Mon-Friday 8:00AM to 5:00PM EST)
- IT management of PCPE Workstations, PCPE Servers, and PCPE Hypervisors.
- Client approved Basic Security Recommendations (BSRs).

Billable items not included in the PCPE Plan:

- Projects (server migrations, email migrations, office moves, working with software and hardware vendors to implement their software and/or equipment, etc.)
- Implementation of approved Basic Security Recommendations.
- Billable overtime for client requests that fall outside normal business hours, projects, emergencies, etc.
- On-site support at client's remote location(s) located outside of Fairfield and New Haven Counties in CT and Westchester County in and if USCC dispatches a local resource to support the remote location.

Services not included in the PCPE plan and not provided by USCC:

- See Shared Cyber Security Responsibility

PCPE Workstations

The Proactive Care Plus Executive (PCPE) Workstation plan includes

- Monitoring and alerts of Antivirus, Hardware Health, Disk Space, and Operating System Performance
- Automatic deployment of whitelisted Microsoft Critical and Security Patches

- Webroot Antivirus license

PCPE Servers

The Proactive Care Plus Executive (PCPE) Server plan includes

- Monitoring/alerts of Active Directory, Antivirus, Citrix, DHCP, Disk Space, DNS, Hardware Health, Hyper-V, Microsoft Exchange Server, Microsoft SQL Server, Operating System Performance, Service Health, and VMware
- Automatic deployment of whitelisted Microsoft Critical and Security Patches
- Webroot Antivirus license

PCPE Hypervisors

The Proactive Care Plus Executive (PCPE) Hypervisor plan includes

- Health monitoring and alerts of VMware ESXi host

Proactive Care Plan (PCP)

PCP is our modified managed services program. PCP offers a low flat monthly rate for your computers and servers. PCP clients select a block of pre-purchased hours that can be used for helpdesk, on-site support, and general IT service. PCP is designed for companies that want an active role in managing their network. It works best for companies that need outsourced Supplemental IT Services to complement an internal IT Professional employee that provides Helpdesk Support.

Included in the PCP plan:

- IT Helpdesk and on-site support during normal business hours (Mon-Friday 8:00AM to 5:00PM EST) deducted from the pre-purchased block of hours.
- IT management of PCP Workstations, PCP Servers, and PCP Hypervisors.
- Client approved Basic Security Recommendations.

Billable items not included in the PCP Plan, can be deducted from the pre-purchased block of hours:

- Projects (server migrations, email migrations, office moves, etc.)
- Implementation of approved Basic Security Recommendations (BSRs)
- Billable overtime for projects, emergencies, client requests that fall outside normal business hours, etc.
- If USCC dispatches a local resource to support the remote location, then that time will be billable to the client as well.

Services not included in the PCP plan and not provided by USCC:

- See Shared Cyber Security Responsibility

Block of Hours expire after 2 years from date issued.

PCP Workstations

The Proactive Care Plus (PCP) Workstation includes

- Health monitoring/alerts of Antivirus, Hardware Health, Disk Space, and Operating System Performance
- Automatic deployment of whitelisted Microsoft Critical and Security Patches
- Webroot Antivirus license

PCP Servers

The Proactive Care Plus (PCP) Server includes

- Health monitoring/alerts of Active Directory, Antivirus, Citrix, DHCP, Disk Space, DNS, Hardware Health, Hyper-V, Microsoft Exchange Server, Microsoft SQL Server, Operating System Performance, Service Health, and VMware
- Automatic deployment of whitelisted Microsoft Critical and Security Patches
- Webroot Antivirus license

PCP Hypervisors

The Proactive Care Plus (PCP) Hypervisor includes

- Health monitoring/alerts of VMware ESXi host

Managed Service Plan Comparisons

Managed IT Services	PCPE	PCP
24x7 Server & Workstation Monitoring & Alerts of Health, Hardware, and Performance	✓	✓
Microsoft Critical & Security Updates	✓	✓
Antivirus Protection	✓	✓
Sourcing & Procurement	✓	✓
IT Helpdesk & Onsite Support during normal business hours (Monday-Friday 8:00am to 5:00pm EST)	Unlimited	Block of hours
IT Helpdesk & Onsite Support during non-business hours	Billable OT	Billable OT
IT Project Management	**PCPE**	**PCP**
Strategic Consulting	T&M	T&M
Expert Technology Advice & Consulting	T&M	T&M
Network Design & Implementation	T&M	T&M
Basic Security Recommendations (BSRs)	T&M	T&M
Server and Email Migrations	T&M	T&M
Infrastructure Upgrades & Migrations	T&M	T&M
Secure Enterprise Wireless Solutions	T&M	T&M
Office Relocation & Planning	T&M	T&M
Data & Voice Network Cabling	T&M	T&M
Cyber Security Offerings	**PCPE**	**PCP**
NextGen Firewalls	Add-On	Add-On
Endpoint Protection	Add-On	Add-On
Multi-factor Authentication	Add-On	Add-On
Advanced Spam Filter Protection	Add-On	Add-On
HIPAA Compliant Email Encryption	Add-On	Add-On
Strong Password Policy Implementation	T&M	T&M
Full Disk Encryption	Add-On	Add-On
Security Awareness Training	Add-On	Add-On
Media Sanitization (DoD 5220.22M or Physical Destruction)	T&M	T&M
Log Management for Compliance	Add-On	Add-On
Mobile Device Management (MDM)	Add-On	Add-On
Business Continuity & Disaster Recovery	**PCPE**	**PCP**
Server Backup	Add-On	Add-On

Office 365 & G Suite Backup	Add-On	Add-On
Computer Backup	Add-On	Add-On
Cloud Computing	**PCPE**	**PCP**
Public & Hybrid Cloud Solutions	Add-On	Add-On
Cloud-based Email & Software (SaaS) Solutions	Add-On	Add-On
Scalable Solutions that Grow with Your Needs	Add-On	Add-On
Remote Access: Work from Anywhere	Add-On	Add-On
VoIP	Add-On	Add-On

Shared Cyber Security Responsibility

What is an MSP?

A Managed Service Provider (MSP) is a trusted outsourced IT provider (an IT company) that provides technical support to an organization to ensure IT Systems are operational. As an MSP, U.S. Computer Connection (USCC) can help organizations with:

- Helpdesk support to troubleshoot technical computer, server, network, email, etc.
- Limited technical support and troubleshooting for line of business application issues.
- Remote monitoring of computer and server hardware health and uptime
- IT Advisor for computer, server and network infrastructure upgrades
- Microsoft Critical and Security updates
- Antivirus Protection
- Spam filter for enhanced email security
- Install Firewalls with active security services and make changes as/when requested. However, firewalls are not actively monitored.
- Basic Security Recommendations (this is not a risk assessment or security audit) to inform the client of identified risks and deficiencies uncovered while providing IT services and technical support. Implementation is subject to client approval.

MSPs manage IT systems and networks to ensure they are operational; they provide technical advice for growth, efficiency and security as well as provide technical support.

What is an MSSP?

A Managed Security Service Provider (MSSP) is an outsourced Security Service provider that helps organizations with their Cybersecurity, legal and regulatory compliance needs. MSSPs help organizations with:

- Cybersecurity related services
- Managed Cybersecurity
- Active Log Management and Monitoring
- Compliance Services

- Forensic Investigations
- Managed Intrusion Detection/Prevention Systems (Firewalls)
- Managed Security Services
- Managed Security information and event management (SIEM)
- Penetration Testing
- Risk Assessments and Analysis
- Software as a Service (SaaS) Vendor Security
- Security Consulting Services
- Security Monitoring
- Security Operations Center as a Service (SOCaaS)
- Third-Party Risk Assessments
- Vulnerability Management
- Security Audits/Reviews.
- Etc.

MSSPs can help an organization with the legal, regulatory and compliance needs. They concentrate on IT Security based on the needs of the client.

U.S. Computer Connection LLC (USCC)

U.S. Computer Connection's Responsibility: to communicate any security weaknesses, vulnerabilities, and/or deficiencies identified in the process of providing IT services with the client (your organization).

U.S. Computer Connection (USCC) is a Managed Service Provider (MSP), an IT company that focuses on Cybersecurity, **however, it is not** a Managed Security Service Provider (MSSP). We bring value to our clients by providing IT services that help support the mission and business objectives of their organization. To help protect our clients from the Cybersecurity Threat landscape and help them increase their security posture, we provide Basic Security Recommendations (not to be considered a full/structured Risk Assessment, a Risk Assessment, or a Security Review/Audit). This empowers our clients to make informed risk management decisions based on identified items, organizational needs, and internal/external requirements. These recommendations are not to be considered a risk assessment, security audit or security review. These are internal functions each client must perform on their end as part of due care and due diligence. The client then reviews our recommendations, and based on their Risk Management approach, implements controls based on their level of acceptable risk for their organization.

Companies are subject to different Legal, Regulatory and Contractual requirements in terms of Cybersecurity. Our Basic Security Recommendations are only a subset of items an organization would find are applicable and addressable during their own internal full/structured Risk Assessment. We establish and maintain a mutually beneficial partnership with clients who are

risk averse and decide to mitigate/lower risks by implementing appropriate security controls, which helps them exercise due care and due diligence.

See Basic Security Recommendations (BSRs) for a list of recommendations USCC may provide to a client upon their request.

Clients needing services provided by an MSSP should be aware that USCC does not provide such services.

Client

An organization that retains an MSP (IT Company) is outsourcing its technical support needs, however, the organization is still responsible for the management of their cybersecurity needs to ensure they meet their specific legal, contractual, and regulatory requirements. The client's organization is ultimately responsible for:

- Protecting the data they collect, process, store, or transmit. An MSP or MSSP can make recommendations, but it is up to the organization to approve them and ensure the security controls meet their requirements are enforced.
- Seeking legal advice to determine the legal, regulatory, and contractual obligations the organization is subject to, and how to best comply with them.
- Establishing, managing and monitoring a Cybersecurity program that meets their needs. Some functions may be outsourced, however, the client's organization is ultimately responsible to ensure overall protective efforts are effective.
- Performing risk assessments, risk analysis, and risk management.
- When an MSP or MSSP identifies a vulnerability that represents a risk to the client, the organization is then responsible for performing risk management and determining how to respond to the proposed security controls. Most security controls have an associated cost that must be budgeted for.
- Ensuring they meet legal, regulatory, and contractual obligations in terms of cybersecurity, and advise their MSP and/or MSSP of any specific needs they have.
- Presenting the MSP and/or MSSP with any Risk Assessments that require action on their end.
- Informing the MSP and/or MSSP of any cybersecurity incidents that require their immediate attention.
- Requesting that U.S. Computer Connection LLC (USCC) to provide them with Basic Security Recommendations (BSRs), otherwise, these are presented to clients as they become apparent in the process of providing IT services.

Client Organization's Responsibility: In alignment with your organization's mission, vision, goals, and business objectives, and as part of due care and due diligence, organizations need to take appropriate steps to protect all sensitive data that they process, store, or transfer. It is the

responsibility of each organization to manage its Governance, Risk, and Compliance (GRC) requirements. Including, but not limited to:

Governance: identifying legal, regulatory, and industry requirements that apply to your organization.
Risk: performing Risk Assessments, Analysis, and Management. Determining the risk treatment (accept, mitigate, avoid, transfer) for each identifying risk based on your organization's capabilities, risk appetite, and business requirements.
Compliance: establish compliance goals, manage efforts, and monitor compliance efforts with identified applicable external requirements such as HIPAA, PCI, GLBA, GDPR, State Laws, etc.

No security control is 100% effective 100% of the time, therefore a defense-in-depth approach is necessary to help protect organizations. Any presented Basic Security Recommendations (BSRs) are security controls that your organization can implement, please note they are a small subset of items that can be implemented to help secure a network. As part of due diligence and due care, your organization's internal Compliance Officer should perform a Risk Assessment/Analysis to determine what security controls are needed to properly protect your organization's people, processes, and technology.

Your organization can choose to implement any of the BSRs based on your current capabilities and risk appetite and should perform a full Risk Assessment to identify all applicable risks to your organization and determine risk treatment.

U.S. Computer Connection cannot be held liable for data/security breaches or losses caused due to a client declining to implement recommended basic security controls in order to help protect their systems, data, and employees.

As the following items become available/known to your organization, please help us better serve you by making USCC aware by emailing support@uscomputer.com.
• Any legal and regulatory requirements your organization is subject to. For example, HIPAA, PCI, GLBA, etc.
• Type and location of your most sensitive data. This will allow us to work with you and present BSRs.
• Contact information for your CISO, Compliance Officer, etc. This will allow us to coordinate protection efforts.
• Please let us know if your organization has performed a Risk Assessment/Analysis, and if there are any items that require our attention. We can provide you with a secure link for you to upload this sensitive document.
• It is industry standard for all organizations to have Cyber Insurance, please let us know if you need help answering questions for Cybersecurity questionnaires.

CLIENTS NEED TO EXERCISE DUE CARE AND DUE DILIGENCE IN THEIR EFFORTS OF PROTECTING ANY SENSITIVE DATA THAT THEY PROCESS, STORE, OR TRANSFER.

Basic Security Recommendations (BSRs)

- USCC is an MSP, not an MSSP or a SOC.
- Labor outside the initial quoted implementation will be a billable project.

Network Protection

Strong Password Policy Implementation

Benefits:

- Helps prevent data breaches because of weak passwords.
- Can integrate with Azure Active Directory (AD) for SSO, and Mimecast.
- Two Factor Authentication (2FA) (Workstation, Email, etc.) is an industry best practice, and the only protection against compromised credentials. USCC strongly recommends 2FA to all its clients.
- If using Office 365, Azure AD Sync is an option to help deploy Single-Sign-On (SSO) and ensure strong passwords are used.

Scope of implementation, subject to client approval:

- Coordinate & implement minimum password length, complexity requirements and how often passwords must be changed. The client is provided with a Password Policy document with industry best practices for their modification and approval.
- Review all Accounts in AD to ensure all passwords are changed.
- Coordinate with the client to enforce end-user password change and assist as needed.
- USCC cannot accept, store, or keep user credentials.

Services not provided by USCC:

Active Azure Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with these function.

Ninite Pro

Benefits:

- Helps safeguard computers from being compromised by vulnerabilities of outdated 3rd Party software i.e., Adobe Reader, Java, Chrome, Firefox, etc.
- Enables easy (not automatic) upgrades to new versions and automatically updates Adobe Reader, Java, Chrome, etc. to latest version.

Scope of implementation, subject to client approval:

- Deploy Ninite Pro agent to all Client computers and servers.
- Evaluate policy "Automatically update everything", then set all devices to that policy if appropriate.
- Create a new policy with exceptions if necessary.
- Configure automatic agent deployment via a Group Policy Object (GPO) or Remote Monitoring and Management (RMM) agent.
- Upon client request, upgrade older versions of installed software.

Services not provided by USCC:

- Proactively upgrading software to new versions.

SonicWALL Security Services

Benefits:

- Inhibits network attacks for devices that are behind the Firewall.
- Network level Intrusion Prevention System (IPS), Anti-Spyware, Gateway Anti-Virus.

Limitations:

- Logs are limited to memory availability on the SonicWall. Device overwrites when memory is full or upon device reboot. Logs are normally overwritten within 48 hours.
- Analyzer or another SIEM is needed for log retention beyond 48 hrs.
  Daily or continuous log review auditing is not a service USCC provides.

Scope of implementation, subject to client approval:

- The SonicWall Firewall Security Services are configured as per the "MSP – SonicWALL Security Services Deployment and Renewals" standard. USCC does not provide Actively Managed Firewalls, it only provides professional services to configure the Firewalls at the client request.
- Opening ports on the Firewall follow the Principle of Least Privilege (PoLP), in which only the minimal number of ports are opened to the minimal external IP addresses.
- A backup of the SonicWALL configuration is created before and after every change.
- USCC performs authorized changes on the Firewall when requested by the client.
- USCC has a procedure where any changes that lower the security of a Firewall are subject to change management approval prior to the changes being made.

- Firmware upgrades are performed as needed in the process of providing IT services.

Limitations

- There is no mechanism for Automatic Firmware upgrades. They are done as necessary as part of troubleshooting or upon client request.

Services not provided by USCC:

- Active Firewall Management, Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.

OpenDNS / Cisco Umbrella

Benefits:

- Helps detect and block malicious outbound Botnet traffic and assists in detecting compromised computers.
- Helps protect laptops outside of the office when they are beyond the protection of the Firewall.
- Log retention is 30 days.
- Optional Content Filtering capabilities can help enforce company policies.

Scope of implementation, subject to client approval:

- Deploy Cisco Umbrella (OpenDNS) agent and Certificate to all Client computers and non-DC servers.
- Configure automatic agent deployment via GPO or RMM agent.
- Work with client to implement optional content filtering categories.

Services not provided by USCC:

Active Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.

Enterprise Wi-Fi & Wi-Fi Isolation

Benefits:

- Helps secure your network and data by providing the ability to separate employees and cell phones / guests from the production network.
- Creates an isolated guest network that is separate from your production network.

Scope of implementation, subject to client approval:

- Work with client for hardware installation and location.
- Configure 2 wireless networks: a production network with a 25+ randomly generated character password, and a Guest network isolated from the production network.

- Production password changes can be made upon client request, which will be a billable project. It will require to setup a new wireless name and all production devices to join that new wireless network.
- Firmware upgrades are performed as needed in the process of providing IT services.

Limitations

- There is no mechanism for Automatic Firmware upgrades. They are done as necessary as part of troubleshooting or upon client request.

Services not provided by USCC:

Active Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.

Business Continuity & Disaster Recovery

Datto Backup (Local & Offsite Backups)

Benefits:

- Helps provide a reliable local & cloud backup solution for your data.
- Server Full Block-level backups.
- Local and cloud virtualization capabilities (some models excluded).
- Encryption-at-rest of the backup with Passphrase Encryption.

Scope of implementation, subject to client approval:

- Evaluate protected data size and determine Datto unit size based on 3.5 times the size of protected data for encrypted agents.
- Install Datto agent on servers to be backed up, add passphrase encryption with a 30+ randomly generated character password.
- Configure off-site sync, screenshots, and device hardware alerts.
- Monitor server backups to ensure they take place. *
- Automated daily local server backup screenshots validate the backup.

Out of scope and billable:

- Full local/offsite server restores and virtualizations are billable.
- Off-site-cloud virtualization and full disaster recovery tests are done upon client request as a billable project.
- Proactive disaster recovery, server virtualizations, and off-site virtualization testing is billable done upon client request.

Services not provided by USCC:

- Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.

s

Datto Backup + Passphrase Encryption

Benefits:

- Requires a password to access the backups locally and in the cloud, Industry standard requirement.
- Helps comply with laws and regulations that require Encryption-at-Rest for data backup such as HIPAA, PCI, GLBA, State Laws, etc.
- Encryption requires more hard drive space on the Datto backup unit.

Office 365 Backup

Benefits:

- Facilitates backup of Office 365 e-mail and SharePoint sites.

Scope of implementation, subject to client approval:

- Work with client to obtain SharePoint sites to be backed up.
- Implement approved Office 365 backup.

Out of Scope and Billable:

- Restore emails/files upon client request. *

Services not provided by USCC:

- Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.

Google Suite Backup

Benefits:

- Facilitates backup of G Suite: Gmail, Calendar, Contacts, Drive, and Team Drives.

Scope of implementation, subject to client approval:

- Work with client to obtain scope items to be backed up.
- Implement approved G Suite backup scope.

Out of Scope and Billable:

- Restore emails/files upon client request. *

Services not provided by USCC:

Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.

Laptop Backup – Carbonite Safe Backup Pro

Benefits:

- Facilitates backup of critical information on your laptop into a HIPAA Compliant backup solution (Carbonite Safe Backup Pro/Core).
- For organizations that have Legal Hold requirements, a different version of Carbonite is necessary.

Scope of implementation, subject to client approval:

- Install Carbonite on computers identified by the client.
- Enable 2FA on the Carbonite account.

Out of Scope and Billable:

- Restore files upon client request. *

Services not provided by USCC:

- Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.

Log Management for Compliance

SonicWALL - Analyzer

Benefits:

- Helps meet Firewall logging legal and regulatory compliance requirements.
- Collect and store SonicWall logs on a Server.
- Requires dedicated Server, which requires additional backup space.

Scope of implementation, subject to client approval:

- Determine minimum server software and hardware requirements.
- Install Analyzer software on suitable client server, install and configure new server if approved.
- If requested by client, configure reports to be emailed to the client.

Services not provided by USCC:

- Daily or continuous log review auditing.
- Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.

Windows/PCs - Manage Engine AD Audit

Benefits:

- Helps meet Windows Servers and Computer events and logins logging legal and regulatory compliance requirements.
- Requires dedicated Server.
- Ability to generate limited alerts and reports.
- Useful for compliance reports and investigations.

Scope of implementation, subject to client approval:

- Determine licensing requirements.
- Install Manage Engine ADAudit Plus on a DC and configure as per USCC Standard.
- If requested by client, configure reports to be emailed to the client.
- Quote and renew license yearly.

Out of Scope and Billable

- Upon license renewal or client request, apply software updates.
- Create reports/alerts upon client request.

Out of scope, services not provided by USCC:

- Daily or continuous log review auditing.
- Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.

End-User Protection

Folder Redirection for Documents & Desktop

Benefits:

- Helps protect critical user data by storing the Documents, Desktop and Favorite folders on the server.
- Requires adequate space on the server.
- Laptops should use Carbonite Safe Backup Pro.

Scope of implementation, subject to client approval:

- Configure Folder Redirection Network Share as per USCC Standard.
- Work with client to deploy folder redirection which may require end-user interaction to move files.
- USCC cannot accept, store, or keep user credentials.

Services not provided by USCC:

- Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.

Advanced Spam Filter Protection – Mimecast S1/M2/M2A

Benefits:

- Helps protect your organization from spam, phishing, malicious links, attachments and impersonation attacks that can lead to significant business losses and reportable data breaches.
- Targeted Threat Protection (TTP) includes Attachment, URL & Impersonation Protection.
- S1 = Spam Filter + TTP (Office365 and Google G Suite).
- M2 = S1 + Continuity, needed for Exchange Servers.
- M2A = M2 + 99-year Archiving.
- End user daily spam reports with ability to Release, Permit, and Block email messages.

Scope of implementation, subject to client approval:

- Evaluate license requirements based on number of users.
- Implement Mimecast Spam filter and configure it as per USCC Standard.
- Work with client to configure SPF and DKIM records.
- Work with client to fine-tune spam filter after its implementation.

Out of Scope and Billable:

- Configure DMARC upon client request, requires DMARC monitoring subscription for 1-4 months.

Services not provided by USCC:

- Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.

Advanced Spam Filter Protection (ATP) - O365

Benefits:

- Helps guard your organization from malicious links and attachments.
- Daily end-user spam reports with ability to release flagged e-mails.

Scope of implementation, subject to client approval:

- Implement ATP and configure it as per USCC Standard.
- Enable daily end-user spam report.
- Work with client to configure SPF and DKIM records.
- Work with client to fine-tune spam filter after its implementation.

Out of scope, services not provided by USCC:

- Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.

Security Awareness Training - KnowBe4*

Benefits:

- End-user training modules to empower your team to be the first line of defense against threats to your network and client data.
- Video training, infographics, PDF's, and mock/training Phishing Campaigns to teach end-users how to spot risky e-mails containing unsafe link / attachments and CEO Fraud.
- Promotes a security conscious culture and fosters behavioral change to help secure your network environment.

Scope of implementation, subject to client approval:

- Work with client to identify client's internal KnowBe4 manager.
- Setup account and train client KnowBe4 manager on how to create phishing and training campaigns.
- Create re-occurring random phishing campaign.
- Client's internal KnowBe4 manager is responsible of the effectiveness of the Security Awareness Program, creating Phishing and Training Campaigns, and ensuring end-users meet training deadlines.
- USCC can help the client's internal KnowBe4 manager upon request.

Services not provided by USCC:

- The Client KnowBe4 manager is solely responsible for the effectiveness and enforcement of the Security Awareness Program.

USCC will not monitor Training or Phishing campaign training failures, this is the responsibility of the Client KnowBe4 manager.

Remove Local Admin Privileges

Benefits:

- Limits the damage that malware, exploits, and viruses can cause by ensuring attacks cannot run at the Administrator Level.
- Designates a limited/select number of Admin-UserName accounts per company that can make changes and install software on computers

Scope of implementation, subject to client approval:

- Work with client to coordinate removal of local admin privileges across all desktops and computers.

- Create an Admin-PC and/or Admin-Name account for approved and designated client Local Admins to perform necessary tasks.
- USCC recommends to setup a BIOS password to prevent the usage of bootable media that could reset local administrators.

Out of scope, services not provided by USCC:

- USCC does not monitor for changes made to the local Administrators group.

Secure VPN

Benefits:

- Establishes a secure VPN connection over insecure or public internet connections.

Scope of implementation, subject to client approval:

- The client will install the app, authenticate, and use as needed.

Out of scope, services not provided by USCC:

- USCC encourages the use of a secure VPN while a device is on an insecure network, however it is up to the end-user to manually enable the VPN.

Two Factor Authentication / MFA

Computer / Server 2FA - Duo Security

Benefits:

- Deters unauthorized access to Computers, Servers, Exchange Webmail and more.
- If credentials are compromised, 2FA inhibits the attacker and can provide red flags / warnings that unauthorized access attempts are taking place.
- USCC strongly recommends implementing 2FA on email, VPN remote access, computers, servers, etc.

Scope of implementation, subject to client approval:

- Work with client to identify applications to be protected by Duo.
- Deploy Duo to client approved applications, users, locations, etc.
- Provide support to end-users, including bypass codes and Duo re-activations.

Out of scope, services not provided by USCC:

- Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.
- USCC cannot accept, store, or keep user credentials.

Office 365 - Azure MFA

Benefits:

- Deters unauthorized access to Office 365 services by ensuring access is only possible with MFA. MFA can be set to re-authenticate every 30-60 days.
- USCC recommends enhanced end-user security service, Enterprise Mobility + Security E5.

Scope of implementation, subject to client approval:

- Coordinate with client to Enforce MFA to ALL Office 365 users except for the Sync_ account used for AzureAD Sync (MFA is NOT supported).
- Help end-users re-configure email on Outlook and Mobile devices.
- Enable Phone Sign-In for O365 and OAuth2 for Outlook 2016+.
- MFA requires Outlook 2016+.
- App passwords should not be used due to critical security vulnerabilities.

Out of scope, services not provided by USCC:

- Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.
- USCC cannot accept, store, or keep user credentials.

Email Protection (Office 365 / G-Suite / Exchange)

Enforce MFA for ALL Accounts

Benefits:

- Users tend to use the same email and password across multiple accounts, when any of those accounts have been compromised then the user's other accounts are vulnerable. The website https://haveibeenpwned.com/ allows you to check a corporate email address to see if that email has been subject to a data breach. If your users have the same email and password as a recent data breach, without Multi-Factor Authentication (MFA) attackers could use those credentials to access that email account. Accounts without MFA are getting compromised by attackers.
- MFA should be enforced for all email accounts in your email system to protect accounts from unauthorized access.
- Without protecting your email accounts with MFA/2FA, those accounts can be accessed by anyone on the internet with the right password.

Scope of implementation, subject to client approval:

- Work with client to identify best option for MFA to secure their email system.
- Upon project approval, work with end-users to enforce MFA.
- Office 365 Modern authentication requires Outlook 2016 and above.

Disable App Passwords / Enable OAuth2

Benefits:

- For Office 365, Microsoft is discontinuing the legacy App Passwords needed for MFA in favor of Modern Authentication due to vulnerabilities associated with App Passwords.
- Disabling App Passwords help protect from unauthorized access.

Scope of implementation, subject to client approval:

- Upon project approval, work with end-users to enforce MFA with Modern Authentication.
- Office 365 Modern authentication requires Outlook 2016 and above.

Disable IMAP/POP3

Benefits:

- Disabling IMAP/POP3 helps protect from unauthorized access.

Scope of implementation, subject to client approval:

- Work with client to identify existing usage of IMAP/POP3 if any, then disable IMAP/POP3 for all accounts.
- If a third-party vendor relies on IMAP/POP3, Microsoft has made API integration possible to allow vendors to migrate away from IMAP/POP3.

Mobile Device Policy (Encryption, PIN, Timer)

Benefits:

- Organizations can protect corporate email from unauthorized disclosure on lost/stolen Mobile devices by implementing an email Mobile Device Policy**.**
- The Mobile Device Policy includes settings to require a password, require encryption, and require an inactivity time-out on the mobile device with corporate email. A lost/stolen device without these settings will expose corporate email.
- iPhones, iPads, and modern Android devices where the user has already set a password, are already protected full disk encryption.

Scope of implementation, subject to client approval:

- Coordinate with client on Mobile Device Policy requirements and enforcement.

Enterprise Mobility + Security E5

Benefits:

- Helps protect your Office 365 account and data by providing Conditional Access, Risk-based conditional access and Data Loss Prevention (DLP) by automatically encrypting outgoing sensitive data.
- Helps identify risky sign-ins to identify compromised O365 accounts.

Scope of implementation, subject to client approval:

- Coordinate with client to identify licensing requirements.
- Implement client requested features from Enterprise Mobility + Security E5.

Data Protection

Password Manager - Keeper Security

Benefits:

- Helps users create a long and unique randomly generated password for each website.
- Passwords can be securely shared between users.
- Protected with a Master Password and 2FA.
- When a user leaves the organization, the passwords can be revoked and transferred to a designated person.
- Zero Knowledge & HIPAA compliant Business password management solution.

Scope of implementation, subject to client approval:

- Work with client to provision Keeper Account and configure it as per USCC Standard.
- Enforce 2FA for all keeper accounts.
- Train client on how to use Keeper Security.
- End-users will import their passwords into Keeper Security.
- Remove USCC Admin Access to Keeper Security.
- USCC cannot accept, store, or keep user credentials.

Services not provided by USCC:

- Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.
- USCC cannot import end-user passwords into Keeper due to exposure to passwords.

E-mail Encryption - Share File - Advanced

Benefits:

- Send and receive end-to-end encrypted e-mails via the Outlook plug-in or web portal. It can get read and file download receipts.
- Helps meet legal & regulatory requirements.
- Allows users the ability to request sensitive files/information via a link.
- Supports 2FA.

Scope of implementation, subject to client approval:

- Work with the client to setup account on a HIPAA compliant datastore.

- Configure account as per USCC Standard, enforce 2FA.
- Configure Single Sign-On (SSO) with Azure AD if the client uses Office 365 and has MFA.
- Make business owner a Super Admin and remove USCC account from ShareFile.

Services not provided by USCC:

- USCC cannot retain active management of ShareFile, as the Super Admin account gives the user full access to all data.
- Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.

E-mail Encryption - Mimecast

Benefits:

- Send and receive encrypted e-mails based on policies or keywords like [encrypt] for outbound e-mails.
- Apply policy-based encryption to Data Loss Prevention (DLP) policy to protect PII, HIPAA, and other Sensitive information.

Scope of implementation, subject to client approval:

- Work with the client to implement Email Encryption, only works for outbound emails and two-way Email Encryption for outbound emails.
- Upon client request, implement client requested DLP policy.

Services not provided by USCC:

- Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.

E-mail Encryption - O365

Benefits:

- Send and receive encrypted e-mails based on policies or keywords like [encrypt] for outbound e-mails.
- Apply policy-based encryption to the Data Loss Prevention (DLP) to protect PII, HIPAA, and other Sensitive information.

Scope of implementation, subject to client approval:

- Work with the client to implement Email Encryption, only works for outbound emails and two-way Email Encryption for outbound emails.
- Upon client request, implement client requested DLP policy.

Services not provided by USCC:

- Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.

Laptop Full Disk Encryption - SimplySecure / Beachhead

Benefits:

- Prevents unauthorized data disclosure by applying Full Disk Encryption
- Lost or stolen laptops can be remotely wiped once it establishes a connect to the internet and receives the command.
- The system can validate/prove the compromised device was fully encrypted.
  Requires Windows 8/10 Pro and an existing built-in TPM chip.

Scope of implementation, subject to client approval:

- Work with client to deploy BeachHead agent and start BitLocker encryption on client approved workstations.
- Provide end-users with hard drive recovery key as needed during Operating System or Firmware upgrades. This key is required to boot.
- Optionally, clients with TPM capable Windows 10 computers can deploy Domain managed BitLocker. Keys are not centrally managed which can cause issues without having the recovery key, and therefore no way to confirm if the computer had Full disk encryption at the time it is lost/stolen.

Services not provided by USCC:

- Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.

Media Sanitization (DoD 5220.22M or Physical Destruction)

Benefits:

- Prevents unauthorized data disclosure by securely wiping Hard Drives and media with DoD 5220.22M Standard.
- SSD/Flash Drives are Crypto Erased with BitLocker Full Disk Encryption.
- Physical Destruction prevents data recovery.

Scope of implementation, subject to client approval:

- USCC, upon the client's quote approval, will wipe or physically destroy hard drives for computers/servers being decommissioned.
- Physical Destruction by 3-holes drilled on the hard drive or by bending the hard drive platters with https://purelev.com/
- $50 per computer and $150 per server.

Out of scope

- Clients are responsible of notifying USCC when a multifunction copier is being replaced, or any other device that may contain storage.
- Clients are responsible of requesting that USCC wipe or physically destroy media prior to disposal.

Services not provided by USCC:

- USCC is not responsible for client's improperly disposing of equipment containing sensitive data.

Azure Information Protection (AIP) Data Encryption

Benefits:

- Helps protect sensitive data by applying Encryption-at-Rest.
- Files are only accessible by authorized users regardless of their location.
- Azure Rights Management (RMS) uses the following encryption types: AES 128/256-bit encryption for Documents, RSA 2048-bits for Key protection and SHA-256 for Certificate signing.

Scope of implementation, subject to client approval:

- Work with client to identify scope of data to be encrypted.
- Setup Labels and configure Encryption levels, train the client on how to use the AIP encryption Client.

Services not provided by USCC:

- Client end-users are solely responsible of data encryption and decryption.
- Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.

Network Infrastructure Billable Projects

Desktop BIOS & Firmware updates

Benefits:

- Helps protect computers from attacks on hardware and firmware related vulnerabilities, like Meltdown and Spectre.
- It is recommended that BIOS and firmware updates are applied at least once per year.

Scope of implementation, subject to client approval:

- Upon client request, USCC will work with the client to evaluate and estimate labor for this project.

- Approved BIOS and Firmware upgrades on network devices will take place after hours to avoid downtime, which will incur over-time rates.
  Please note that on any BIOS and Firmware upgrades, there is always a risk of hardware failure. Failed BIOS and Firmware upgrades occur, and USCC is unable to recover the hardware or firmware from such failures. While USCC takes precautions to minimize these issues, they randomly occur, and we cannot guarantee they will not happen. If they do happen, new hardware at the expense of the client will be necessary, unless the computer is under warranty.

ESXi Version Upgrades

Benefits:

- Helps protect virtualized servers by ensuring that the latest ESXi version patches security vulnerabilities
- Requires server downtime and the hardware must be compatible with the latest version of ESXi.

Scope of implementation, subject to client approval:

- Upon client request, USCC will work with the client to evaluate and estimate labor for this project.
- Approved ESXi, BIOS, and Firmware upgrades on network devices will take place after hours to avoid downtime, which will incur over-time costs.
- Please note that on any BIOS and Firmware upgrades, there is always a risk of hardware failure. Failed BIOS and Firmware upgrades occur, and USCC is unable to recover the hardware or firmware from such failures. While USCC takes precautions to minimize these issues, they randomly occur, and we cannot guarantee they will not happen. If they do happen, new hardware at the expense of the client will be necessary, unless the computer is under warranty.

End of Life Software migrations

Benefits:

- Helps protect your servers, computers, users, and data from attacks that target outdated and vulnerable software.
- Non-supported software puts your organization at risk of being targeted by attackers that look to gain and maintain access to your network.
- Vendors eventually stop supporting and releasing security patches for their outdated software.

Scope of implementation, subject to client approval:

- USCC strives to proactively work with clients to quote on hardware, software, license, and service renewals. USCC will process client requests in the order they are received.

- Scope of implementation varies by hardware, software, license, and service.

Services not provided by USCC:

- USCC does not monitor or manage line of business applications or their end of life, except for the hardware, software, licenses, and services USCC provides its clients.

Desktop Upgrades

Benefits:

- Helps address the vulnerabilities and risks of having older Desktop Operating Systems no longer receiving security updates.
- Vendors eventually stop supporting and releasing security patches for their software for older Desktop Operating Systems.

Scope of implementation, subject to client approval:

- USCC strives to proactively work with clients to quote on hardware, software, license, and service renewals. USCC will process client requests in the order they are received.
- Scope of implementation varies by hardware, software, license, and service.
- Upon client request, USCC will provide a quote to renew the warranty of desktops and/or laptops.

Services not provided by USCC:

- USCC does not monitor or manage line of business applications or their end of life, except for the hardware, software, licenses, and services USCC provides its clients.

Server Migrations

Benefits:

- Helps address the vulnerabilities and risks of having older hardware / servers that can cause downtime.
- Specific recommendations for server migrations are made after reviewing the network environment.

Scope of implementation, subject to client approval:

- USCC strives to proactively work with clients to quote on hardware, software, license, and service renewals. USCC will process client requests in the order they are received.
- Scope of implementation varies by hardware, software, license, and service.
- Upon client request, USCC will provide a quote to renew the warranty of Servers.

Services not provided by USCC:

- USCC does not monitor or manage line of business applications or their end of life, except for the hardware, software, licenses, and services USCC provides its clients.

Email Migrations

Benefits:

- Helps address the vulnerabilities and risks of having older hardware / servers / e-mail systems that can cause downtime.
- Specific recommendations for e-mail migrations are made after reviewing the network environment.

Scope of implementation, subject to client approval:

- USCC strives to proactively work with clients to quote on licenses, migration tool cost, labor, and service renewals. USCC will process client requests in the order they are received.
- USCC will work with the client to define the scope of the email migration. In most cases, USCC recommends the client to migrate from an on-premise exchange server to Office 365, depending on the client business needs. As per Microsoft's recommendation, and Industry best practice: USCC recommends organizations to use Azure AD Sync when a domain controller is present, and to enforce Multi Factor Authentication (Microsoft MFA) for all users.
- USCC recommends migrating only the data that is necessary but being aware that any mailboxes not migrated will not be available in the cloud or the new email server.

Out of scope, services not provided by USCC:

- Log Management, Threat Detection and correlation services. An MSSP or SOCaaS can help with that function.

Managed Service Plan Descriptions

Managed IT Services

24x7 Server & Desktop Monitoring & Alerts of Health, Hardware, and Performance

- See Proactive Care Plan (PCP)
    - PCP Workstations
    - PCP Servers
    - PCP Hypervisors
- See Proactive Care Plan Executive (PCPE)
    - PCPE Workstations
    - PCPE Servers
    - PCPE Hypervisors

Microsoft Critical & Security Updates

Benefits:

- Automatic non-blacklisted Microsoft Critical & Security updates deployment help protect the organization from vulnerabilities that could be exploited and cause harm to the organization.
- Both the PCPE and PCP Service Plans include Automatic deployment of non-blacklisted Microsoft Critical and Security updates.
- Clients that approve the Add-on Ninite Pro also receive Automatic Third-party patching for applications listed on https://ninite.com/applist/pro.html

Scope of implementation, subject to client approval:

- Once Microsoft critical and security updates are released, they are tested in a Test group, then a Pilot group, then deployed to the rest of the organization. This is done strategically to minimize the impact of bad updates and to allow the quick Blacklisting and removal of such updates.
- The organization servers and computers get non-blacklisted updates after the Test and Pilot groups in the organization have received the patches, this normally takes 14-21 days.
- For clients that approve Third-party patching, Ninite Pro is deployed, and updates are tested on a small group. Computers are set in a policy to update all applications (only adding exceptions when necessary and requested by the client).
- USCC will upgrade versions of older third-party software supported by Ninite Pro upon client request. Patches are automatically applied, but software version upgrades require client coordination and approval.
- Patch testing: Microsoft critical and security updates are tested on a small group for each client in a Test group for 1 week, then a larger Pilot group for 7 days, then finally deployed to all the remaining (Production) group 14-21 days after their release. USCC may blacklist Microsoft critical and/or security updates/patches known to downtime and other issues. This is the standard deployment and best practices method using the ConnectWise Automate Patch Manager.
- Patches may be blacklisted if they impact the NIC (network) drivers of a computer/server (normally Windows 7/Server 2008 family).
- Microsoft stopped releasing security and critical updates for Windows 7, Server 2008, Server 2008 R2, and SBS 2008/2011 on January 14, 2020: any devices with these operating systems are End-of-life (EOL) and need to be upgraded to new supported hardware/software.
- Patch deployments follow the ConnectWise Automate Patch Manager best practices. Deployments are done in small increments, but they are not tested in a test environment prior to deployment. If patches cause issues, they can be blacklisted and uninstalled.

Out of scope and billable:

- USCC does not automatically upgrade third-party software supported by Ninite Pro to the latest version, unless requested and approved by a client.

Services not provided by USCC:

- USCC does not perform Vulnerability or Penetration testing, which may be required by some legal or regulatory compliance requirements. These functions are normally performed by an MSSP, as previously described.

Antivirus Protection

Benefits:

- Webroot Antivirus is a centrally managed and Cloud-based Antivirus.
- It has a low performance impact on Servers and Workstations.
- Windows devices support Automated Full scans when a Threat is detected.

Scope of implementation, subject to client approval:

- It is critical that ALL computers and servers within a network are managed under a Managed Service Plan (PCPE or PCP) so that the Webroot integration and Automation can protect them.
- Webroot Antivirus will be licensed and deployed to managed computers and Servers that have the RMM agent installed.
- USCC recommends a layered approach in which a Firewall with Security Services protects the network, Webroot Antivirus protects the device, OpenDNS helps protect internet traffic by blocking detected malicious traffic, MFA protects publicly available resources, etc.

Out of scope, services not provided by USCC:

- Active Log Management, Threat Detection, and correlation services. An MSSP or SOCaaS can help with that function.

Sourcing & Procurement

Benefits:

- Recommendations based on client's needs.
- Competitive pricing.
- Standardize client's hardware.

Scope:

- Research & vetting out ideal solution (hardware, software, service) based on client's needs.
- Procure best pricing from suppliers based on our purchase volume.
- Minimize turnaround time by streamlining logistics.

Out of scope:

- Some Printers, Apple products and software must be purchased directly by the client.

IT Helpdesk & Onsite Support during normal business hours (Monday-Friday 8:00am to 5:00pm EST)

Benefits:

- Reliable technical expertise.
- Allows you to focus on your core business.
- Remote or Onsite technical support.

Scope:

- Helpdesk
  - Diagnose technical issues.
  - Computer upgrades, replacements, migrations, and troubleshooting.
  - Email setup on Outlook/Mobile devices, connectivity issues, and troubleshooting.
  - Troubleshoot connectivity issues: printers, VPN, network, WiFi, Email, QuickBooks, etc.
  - Virus removal and clean up.
  - Spam filtering issues.
  - Support of USCC provided products and services.
  - User Access Management: creation/termination.
- System Administration
  - Server maintenance
  - Firewall change requests
  - Spam filter management
  - Project deployments of approved products and services.

Services not provided by USCC:

- Software functionality training: USCC will help re-install Microsoft Office, QuickBooks, and other approved software if proper licensing is available. However, the specific usage of software and their functionality is outside of the services USCC provides. For example, USCC can get QuickBooks installed and connected to the Server/Network Share, and the client would need to know how to use the software. USCC does not provide Software functionality training.

IT Helpdesk & Onsite Support during non-business hours

Benefits:

- We have staff on an on-call rotation to help with after-hours billable support for emergencies.

Scope:

- After hours billable Over-time Helpdesk support: lost/stolen devices, ransomware infections, C-Level support.

- After hours billable Over-time System administration support: server down, site down, server hardware failures, email flow issues, etc.
- Pre-approved and pre-coordinated project deployments of approved products and services.

Out of scope:

- Items from "IT Helpdesk & Onsite Support during normal business hours (Monday-Friday 8:00am to 5:00pm EST)", unless when prior authorization has been provided by the primary contact or business owner and coordinated.

IT Project Management

Strategic Consulting

Benefits:

- We employee subject matter experts in various fields. They are trained, knowledgeable, and can help provide guidance on planning, designing, and implementing a security oriented, scalable and efficient IT infrastructure.

Scope:

- Assess current & future state of client's IT and align solutions based on present and future client initiatives and business needs.
- Strategic consulting is based on the products and services we provide and have expertise on.

Out of scope:

- We welcome the opportunity to help your organization with its IT needs, items not listed in this document may be outside of our area of expertise.

Network Design & Implementation

Benefits:

- We employee subject matter experts in various fields. They are trained, knowledgeable, and can help provide guidance on planning, design, and implementation of IT infrastructure that promotes network security, scalability & efficiency.

Scope:

- Assess current & future state of client's IT and align solutions based on present and future client initiatives and business needs.
- Plan based approach with client for growth-oriented initiatives.
- Work with client's software vendors to ensure compatibility in hardware and forward progression.
- Network diagrams done upon client request as a billable item.

Out of scope:

- See "Shared Cyber Security Responsibility".
- See all "Out of Scope" and "Services not provided by USCC".

Basic Security Recommendations (BSRs)

Benefits:

- Clients can request a Basic Security Recommendations (BSR) list for their network.
- Otherwise, as USCC provides its products and services, it will notify its clients of deficiencies that it identifies that require attention. USCC will provide the client with a simple list of recommendations and a quote.

Scope of implementation, subject to client approval:

- BSRs are performed upon client request, when quoting a server/email migration, or if items are identified in the process of USCC providing its products and services.
- USCC will present a simple report and a quote with recommendations, it is up to the client to perform risk management and risk mitigation.
- See "Basic Security Recommendations (BSRs) – " sections for details.

Services not provided by USCC:

- Active Log Management, Threat Detection, and correlation services. An MSSP or SOCaaS can help with that function.
- USCC does not perform Risk Assessments/Analysis for its clients as it is a conflict of interest and it is a function that belongs internally to the client organization. A Basic Security Recommendation (BSR) report is not a Risk Assessment, a Security Audit or a Security Review.
- Client organizations are responsible of: identifying and managing what legal, regulatory, contractual and other requirements apply to their organization; performing risks assessments/analysis/management; managing risk to their organization based on their risk appetite and tolerance; implementing an internal Information Security Management Program, Risk Management Program, Third-party Risk Management Program, etc., in order to help protect their organization.

Server and Email Migrations

- See BSR "*ESXi Version Upgrades*"
- See BSR "*Server Migration(s)"*
- See BSR "*End of Life Software migrations*"
- See BSR "Desktop Upgrades"

Infrastructure Upgrades & Migrations

- See BSR "*ESXi Version Upgrades*"
- See BSR "*Server Migration(s)"*
- See BSR "*End of Life Software migrations*"
- See BSR "Desktop Upgrades"

Secure Enterprise Wireless Solutions

- See BSR "Enterprise Wi-Fi & Wi-Fi Isolation"

Office Relocation & Planning

Benefits:

- Assist in smooth transition to a new location ensuring IT Infrastructure is in place for go-live date.

Scope:

- Design and implement client approved IT infrastructure recommendations.
- Setup computers and/or servers at new location.
- Collaborate with project manager and moving company.
- Move the server to the new location.

Services not provided by USCC:

- Move workstations, printers, peripherals, furniture, etc.

Data & Voice Network Cabling

Benefits:

- Cost-effective and reliable cable runs that ensure optimal network connectivity.

Scope:

- Each cable is tested, labeled, certified and color coded.

Out of scope:

- High voltage work.

Cyber Security Offerings

- USCC is an MSP, not an MSSP or a SOC.

NextGen Firewalls

- See BSR "SonicWALL Security Services"

Endpoint Protection

- See BSR "*Antivirus Protection*"

- See BSR "*OpenDNS*"
- See BSR "*Ninite Pro*"

Multi-factor Authentication

- See BSR "*Computer / Server 2FA - Duo Security*"
- See BSR "Office 365 - Azure MFA"

Advanced Spam Filter Protection

- See BSR "*Advanced Spam Filter Protection – Mimecast S1/M2/M2A*"
- See BSR "Advanced Spam Filter Protection (ATP) - O365"

HIPAA Compliant Email Encryption

- See BSR "*E-mail Encryption - Share File - Advanced*"

Strong Password Policy Implementation

- See BSR "*Strong Password Policy Implementation*"

Full Disk Encryption

- See BSR "*Laptop Full Disk Encryption - SimplySecure / Beachhead*"

Security Awareness Training

- See BSR "*Security Awareness Training - KnowBe4*"

Media Sanitization (DoD 5220.22M or Physical Destruction)

- See BSR "Media Sanitization (DoD 5220.22M or Physical Destruction)"

Log Management for Compliance

- See BSR "*Windows/PCs - Manage Engine AD Audit*"
- See BSR "SonicWALL – Analyzer"

Mobile Device Management (MDM)

Benefits:

- Managed full disk encryption with FileVault.
- Central management of Macs and Mobile devices and ability to remotely wipe them when they are lost/stolen.

Scope of implementation, subject to client approval:

- USCC will work with client to identify devices that need to be protected by MaaS 360.

- USCC will install the MaaS 360 on the approved agents, and upon client request remotely wipe lost/stolen Macs.
- Client is responsible of contacting USCC to report lost/stolen devices and request them to be wiped.

Services not provided by USCC:

- Active Log Management, Threat Detection, and correlation services. An MSSP or SOCaaS can help with that function.

Business Continuity & Disaster Recovery

Server Backup

- See BSR "*Datto Backup (Local & Offsite Backups)*"
- See BSR "Datto Backup + Passphrase Encryption"

Office 365 Backup

- See BSR "Office 365 Backup"

Google Suite Backup

- See BSR "Google Suite Backup"

Laptop Backup

- See BSR "Laptop Backup – Carbonite Safe Backup Pro"

Cloud Computing

Public & Hybrid Cloud Solutions

Benefits:

- Design and implement a solution that leverages both platforms to maximize uptime and streamline the user's workflow.

Scope of implementation, subject to client approval:

- Understand need, determine resources needed such as memory and hard drive and provide a quote.

Out of scope:

- See "Shared Cyber Security Responsibility".

- See all “Out of Scope” and “Services not provided by USCC”.
- Any “MSSP” Services.

Cloud-based Email & Software (SaaS) Solutions

- See BSR “*Email Migrations*”
- See BSR “*Office 365 Backup*”
- See BSR “*E-mail Encryption - O365*”
- See BSR “*Office 365 - Azure MFA*”
- See BSR “E-mail Encryption - Share File - Advanced”

Remote Access: Work from Anywhere

Benefits:

- Remote access to server or workstation(s).

Scope of implementation, subject to client approval:

- Upon client request, provide 2FA secure Remote Access to workstations or servers.
- Upon client request, work with clients to identify best Remote Connectivity solutions.

VoIP

Benefits:

- Scalable and simple to use
- Easy to configure.
- Great for remote workforce.

Scope of implementation, subject to client approval:

- Work with VoIP carrier to transfer phone lines.
- Configure network for QoS.
- Install phones.

****SERVICES OUTLINED ABOVE ARE THE SERVICES WE OFFER****