IT Service Catalog

Headquarters:

1 Northfield Plaza,

Suite 300,

Northfield, IL 60093

www.ciolanding.com

Effective July 31, 2026. These Service Descriptions supersede and replace all prior versions.

Contents

Contents 2
1. Definition of Terms 4
2. Technical Requirements 6
3. Service Scope 6
4. Support Desk 6
4.1. Incident / Service Request Workflow 7
4.2. Support Desk Service Levels 7
4.3. Fair Usage 8
4.4. Data Recovery Service Levels 8
4.5. New Hires and Termination requests 8
4.6. Network Availability Service Levels 8
4.7. Vendor Service Levels 9
4.8. Priority Matrix 9
4.9. Customer Satisfaction 9
5. Access Management 10
Service Descriptions 11
6. Support Desk 11
7. Managed Workstation 11
8. Workstation Disk Encryption 11
9. Managed Server 12
10. Managed Inbox 12
11. Managed NAS 13
12. Managed Mobile Device (iOS) 13
13. Managed Network Printer 13
14. Cloud Management 13
15. Anti-Phishing Tool 14
16. Anti-Spam 14
17. Cyber Security Awareness Training 14
18. NOC 15
19. Remote Managed Site 15
20. Managed Advanced Network Site 15

© Scott & Scott, LLP

21. DMARC Policy Monitoring 15
22. Client Success Manager (CSM) 16
23. Technology Alignment Manager (TAM) 16
24. Current Plans 16
• Advanced Plan 16
• Add-Ons 17
25. Backup and Recovery 18
Mailbox Backup 18
Cloud Storage Backup 18
Workstations Backup Solution 19
Collaboration Platform Backup 19
Server Backup Solution 19
25.1 Server Backup Frequency 19
25.2 Smart Data Transport 19
25.3 Remote Storage provided by CIO Landing 19
25.4 Retention Policy 19
25.5 Ownership of the Data 20
25.6 Restore and Disaster Recovery 20
26. Hardware support 20
27. Software support 20
28. Internet Services 20
29. Software License Management 21
30. Enterprise Governance: Policies and Procedures 21
31. Project Services 21
32. Technology Business Review 22
33.Third Party IT Supplier Management 22
Appendix 1 – In Scope Service Summary 23
Appendix 2 - Out of Scope Services Summary 25
Appendix 3 - List of Approved Connected Devices 27

© Scott & Scott, LLP

1. Definition of Terms

Agreement	Terms and Conditions accepted by both parties.
Access Management	The process responsible for allowing only authorized users to access certain assets and IT services while preventing unauthorized users from accessing them.
Basic support	CIO Landing will provide a level of support which comprises of basic troubleshooting where the peripheral device is compatible with the computer and operating system. We cannot support equipment purchased independently which may be incompatible with the computer or operating system, or when the software required for its use, conflicts with other critical software on the system.
BDR	Backup Disaster Recovery (can relate to the server that stores your backups). The service provided enables backups to take place and the restoration of data in a disaster situation. Also known as IT Service Continuity.
CIO	Any references to CIO refer to CIO Landing Services, MSP.
Configuration Item (CI)	A CI is a component of an IT infrastructure for example, a single module such as a monitor, workstation, docking station or more complex items, such as a complete system.
Cybersecurity	The functions that control and protect access to system and network resources. Also known as IT Security Management.
Emergency	Requests considered an emergency are where one or more users are unable to work and the request needs to be dealt with on a higher priority.
HIPAA	Health Insurance Portability and Accountability Act is the US legislation that provides data privacy and security provisions for safeguarding medical information.
Incident	An unplanned interruption to an IT service or reduction in the quality of an IT service or failure of a Configuration Item (CI).
ITIL	IT Infrastructure Library is a set of best practice guidelines within the IT Managed Services Industry.
LOB	Line of Business. This refers to client-specific business applications.
Location/ Site	A supported location/ site refers to a site belonging to the Client which at a minimum contains a router and where a company conducts all or part of its business.
Major Incident	An event which has significant impact or urgency for the business or organization, and which demands a response beyond the routine Incident Management process.

© Scott & Scott, LLP

Master Customer Agreement	The contract reached between the MSP and the Client in which both parties agree to the terms that will govern future agreements.
MDR	Managed Detection and Response is a cybersecurity service that provides organizations with advanced threat detection, incident response, and continuous monitoring capabilities.
MSP	Managed Service Provider. This term refers to CIO Landing Services.
NOC	Network Operations Center. The team that is responsible for management and control of the client network.
On-Boarding process	This refers to the process of transitioning the client's current IT infrastructure support to CIO Landing. It involves three main steps: an initial assessment of the existing infrastructure, the start of service, and the final implementation of the service after the migration of servers.
Priority	A category used to identify the relative importance of an incident, problem, or change. Priority is based on impact and urgency and is used to identify required times for actions to be taken.
PST	Professional Services Team is made up of experienced network architects, infrastructure specialists and desktop engineers managing your IT infrastructure.
Recommended Vendors	A third-party supplier that has been suggested to the Client by CIO Landing, and with whom CIO Landing have an official partnership.
Security Services	Management of server, data, and network security through early identification of internal and external security threats via alert reporting. **Also see Cybersecurity.**
Server Capacity	The storage space of IT servers required to deliver the agreed service level targets in a cost effective and timely manner.
Service Request	A user request for information or advice, or for a standard change or for access to an IT service e.g., password reset.
SLA	A Service Level Agreement is an agreement between the MSP and the Client defining detailed service level targets and mutual responsibilities.
SOP	Standard Operating Procedure. Documented process or set of procedures that outlines how CIO Landing performs tasks stored in the documentation platform.
SOW	The Statement of Work is the document which captures and defines the deliverables, detailed requirements, pricing and governance conditions of the IT Service Proposal between CIO Landing Services and the Client.
SSO	Single Sign On. This refers to authentication to several software systems with a single id and password.

© Scott & Scott, LLP

2. Technical Requirements

CIO Landing recommends that the Client's existing environment meet the following requirements, to avoid additional maintenance costs, and are subject to change in line with technology advances:

- All Servers with Microsoft Windows Operating Systems must be running currently supported Microsoft Windows Server editions as stated on the Microsoft website.
- All Workstations with Microsoft Windows Operating Systems must be running Pro or superior edition of the currently supported Microsoft Windows editions as stated on the Microsoft website.
- All computers running Apple Operative Systems and iPad's, should be running any of the latest three supported versions published on the Apple website.
- All NAS devices must be Synology with cloud sync and virtualization capabilities.
- All Server and Desktop Software must be Genuine, Licensed and Supplier-Supported.
- All Server, Desktop, Laptop, Switches, Access Points, Routers, Firewalls and Printer hardware must be business class grade to receive our support. Otherwise, CIO Landing is not responsible for the performance or time to repair or remediate any malfunctions.
- Hardware warranty on network and server equipment must be in force. Without a valid warranty, response time on equipment will no longer be guaranteed.
- The environment must have a currently licensed, Supplier-Supported Hardware Firewall between the Internal Network and the Internet.
- Any Wireless data traffic in the environment should be secured with a minimum of 128bit data encryption.
- Wires must be clearly labelled and tested to CAT6 standard or higher.

CIO Landing is open to accepting new clients even if their infrastructure does not currently meet the standards, requirements, and best practices outlined in these guidelines. In such cases, CIO Landing may assess the client's infrastructure and offer recommendations to bring it up to the required standards.

3. Service Scope

The CIO Landing's IT Services are described in more detail in the following pages and will give you an introduction to our specialist teams who work seamlessly together during the Standard CIO Landing Office Hours, unless otherwise specified.

4. Support Desk

CIO Landing will respond to the Client's Incident or Service Request under the provisions detailed in the SOW, and in accordance with the agreed Service Levels.

Access to the Support Desk by authorized personnel is made by one of the following methods:

- Calling +1 (847) 868-9208
- Emailing support@ciolanding.com

© Scott & Scott, LLP

- Creating a ticket on our CIO Landing ticketing system direct from the CIO Client Portal
- Creating a ticket on our CIO Landing ticketing system direct from the CIO icon in the System Tray

All requests for support must first be logged in with the Support Desk before they are passed to the next level of support if deemed necessary by the Support team.

4.1. Incident / Service Request Workflow

The Support Desk team will promptly open and address all Incidents or Service Requests. If you send an email, it will be automatically assigned a priority, and you will receive an email with a reference number for your request. Please note that email requests may take slightly longer to process compared to direct phone calls. If you need immediate assistance, it is recommended to call us initially.

The Support Desk team will provide remote support whenever possible. If the Support Desk team is unable to resolve the issue, the Incident or Service Request will be escalated.

Each Incident or Service Request will be assigned a priority based on impact and urgency and a reference number for easy tracking (e.g., #123456).

Once the incident or request has been investigated and diagnosed, you will be provided with a resolution and the Incident record will be closed.

After an Incident or Service Request is closed, you will receive an email summary for your reference in case you have any further inquiries. Additionally, you will receive a Customer Satisfaction Survey to gather your feedback.

All contact with the Support Desk team is followed up with an email confirming your unique reference number and a short summary of the incident or request. All calls may be recorded for training and quality purposes.

4.2. Support Desk Service Levels

CIO Landing will provide the following levels of service for all incidents logged at the Support Desk and are in accordance with the priorities described in Section 4.1 based on impact and urgency.

During Standard CIO Landing Office Hours, our goal is that 85% of incidents will meet the following service levels:

PRIORITY	RESPONSE TIME	STATUS UPDATE	RESOLUTION TIME
1	1 hr.	2 hrs.	4 hrs.
2	1 hr.	2 hrs.	8 hrs.
3	2 hrs.	4 hrs.	16 hrs.
4	8 hrs.	16 hrs.	32 hrs.

**All times listed in business hours.*

© Scott & Scott, LLP

After Standard CIO Landing Office Hours:

PRIORITY	RESPONSE TIME	STATUS UPDATE	RESOLUTION TIME
1	2 hr.	ASAP/ Best effort	ASAP/ Best effort
2	4 hr.	ASAP/ Best effort	ASAP/ Best effort
3	4 hr.	ASAP/ Best effort	ASAP/ Best effort
4	8 hr.	ASAP/ Best effort	ASAP/ Best effort

**All times listed in business hours.*

4.3. Fair Usage

If Client usage of services exceeds the expected number of tickets specified below. Client may be subject to increased Service Fees or charges, suspension of services, or termination.

Fair Usage Cap

- Service Desk: 0.5 tickets per user per month.
- Professional Services: 0.25 tickets per user per month.
- Centralized Services: 0.20 tickets per user per month.

4.4. Data Recovery Service Levels

For individual file restores, we require the user to follow the Incident Management procedures, whereby the above Service Desk SLA's will apply.

4.5. New Hires and Termination requests

Account creation for new employees will take a minimum of 5 (five) business days to complete. This timeframe includes the creation of all necessary accounts and the setup of the employee's workstation. If hardware needs to be obtained based on vendor availability, additional time will be required.

**There may be additional fees for requests related to new user setups. Additionally, if requests for new hires are received within a timeframe shorter than the minimum specified above, an extra charge will apply.*

For account deletions, due to the nature of the request, we will immediately disable all accounts on receipt of the request from a manager and will proceed to delete all accounts within 5 business days unless specified otherwise by the Client.

4.6. Network Availability Service Levels

The service level agreement regarding network availability depends on several factors, including the location of the Client site, the internet provider in that area, and the service contract terms and conditions that the Client agreed to. CIO Landing may manage the Internet Service Provider on your behalf but shall not be held responsible for any network outages directly related to the third-party supplier or for any related SLAs.

© Scott & Scott, LLP

As an example, at the time of writing, the Comcast Availability Service Level commitment for standard wholesale dedicated internet stated that availability for each company port would stay below 99.9% in any given Service billing month. Comcast will issue a Service Credit based on the cumulative amount of Service Outage time in a calendar month if availability is less than the commitment. Further details can be found in your ISP agreement.

There are also Service Levels on network latency, where on average, in any given service calendar month, roundtrip latency will not exceed 55ms. For up-to-date Service Levels, see the individual ISP agreement.

4.7. Vendor Service Levels

Where CIO Landing needs to contact a third-party vendor, please be aware that each vendor offers their own service levels, which may differ to those offered by CIO Landing and will supersede the defined CIO Landing service levels when support is required.

4.8. Priority Matrix

The Support Desk team will log Incidents and Service Requests in the ticketing system based on the impact and urgency of the issue. Factors such as the number of users affected, and the criticality of the affected business application or services will be considered. The priority matrix will guide the assignment of appropriate priorities to these incidents and requests.

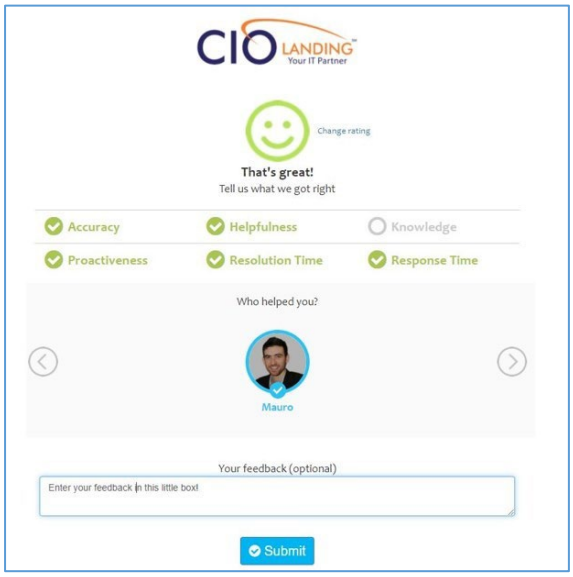
PRIORITY = IMPACT + URGENCY	**HIGH URGENCY** Whole company is affected	**MEDIUM URGENCY** Departments or large group of users are affected	**LOW URGENCY** One user or a small group of users is affected
HIGH IMPACT Major business processes are stopped	**Priority 1 – Critical**	**Priority 1 - Critical**	**Priority 2 - High**
MEDIUM IMPACT Business is degraded, but there is a workaround	**Priority 2 - High**	**Priority 2 - High**	**Priority 3 - Medium**
LOW IMPACT More of an irritation than a stoppage	**Priority 3 - Medium**	**Priority 3 - Medium**	**Priority 4 – Low**

4.9. Customer Satisfaction

We aim to ensure you receive the best customer service we can provide, and as such, we are dedicated to continuous service improvement.

© Scott & Scott, LLP

For every Incident or Service Request you place with us, you will receive the option to provide feedback on the service you received from our Support teams.





Any feedback we receive below the AWESOME or GOOD rating, is seen as an opportunity for improvement and will be followed up by a member of our Support team. We review every survey to improve our service quality.

5. Access Management

CIO Landing will handle user administration tasks, including creating accounts for new employees, modifying existing accounts, and deleting accounts for employees who leave. These tasks will be performed in accordance with the Standard Operating Procedures established with the Client.

For new employees, all requests must be sent to the Support Desk team by the manager of the new employee/HR department, at least 7 business days in advance of the start date.

CIO Landing will be responsible for creating computer login accounts, LOB application accounts (where admin access has been provided by the Client), email accounts, Microsoft 365 accounts, and the addition of the employee to the agreed security solution.

CIO Landing will also set up a new workstation with the required Business Applications and configuration in line with your business needs*.

**Subject to additional charges*

© Scott & Scott, LLP

Service Descriptions

6. Support Desk

We will provide end-user support through a dedicated Support Desk, which will include remote troubleshooting of hardware, software, and network issues, as well as handling password resets and access requests. Our team will ensure delivery of timely, efficient, and effective support to all users, minimizing downtime and maximizing productivity.

We will manage user accounts and access rights. Additionally, we will assist with software installations and updates, ensuring that users have the latest software versions.

To find a detailed list of services and tools included in each plan, please refer to the 'Current Plans' section.

Out of Scope: User training on specialized software or applications, mass permissions changes, or largescale user migrations. Any requirements such as these will incur additional charges.

7. Managed Workstation

We provide support for physical and virtual workstations. This includes configuring and maintaining operating systems and software applications, managing software updates and patches, setting up user accounts and access rights, monitoring performance and addressing issues, and providing technical support to the end-users' workstation.

We will take measures to safeguard workstations against viruses, malware, and other security threats by installing and maintaining our security software products. Furthermore, we will ensure adherence to company policies and relevant laws and regulations concerning workstation usage and data security.

We will regularly monitor workstation capacity levels to ensure optimal performance. It is important to inform CIO Landing in advance about peak periods of business activity. Additionally, essential workstation administration tasks, such as setting up and configuring printers, scanners, and other peripherals, will be included in our services.

To find a detailed list of tools included in each plan, please refer to the 'Current Plans' section.

Out of Scope: Workstation rebuilds, workstation backup, large-scale migrations, software mass deployments/updates, software migration, or projects like virtualization. Any requirements such as these will incur additional charges.

8. Workstation Disk Encryption

We will install and configure Workstation Disk Encryption software, seamlessly integrating it with your workstations. Computers must meet specific requirements, including hardware (TPM version 1.2 or higher) and software (appropriate operating system licenses).

© Scott & Scott, LLP

9. Privileged Access Management (PAM)

We will deploy and manage a Privileged Access Management (PAM) solution to provide secure, controlled administrative access for authorized users while reducing the need for permanent local administrator privileges.

We will deploy and manage a Privileged Access Management (PAM) solution to provide secure, controlled administrative access for authorized users while reducing the need for permanent local administrator privileges. This service helps improve endpoint security by allowing administrative rights only when required and under an approved workflow.

We will configure and maintain standard privilege elevation policies, manage application approval requests, and monitor privileged activity to ensure compliance with security best practices. We will also maintain approved application rules and review elevation requests when required.

Out of Scope: This service is focused on privilege elevation and does not include password vaulting, full identity governance, third-party PAM platform administration, or custom approval workflows outside our standard offering. Some of these items may be available under other managed services, separate projects, or custom agreements.

10. Managed Server

We will provide support for both On-Premises and Off-Site server infrastructure, including file servers, print servers, and Exchange servers. Additionally, we will monitor server capacity levels to ensure optimal performance. It is important to communicate specific peak periods of business activity to CIO Landing in advance.

Essential server administration functions, such as monitoring backups, managing group policies, DNS, and DHCP servers, performing routine server optimization and housekeeping, are also included.

To find a detailed list of tools included in each plan, please refer to the 'Current Plans' section.

We will manage all server licenses and maintenance subscriptions on your behalf. CIO Landing will provide a Quote to the Customer and only proceed once approval has been received.

Out of Scope: Server rebuilds, removals, cloud migrations, software migrations, or projects such as server virtualization. Any requirements such as these will incur additional charges.

11. Managed Inbox

We will provide support for mailboxes (all those that do not belong to a specific human user, e.g., info@yourcompany.com, or the current user is not a Managed User), ensuring that all email accounts are set up correctly and functioning properly. Mailboxes will be protected with our anti-spam solution and other security tools. To find a detailed list of tools included in each plan, please refer to the 'Current Plans' section.

Out of Scope: Support for third-party email applications or plugins, or email integrations with other software applications. Any requirements such as these will incur additional charges.

© Scott & Scott, LLP

12. Managed NAS

We will provide support for network-attached storage (NAS) devices, ensuring that all data stored on the NAS is secure, backed up, and accessible to authorized users.

We will monitor NAS storage capacity and usage, ensuring that adequate storage space is available for current and future data storage needs. We will assist users with NAS setup and configuration, ensuring that the NAS is set up to meet the organization's specific needs. This may include configuring user permissions and access controls, creating, and managing shared folders, and configuring automatic file synchronization.

Out of Scope: Support for third-party applications or plugins installed on the NAS, or integrations with other software applications. Any requirements such as these will incur additional charges.

13. Managed Mobile Device (iOS)

We will provide support for managed iPhones and iPads, ensuring they are up to date, secure, and properly configured for business use.

We will perform regular iOS and iPadOS updates to maintain device security and performance. We will monitor device status, ensuring compliance with company policies and identifying any potential security risks. We will assist with remote device wipes when necessary to protect sensitive data. Additionally, we will handle the installation and management of approved business applications.

Out of Scope: Support for third-party applications beyond installation, troubleshooting personal apps, hardware repairs, or unauthorized modifications (e.g., jailbreaking). Any requirements beyond the defined scope may incur additional costs.

14. Managed Network Printer

We will deploy and configure a Cloud Printing solution, seamlessly integrating it with your existing environment. This service eliminates the need for traditional print servers, enabling users to print securely and efficiently.

15. Cloud Management

We will allocate up to 4 (four) hours per month for essential management and administration of Azure services. This includes monitoring, maintaining, and optimizing various cloud resources like SharePoint, virtual machines, storage, and networking. Our aim is to ensure these resources are running efficiently and effectively. In case of any issues or incidents, we will promptly respond and take necessary actions. Additionally, 1TB of a collaboration platform such as SharePoint cloud backup storage is included.

Out of scope: Specific industry or regulatory compliance requirements, such as HIPAA, SOC2 or GDPR. Advanced analytics or custom developments. Any requirements such as these will incur additional charges.

© Scott & Scott, LLP

16. Anti-Phishing Tool

We will provide an Anti-Phishing tool, which will be designed to protect against phishing attacks and other email-based threats.

The Anti-Phishing tool will be installed and configured by CIO Landing and will be integrated with the Client's email system to provide real-time scanning and protection against suspicious and malicious emails. The tool will be regularly updated to ensure that it is able to detect and prevent new threats as they emerge.

We will monitor the Anti-Phishing tool for any potential issues, proactively addressing any problems before they cause downtime or loss of productivity. In the event of a tool failure or issue, CIO Landing will promptly replace or repair the tool.

Out of Scope: Support for any other email protection tools or customizations of any sort is not included. Requirements such as these will incur additional charges or may be denied accordingly.

17. Anti-Spam

We will provide an Anti-Spam email filtering solution which will be designed to protect against spam emails, viruses, and other email-based threats.

The Anti-Spam solution will be installed and configured by CIO Landing and will be integrated with the Client's email system to provide real-time scanning and protection against suspicious and malicious emails (inbound and outbound). The solution will be regularly updated to ensure that it is able to detect and prevent new threats as they emerge.

We will monitor the Anti-Spam for any potential issues, proactively addressing any problems before they cause downtime or loss of productivity. In the event of a solution failure or issue, we will promptly replace or repair the solution.

Out of Scope: Support for any other email protection tools or customizations of any sort is not included. Requirements such as these will incur additional charges or may be denied accordingly.

18. Cyber Security Awareness Training

We will provide online cyber security awareness training to the Client, which will be designed to educate employees on safe and secure computing practices, including but not limited to best practices for password management, phishing prevention, and safe browsing habits. The online cyber security awareness training program will be tailored to the specific needs of the Client. The training will be designed to be engaging and interactive and will include practical exercises and real-world examples to help employees understand the importance of online security. We will provide regular updates and training modules to keep employees up to date on the latest online security threats and trends.

© Scott & Scott, LLP

We will monitor the effectiveness of the online cyber security awareness training program and will adjust as necessary.

Out of Scope: Support for any other security awareness training or education programs. Customizations of any sort are not included.

19. NOC

We have 24 x 7 x 365 network auditing tools that allow us to monitor the critical devices within your IT infrastructure, to identify potential issues or trends. We will track event logs related to:

- Network and Server uptime
- Anti-Virus
- Server hardware integrity and reliability
- Storage space and availability
- Firewall, routers & switches

CIO Landing will document critical system alerts, scans and event resolutions following alerts received by our remote monitoring and management tool. If an issue is detected during monitoring, we will investigate and attempt to rectify the situation promptly using remote methods. Critical alerts are automatically logged into our CIO Landing ticketing system and constantly reviewed.

20. Remote Managed Site

Includes remote monitoring and maintenance of firewalls, switches, access points, and Internet Service Provider (ISP) monitoring.

Out of scope: Upon request onsite visits.

21. Managed Advanced Network Site

Comprehensive ongoing management of complex network environments built on enterprise-grade UTM firewalls. Designed for environments that require enhanced security, custom configurations, and greater attention than standard managed sites, this service includes continuous monitoring, advanced firewall policy and configuration management, VPN maintenance and enhancement. It also covers firmware lifecycle management with follow-up on new releases, network segmentation, and periodic reviews of security templates and standards to ensure alignment with best practices.

22. DMARC Policy Monitoring

We offer DMARC (Domain-based Message Authentication, Reporting and Conformance) policy monitoring services to help protect your organization's email domain from being used in email fraud and phishing attacks.

Our team will help configure and manage DMARC policies to ensure email messages are authenticated and legitimate. We will also monitor and report on email activity to identify potential issues and provide guidance on best practices to improve email security.

© Scott & Scott, LLP

Out of Scope: This support agreement does not include monitoring other email security protocols or third-party email services. Any requirements such as these will incur additional charges.

23. Client Success Manager (CSM)

The Client Success Manager is the primary relationship advocate for the client, ensuring it receives maximum value from your managed IT services. The CSM focuses on communication, transparency, and service satisfaction.

24. Technology Alignment Manager (TAM)

The Technology Alignment Manager ensures that your IT environment adheres to industry's best practices, security standards, and the MSP's proven framework. They bridge the gap between daily operations and strategic readiness by regularly evaluating your technology stack.

25. Current Plans

• Advanced Plan

- **Managed User**
  - Support Desk
  - Anti-Spam
  - Anti-Phishing tool
  - Email, Cloud-based collaboration and Storage solutions (E.g: Teams/Google Meet and OneDrive/Google Drive) cloud backup.
  - Online security awareness training.
- **Managed Workstation**
  - Anti-Virus protection
  - Security updates and Patching
  - Managed Detection and Response (MDR)
  - Next Gen AI Anti-Virus Enterprise Class
  - Workstation Encryption
  - Privileged Access Management (PAM)
- **Managed Server**
  - 1TB per server.
  - Anti-Virus protection
  - Security updates and Patching
  - Managed Detection and Response (MDR)
  - Next Gen AI Anti-Virus Enterprise Class
- **Managed Inbox**
  - Anti-Spam
  - Anti-Phishing tool
  - Email backup

© Scott & Scott, LLP

The Advanced Plan also includes DMARC Policy Monitoring.

Clients additionally benefit from the expertise of our Client Success Manager (CSM) and Technology Alignment Manager (TAM).

Agreements signed in previous years may have different features.

• Add-Ons

CIO Landing can provide the following recurring services or tools upon request:

- **Password Manager:** We will deploy and configure a Password Manager solution, seamlessly integrating it with your systems. This service securely stores and manages user credentials, enforces strong password policies, and provides easy access to passwords across devices. It enhances security by reducing the risk of credential theft and simplifies password management for your team.
- **Vulnerability Assessment:** Our Vulnerability Assessment service offers robust solutions tailored for comprehensive security. It includes network asset discovery, vulnerability tracking, and remediation planning guidance. With features like internal and external scans and Active Directory assessments, we ensure your systems are continuously monitored and secured. **Note:** While remediation guidance is provided, the actual remediation efforts are out of scope for this service.
- **Email encryption:** We will install and configure Email Encryption software, seamlessly integrating it with your email systems. This service works with Data Loss Prevention (DLP) and allows users to encrypt emails on demand, ensuring the security and confidentiality of your email communications.
- **Advanced Email Encryption:** We will install and configure Advanced Email Encryption software, seamlessly integrating it with your email systems. This service works with Data Loss Prevention (DLP) and allows users to encrypt emails automatically and on demand, ensuring the security and confidentiality of your email communications.
- **Email Archiving:** We will deploy and configure an Email Archiving solution, seamlessly integrating it with your email systems. This service securely stores and organizes your emails for long-term retention, ensuring data integrity and compliance with regulatory requirements. It enables easy search and retrieval of archived messages, optimizing email management and supporting ediscovery needs for your business.
- **DNS Filtering:** We offer a DNS filtering solution focused on maintaining web browsing security and adding an extra layer of protection for remote devices. This service blocks access to malicious sites, ensuring safe browsing for all users. In addition, it allows the company to define browsing policies by filtering access to specific categories of content such as adult sites, gambling sites, and other non-business-related websites.

- **Always-on VPN - SASE User Access:** A cloud delivered SASE solution offering secure, seamless access for remote teams across any location.

- **SASE Cloud Gateway:** A cloud delivered SASE solution providing secure, seamless access for remote teams wherever they work. Minimum 1 (one) per company.

© Scott & Scott, LLP

26. Backup and Recovery

CIO Landing offers a complete Backup and Disaster Recovery Solution (BDRS) designed to backup multiple Windows, Linux Servers, along with mailbox backup, cloud storage backup and collaboration platform backup.

Services provided can include provision of:

- An On-site Server (BDR) to carry out data backups and send data to offsite storage datacenter.
- A standby server in the event of a main server/s fail (role played by BDR)
- Daily data backups to the BDR depending on requirements.
- Daily data restoration of files, folders, emails, or email stores on demand when subscribed to the email backup service.
- An Off-site data backup should a total catastrophic event destroy the local backup.
- Full recovery of data and operation at our off-site datacenter facilities*

* CIO Standard backup retention period is set to 90 days. Please refer to the 'Current Plans' section to see the included data storage per server.

Please see additional notes in the Terms and Conditions of the SOW regarding loaned equipment.

For Clients who subscribe to backup services or server support, we include a basic level of data encryption that refers to data in transit or data at rest. Backup files are transferred to the Data Center in an encrypted form. Our software communicates with the remote servers using SSL/TLS (Secure Socket Layers/ Transport Layer Security) technology.

Mailbox Backup

Our Mailbox Backup service ensures the secure preservation of your email data, offering reliable recovery options in case of data loss, accidental deletions, or system failures. CIO Landing manages the installation, configuration, and integration of the Mailbox Backup service with your email system. Regular updates are conducted to stay ahead of emerging threats, ensuring continuous protection for your valuable email data. Proactive monitoring enables us to address potential issues promptly, minimizing downtime and preserving productivity. Please note that customization beyond our standard service may incur additional charges.

Cloud Storage Backup

Our Cloud Storage Backup service provides comprehensive protection for your cloud-based data, ensuring its secure storage and easy recovery. CIO Landing installs, configures, and integrates the backup solution with your cloud storage account. This service extends to users of various cloud storage platforms. Regular updates are implemented to detect and prevent new threats, providing continuous security for your stored files. Proactive monitoring helps us address potential issues swiftly, minimizing any impact on your data accessibility. Customizations beyond the standard service may result in additional charges.

© Scott & Scott, LLP

Workstations Backup Solution

Our Workstations Backup Solution offers seamless protection for your organization's workstation data. With automatic cloud-based backups, critical files are securely stored off-site, minimizing the risk of data loss.

Collaboration Platform Backup

Our Backup service, designed to protect against data loss and ensure efficient recovery options. CIO Landing manages the installation, configuration, and integration of the backup solution with your collaboration platform. This service also extends to users of other collaboration platforms. Regular updates are applied to stay ahead of emerging threats, guaranteeing the ongoing security of your valuable collaboration data. Proactive monitoring enables us to address potential issues promptly, minimizing downtime and preserving productivity. Any customizations beyond our standard service may be subject to additional charges.

Server Backup Solution

Whether your servers are located on premises or in the cloud, we provide flexible backup options tailored to your needs. With automatic backups, both on-site and off-site, your data remains secure and accessible.

26.1 Server Backup Frequency

We provide daily backups which allows multiple restore points to recover the most current version of your data just prior to the data loss event. Off-site backup frequencies will be dependent on image sizes and internet bandwidth available.

26.2 Smart Data Transport

Data transmission can easily be configured to minimize bandwidth consumption. Our technology leverages Adaptive Bandwidth Throttling, which allows us to set a limit on outbound bandwidth used. A backup internet connection may be used for backup file transfer.

26.3 Remote Storage provided by CIO Landing

- Redundant storage with backup images is stored in US Datacenters.
- Connectivity provided by multiple providers with automatic failover capabilities.
- Full 24/7 physical security personnel at each facility including security cameras, and key card access.
- Fire suppression and environmental control provided.
- Automatic backup power provided by on-site generators.

26.4 Retention Policy

Local backups are kept for a minimum of 7 days. We will store as many backups as possible depending upon the storage available. The Client is responsible for advising the length of time they need CIO Landing to retain backups for. Retention is based on hard drive space available on the backup server. When the storage space is full, CIO Landing will overwrite the oldest backup copy first.

Off-site backups are kept for 90 days on a First In First Out (FIFO) basis. We can retain backups for as long as required by the Client. Cloud storage space is included in the CIO Landing plans. For details regarding inclusions and limitations, kindly consult the Current Plan.

© Scott & Scott, LLP

26.5 Ownership of the Data

The backup data being stored on the BDR and at the Data Center remains the sole property of Client. If the Client chooses to terminate services, CIO Landing will assist the Client in the orderly termination of services. This could involve copying the backup image to an external drive which can be synchronized with the data on the BDR. The Client agrees to pay CIO Landing the actual costs of rendering such assistance.

26.6 Restore and Disaster Recovery

CIO Landing will attempt to retrieve backups within 24 hours of the first request. The BDR can also be used to perform a bare metal restore to dissimilar hardware which means that when a new server arrives, the BDR can be used to restore the most current data to that new server regardless of the server hardware. Restoration speed will depend on hardware performance and internet bandwidth.

27. Hardware support

CIO Landing is an authorized reseller of various IT products, such as workstations, printers, and laptops. We strongly recommend purchasing the required hardware through our recommended suppliers. This ensures that your business infrastructure meets the necessary technical specifications and allows you to benefit from potential costs savings available through our IT partnerships.

If hardware is purchased through CIO Landing, we will take responsibility for liaising with the vendor throughout the entire lifecycle.

If purchases are made outside of CIO Landing, it will be the Client's responsibility to manage the vendor, request the RMA (return merchandise authorization) in the event of failure, and handle the shipment of equipment.

CIO Landing serves as a reseller for a wide range of brands, and our partnerships enable us to offer faster replacements for any products that may fail.

28. Software support

We offer tailored IT solutions to our clients, including products such as Microsoft 365, Adobe suite, and common Line of Business apps e.g. (QuickBooks, Clio, Zoom).

Support for other software will be provided on a best effort basis. Customization of any sort is not included. Requirements such as these will incur additional charges or may be denied accordingly.

29. Internet Services

For the client's business premises only, CIO Landing will liaise with our recommended vendors for any new or existing internet services in the event of a service disruption. However, we cannot be held responsible for any outages caused by the Customer or any Third Party.

Upload and download speeds vary according to the provider.

© Scott & Scott, LLP

We will also provide you with alternative options for a backup internet line at any of your office locations where required.

Out of Scope: CIO Landing will not be responsible for any early termination fees of existing internet providers if the Customer requests to change ISP's.

We will not be responsible for managing the internet service provider for remote workers, nor will we take responsibility for any delays caused by home internet services (such as fiber and broadband). We will also not engage with any individual ISPs regarding home-related issues unless the location has specifically been included in the SOW.

30. Software License Management

CIO Landing recommends its customers utilize the Microsoft 365 Suite, and we will handle the management of licensing as part of our service. If a license is no longer needed, it is the Client's responsibility to inform CIO Landing, so that it can be either removed or reallocated. This helps prevent unnecessary costs associated with overprovisioning.
Specific Line of Business applications which require licenses should be managed by the Customer, unless otherwise agreed.

31. Enterprise Governance: Policies and Procedures

All processes and procedures described in this agreement are documented in our Knowledge Base, along with our Standard Operating Procedures.

Once Client-specific processes are provided to CIO Landing during and after the onboarding process, they can be added to the Knowledge Base. This enables us to offer support in those specific areas.

32. Project Services

As a general concept, projects will be determined by the "3/3/3 Rule" A project will be considered billable if it meets any of the following criteria:

- Involves the participation of three or more individuals.
- Encompasses more than three tasks.
- Is projected to require more than three hours of work.

No project work is included in our maintenance plans.

However, CIO Landing offers planning, design, and implementation services for projects related to existing equipment or equipment migration. These services are subject to additional fees. To proceed with such projects, CIO Landing will require collaboration with the Client to establish a detailed scope, agree on a clear proposal with defined objectives, and determine the expected outcomes.

© Scott & Scott, LLP

In the event that the Client does not concur with the selected project execution approach proposed by CIO Landing, the project will be terminated. Subsequently, a new project shall be initiated, guided by an execution strategy mutually agreed-upon with the Client.

33. Technology Business Review

Upon the agreed timeframe, we will generate a comprehensive IT Service Report as part of our Technology Business Review, available upon request. This report will include the following information:

- An overview of the Support incidents and requests raised since last review.
- A summary of your company's infrastructure performance
- Review of IT strategy and business goals
- Risk Register
- Updates on any new and existing projects
- Customer satisfaction and areas for improvement

Furthermore, it will give you the opportunity to discuss any other areas you wish to prioritize, enabling you to align your IT strategy with your business goals.

34. Third Party IT Supplier Management

The Client grants authorization to CIO Landing to contact third-party IT support providers on their behalf. If requested by the Client, we will provide a Vendor Authorization Letter (VAL). It is the Client's responsibility to send this letter to their third-party providers to authorize CIO Landing to make changes on their behalf. We can assist in coordinating this process.

Please note that services performed with any of the Client's third-party vendors, whether a VAL has been signed or not, may be billed separately and outside the scope of the Services.

© Scott & Scott, LLP

Appendix 1 – In Scope Service Summary

The following is a summary of the services that are covered by this Managed IT Service.

Incident Management
- Remote Service Desk Support for Workstations & Servers
- IT Support by Telephone, Email and On-site visits
Workstations Support & Access Management
- Manage workstation computers (Windows, Mac)
- Manage mobile devices (Android, iOS)
- Management of network devices (Printers, Scanners, UPS, NAS)
- Provide support to Line of Business applications (MS Office suite, browsers)
- Setup new computers (installation of LOB apps per company guidelines)
Remote Monitoring (e.g. Networking, Capacity, Events)
- Monitor Windows Servers & VMWare (24 x 7 x 365)
- Monitor server resources, roles & services
- Performance Monitoring & Capacity Planning
- Install firmware/ driver updates as needed
- Install & maintain approved Line of Business applications
- Critical Services / device alerting and internet connectivity
- Monitor logs for potential issues
- Monitoring of on and offsite backup status
Server Support (Change, Release & Deployment Management)
- Windows patch management on all servers
- Performance Monitoring & Capacity Planning
IT Information Security Management
- Provision of security software, updates, and monitoring
- Monitoring of suspicious network activity
- Web access protection
- Management of Client provided File Security & VPN Policy
- Management of Client provided content filtering policy/ traffic shaping

© Scott & Scott, LLP

- Cybersecurity awareness training
IT Supplier Management
- 3rd party Supplier Management Services
- Domain/ DNS/ SSL Certificates Management
- Application Management*
Documentation for process & procedure standardization
- Comprehensive documentation of: Network infrastructure, LOB applications, and IT management procedures.
- Hardware and Software Changes
- IT Security policies
Other
- Email management
- Technology Solution Consulting & Engineering*

**Labor only. Where 3rd party maintenance agreements exist.*

Only devices that have the CIO Landing agent installed on the system or an MDM agent installed will be supported, for mobile devices this extends only to basic functionality, e.g., configuration of business applications.

Offboarding will be limited to the removal of our software stack. Any additional work beyond this scope may incur an additional charge.

© Scott & Scott, LLP

Appendix 2 - Out of Scope Services Summary

The following is a more detailed summary of the services and costs that are not covered or supported on the Managed IT Service Quote.

CIO Landing specifically excludes the following services.

Disaster Recovery
• Failure due to acts of God, building modifications, power failures or other adverse environmental conditions or factors. • Recovering and rebuilding after floods, fires, earthquakes, lightning strikes, pipe leaks, power surges/ failures, ransomware attacks, security breaches, etc. • Backup & Disaster Recovery Plan
Hardware Removal and Recycling
• We can suggest 3rd party destruction companies for the removal of old computers/ servers/ phones or networking equipment. CIO Landing will separate the Hard drives, if needed, from such devices and will provide to a 3rd party destruction company who will provide certification of destruction for a nominal fee.
IT Security Audits
• CIO Landing may fully cooperate with the Client in any IT Security audit, however the time spent will be part of a separate agreement.
Maintenance of modified IT equipment
• Service and repair made necessary by the alteration or modification of equipment other than that authorized by MSP, including alterations, software installations or modifications of equipment made by Client's employees or anyone other than CIO Landing.
Office Location Moves (not individual desk moves)
• Moves from one office location to another are not included. If any moves are planned, we can help with setting up equipment, but this will be part of a separate agreement.
Out of Vendor Warranty/ Support
• Parts, equipment, or software not covered by vendor/manufacturer warranty or support.
Programming
• Programming (modification of software code) and program (software) maintenance.

© Scott & Scott, LLP

Server rebuilds or removals
• Server rebuilds or removals plus cloud migrations or projects such as server virtualization.
Shipping and handling fees
• Cost of transporting IT equipment, for example for new employee workstations.
Training & Education
• IT Training other than security awareness related.
Wiring
• Of any kind.

© Scott & Scott, LLP

Appendix 3 - List of Approved Connected Devices

CIO Landing provides support for USB or network connected devices that pertain to normal business operation. Gaming devices, surveillance equipment and such like are considered out of scope. We do not provide support for all devices that connect to the internet.

Descriptions in this document are subject to change any time without notice.

© Scott & Scott, LLP