



# DCB TECHNOLOGY, LLC

Effective February 29, 2024. This Schedule of Services supersedes and replaces all prior versions.

## Schedule of Services

### **MANAGED SERVICES**

The Services to be performed for Client by Provider are set forth in the Order. Although the quantities may be adjusted without an Order, additional Services may be added only by entering into a new Order including those Services. The ordered subscription can be upgraded, but cannot be downgraded during the Initial Term.

#### **Business Essentials Plus**

- Managed Endpoint Security
- Proactive Health Monitoring
- Proactive Remediation
- Automated Monthly Tune-ups for Windows devices
- System Patch Management
- Monthly Executive Report
- Systems Monitored by 24x7x365 SOC (Security Operations Center)

#### **Business Complete Care**

- Managed Endpoint Security
- Proactive Health Monitoring
- Proactive Remediation
- Automated Monthly Tune-ups for Windows devices
- System Patch Management
- Monthly Executive Report
- Monitored by 24x7x365 SOC (Security Operations Center)
- Cloud-based file-level System Backup up to 50GB per Workstation or Server (additional fees apply after 50GB data used)

#### **Business Complete Care with Productivity Suite**

- Managed Endpoint Security
- Proactive Health Monitoring
- Proactive Remediation
- Automated Monthly Tune-ups for Windows devices
- System Patch Management
- Monthly Executive Report
- Systems Monitored by 24x7x365 SOC (Security Operations Center)
- MDR for Microsoft 365 (Client must utilize Microsoft 365 for email and entire tenant must be managed by DCB Technology, LLC)
- Cloud-based file-level System Backup up to 50GB per Workstation (additional fees apply after 50GB data used)

- Premium Installable Microsoft Office 365 Apps
- 1TB OneDrive Cloud Storage
- Microsoft Exchange Email Hosting
- Proofpoint Essentials Email Security (Client must utilize Microsoft 365 for email and entire tenant must be managed by DCB Technology, LLC)
- Network-wide DNS filtration service (if client has a Static IP and requests this service to be activated)

### **Home Essentials +**

- Managed Anti-Virus monitored by IT Professional
- System Health Monitoring
- Automated Monthly Tune-ups for Windows devices
- System Patch Management
- Proactive Remediation of Common Issues (i.e. jammed print queue)

### **Home Complete Care**

- Managed Anti-Virus monitored by IT Professional
- System Health Monitoring
- Automated Monthly Tune-ups for Windows devices
- System Patch Management
- Proactive Remediation of Common Issues (i.e., jammed print queue)
- Cloud-based file-level System Backup up to 50GB per Workstation (additional fees apply after 50GB data used)

### **Network Patch Management with IDS/IPS Monitoring**

- Businesses with Ubiquiti or Unifi hardware managed by Provider will receive firmware updates as they are released, tested, and approved by Provider.
- Provider will monitor Intrusion Prevention System (if applicable) for threats and endeavor to take action as required to mitigate.

### **MANAGED SECURITY SERVICES**

Provider, through its Third-Party Services Providers will make its best effort to ensure the security of Client's information through third-party security software ("Security Software"). Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of this Service is subject to the applicable Third-party Service Providers agreements regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client acknowledges that Third-Party Service Providers and their licensors own all intellectual property rights in and to the Security Software. Client will not engage in or authorize any activity that is inconsistent with such ownership. Client acknowledges and agrees to be bound by any applicable Third-Party Service Provider agreements regarding terms or use or end user licensing terms, and Client understands that any applicable agreement regarding terms of use or end user licensing is subject to change without notice.

**Firewall, Anti-malware, and Intrusion Detection** – Provider will install and configure of firewall traffic policies, apply updated firmware when applicable, and configure changes when needed. With respect to the firewall, Provider will include the following:

- Intrusion Prevention - provides real-time protection against network threats, including spyware, SQL injections, cross-site scripting, and buffer overflows.
- URL Filtering - blocks known malicious sites, and delivers granular content and URL filtering tools to block inappropriate content.
- Gateway Antivirus - continuously updated signatures, identify and block known spyware, viruses, trojans, worms, rogware and blended threats – including new variants of known viruses.

**Network Discovery** - generates a visual map of all nodes on your network, making it easy to see where you may be at risk.

**Reputation-Based Threat Prevention** - Cloud-based web reputation service that aggregates data from multiple feeds to provide real-time protection from malicious sites and botnets, while dramatically improving web processing overhead.

**Spam Prevention** - Real-time, continuous, and highly reliable protection from spam and phishing attempts.

**Application Control** – Provides the ability to allow, block, or restrict access to applications based on a user’s department, job function, and time of day.

**APT Blocker** - detects and stops the most sophisticated attacks including ransomware, zero-day threats, and other advanced malware designed to evade traditional network security defenses.

**Intelligent Antivirus** – leverages signature-less anti-malware solution that relies on artificial intelligence to automate malware discovery.

**DNS Filtering** - detects and blocks malicious DNS requests, redirecting users to a safe page with information to reinforce security best practices.

**Anti-malware** - Provider will provide and install anti-malware software of Provider’s choosing for each Device covered by the Order. While Provider will make reasonable effort to ensure Client Devices and Client’s network are safe from viruses, malware, bugs, hacking, phishing schemes or defective or malicious files, programs or links (“Harmful Content”), of any kind whether now known or hereinafter invented, Provider does not guarantee that Client computers or network cannot be infected by Harmful Content. Where this does happen, Provider will provide commercially reasonable Services to mitigate the Harmful Content. Additional Services will be available upon mutual agreement of the parties.

**Remote Access** - Provider will install remote access and remote monitoring and management software on Client’s Devices possibly other equipment at Client’s office. Client grants permission to Provider to install any remote access or remote monitoring and management software deemed necessary by Provider.

**Security Awareness Training & Phishing Simulations** - Provider will acquire and will assign an appropriate number of licenses to support the client environment. The Service will schedule

phishing campaigns to send at random times during a specified period. The campaigns are trackable and fully customizable designed to keep track of every user's participation, making all cybersecurity education accountable and measurable.

#### **Multi-Factor Authentication Services / Password Credential Management Services –**

Provider will configure two-factor authentication for compatible software applications, institute single sign-on services for compatible software applications and customized security policies and procedures. After performing a security assessment and assessing the state of Client's existing policies and procedures pertaining to network security (if any), Provider will work with Client to prepare a new or revised set of policies and procedures that incorporate cutting edge best practices and that take advantage of the other Services delivered by Provider.

#### **Security Operations Center – The Services include:**

- Advanced Malware Protection supported by Security Operations Center (SOC).
- Deployment of advanced malware protection applications to all Windows based devices on customer network.
- 24x7 SOC service analyzes quarantined applications and files, reducing false positives.
- Immediate risk identification – Provides rapid recognition of thousands of viruses and malware attack variants, including cryptomining attacks, as well as the root causes of these malicious behaviors, by quickly identifying and diagnosing corrupt source processes and system settings.

**Security Log Management** – Provider will configure log sources to capture and retain information without creating excessive logging, limit user access to log files, avoid logging sensitive or protected information, secure the processes that generate logs, identify and resolve logging errors, and analyze log entries, prioritize entries, and respond to those requiring action.

**Incident Response** - Provider will assist Client in the hours immediately following a data breach to identify the likely source of the breach and to begin formulating an appropriate response to the breach. However, any assistance with data breach-remediation efforts past the first twelve (12) hours following a breach – including but not limited to breach-notification planning, in-depth forensic examinations of the source of a breach, and significant, post-breach systems reconfiguration – are not within the scope of this Service Attachment. If Client requests Provider's assistance with such activities, Provider will prepare a separate Service Attachment for Project Services that will specify what the charges will be for such assistance.

#### **DATA BACKUP AND DISASTER RECOVERY SERVICE**

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a separate Order including those Services.

**Local Backups** - Using customer provider hardware and software that is approved and supported by Provider (backup software), backups will be performed on the basis specified in the Order. Client owns the hardware and software agents (backup software) used to perform the backups. If Client subscribes to periodic Server Maintenance, Provider will review the backups during Maintenance. Client will notify the Provider of any failures, and upon request, perform simple on-site tasks (e.g., powering down and rebooting hardware).

**Remote Backups** - Provider, through its Third-Party Service Providers will make its best effort to ensure the protection and recovery of Client's information. Data files are backed up via a third-party client-side desktop/server software application (the "Application"), encrypted, and then sent to a storage server at third-party vendor's data center facility. There is no local copy of the backed-up data. Data files can be restored from the cloud but the server itself usually cannot be recovered or "booted" in the cloud. Therefore, this service is not considered a disaster recovery solution. All data is backed up via a third-party client-side desktop/server software application (the "Application"). Provider will monitor the backups daily, notify Client of any failures, and work with third-party to resolve backup failures.

**Cloud Backup** - Provider, through its Third-Party Service Providers will make its best effort to ensure the protection and recovery of Client's information. Data is backed up via a third-party client-side desktop/server application, encrypted, stored locally on a Provider-owned storage device ("Provider Owned Storage"), and then sent to a third-party owned storage server at the Third-Party Services Provider's data center facility. Provider will monitor the status of all scheduled backup jobs, notify Client of Provider-owned storage failures and corrective actions. Provider will also provide remote administrative services of Data Backup Service as requested by Client. Offsite Backup copies will have one-year retention unless specified in Order. Upon termination of these Services, Provider will request return of the backup hardware and remove the Application from Client systems.

### **Disaster Recovery**

Provider will work with Client to develop a comprehensive disaster-recovery plan that incorporates the Services to be delivered under this Service Attachment.

If Client experiences an event precipitating a major, multi-user loss of data, Client may notify Provider that a data loss event has occurred.

As related to any and all backups, Provider reserves the right to remove or trim the backups after 60 days.

Clients that backup their files to DropBox and/or OneDrive do so at their own risk, and Provider is not responsible for the security or reliability of those backups.

### **FILE BACKUP AND RECOVERY**

Provider will create, monitor, and modify up to the number of file backup jobs listed in the Order. Provider will also notify Client by email of backup drive failures and corrective actions. Client is required to identify all devices/drives to be included in backups.

Upon request, Provider will remotely restore files, subject to the number of operations listed in the Order

### **CLOUD AND HOSTING SERVICES**

**Third-Party Cloud & SaaS Vendors** - Provider will provide, install, and support the Third-Party Cloud or software-as-a-service vendors listed on the Order, including but not limited to Microsoft. Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of this software is subject to the applicable third-party cloud or software-as-a-service vendor's agreement regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client agrees to

be bound by any applicable third-party cloud or software-as-a-service vendor's agreements regarding terms or use or end user licensing, and Client understands that any applicable agreement regarding terms of user or end user licensing is subject to change by any Third-Party vendor or software-as-a-service provider without notice.

### **CYBER TRAINING SERVICES**

Provider will implement and manage a managed cybersecurity awareness training platform ordered through a third party on Client's behalf. The program features:

- Enrolling all technology-facing workforce members in the program
- Access to a curriculum of industry-leading cybersecurity awareness education which can be customized to meet the unique needs and regulatory requirements of Client
- Management reporting and visibility into workforce participation and progress in the training
- Regular campaigns to test each workforce member's ability to recognize and effectively respond to cyberattacks which typically target individuals
- Automated enrollment in remedial training for individual workforce members, when appropriate
- Management reporting and visibility into workforce performance on testing campaigns
- Management reporting and visibility into the improvement in workforce awareness and performance over time
- Lowered risk to (Client) from cyberattacks which target unaware and untrained individuals

### **VOIP AND COLLABORATION SERVICES**

Provider will deliver the Voice over Internet Protocol ("VoIP") and associated telephony and collaboration services specified and selected by you on the Order or Proposal. Additional Services may be added only by entering into a new Order including those Services.

The VoIP Services may be provided or delivered by Provider through the use of third-party vendors listed on the Order or Proposal. Use of the VoIP Services are subject to any applicable third-party vendor agreements. Client acknowledges and agrees to be bound by those third-party vendor agreements. Provider shall not be responsible for any third-party vendor service failures when accessing or using the Services. Client agrees to be bound by any applicable third-party vendor's agreements regarding terms and conditions or end user licensing, and Client understands that any applicable agreement regarding terms and conditions or end user licensing is subject to change by any third-party vendor without notice.

Network cabling, conduit, electrical, rack space, and any other required construction or trenching are additional charges are not included with the Service.

\*\*Provider does not provide internet connection. Client is responsible for providing internet connection to use the Service.

**THESE DESCRIPTIONS ARE SUBJECT TO CHANGE ANY TIME WITHOUT NOTICE.**