Effective August 1, 2024. These Service Descriptions supersede and replace all prior versions.

# Schedule of Services

## MANAGED SERVICES

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 new Order including those Services.

### FREEDOM FACTORY PRO

#### Technology Support Services

- Technology Monitoring and Alert Services. FeatherShark will use our remote monitoring and management (RMM) technology suite to monitor and receive alerts on your internet connections, network infrastructure, PC, and laptop computers.
- Remote Helpdesk Services. FeatherShark will provide support services for your personnel for any technical or "how to" issues. Tickets may be filed by phone call, e-mail, or online.
- Unlimited On-site Support. We can resolve the vast majority of all issues remotely, but for items we can't, FeatherShark will provide unlimited onsite support services in your offices during normal support hours.
    - Normal Support Hours. Normal support hours are M-F, 8:00am - 5:00pm Central Time, except holidays.
    - 24x7 Emergency Support. FeatherShark will maintain emergency support outside normal support hours for critical outages and technical issues. We will monitor your networks and critical pieces of your technology outside of working hours, and technicians are on call to resolve issues.
    - Support for all your devices. We will provide support for mobile devices - smart phones and tablets - as it relates to your business technology, not just your PCs and laptops.

#### Strategic Technology Planning

- IT Planning. We will meet regularly via conference call to discuss progress on your ongoing technology initiatives and to align on new priorities.
- Technology R&D. We will perform research and budget development for your technology initiatives as requested.
- Security Planning. We will continually work with you to make sure that your networks and systems are secured against existing and developing threats.
- Technology Replacement Planning. FeatherShark will work with you to develop a plan to refresh your computers and IT equipment regularly on a planned cycle. Each year a portion of your technology will be replaced to make certain that your team is operating on updated equipment and that your costs are manageable and predictable.

#### Centralized Technology Management

- Software-as-a-Service Management. We will manage and support SaaS products used in your IT infrastructure such as directory services, Office 365, File Services, and email protection.
- Vendor Management Services. FeatherShark will serve as your central point of contact and interface with your technology-related vendors, such as telecom, fax/copier, web development, web hosting, domain registrar, and hardware providers.
- Asset and Equipment Tracking. We will maintain a database of your computers under management and networking equipment.
- Equipment Purchasing. We will specify requirements for new technology purchases, and can either purchase technology on your behalf or work with your hardware vendor for purchasing.
- Employee technology on-boarding and termination. Assist with properly on-boarding new employees, providing them with computer and software setups and training.
- Equipment Recycling. At your request, we will arrange for recycling of technology after it is decommissioned.
- Software License Tracking. We will track software application licenses, and maintain a database of your product keys.
- Internet connectivity services. FeatherShark will provide direct contact with Internet Service Providers in all your locations to resolve service issues.
- Endpoint Protection. FeatherShark will manage your endpoint protection strategy and environment, and manage updates, scans, and quarantines of malware.

**Backup and Disaster Recovery.** With Client's assistance, FeatherShark will manage your Backup and Disaster Recovery (BDR) solution, confirming that backups are running as expected and that your systems can be brought back online in case of an outage or disaster.

## 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, rogueware and blended threats – including new variants of known viruses.

**Security Risk Assessment**

- Malware and Vulnerability Review – Using one or more tools to determine the existence of malware or vulnerabilities.
- Personally Identifiable Information ("PII") – Review practices related to PII, including location, treatment, and risk mitigation.
- Report – Provider's findings will be included in a Risk Assessment Report.

**SECURITY ADD-ON SERVICES**

**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.

**Client-Side DNS Filtering -** Provider will acquire and will assign an appropriate number of licenses to support the deployment of client-side DNS Filtering on all laptop systems. The DNS filtering is designed to detect and block malicious DNS requests, redirecting users to a safe page with information to reinforce security best practices and to protect laptops while away from the corporate network.

**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.

**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 twenty-four (24) 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.

## CLOUD AND HOSTING SERVICES

**Public Cloud -** Provider will move all Client's data to a cloud computing platform, allow Client to have access to data via virtual desktop from Client's own devices or device provided by Provider, and manage the cloud environment for Client.

**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 Google, Microsoft, JumpCloud, and Egnyte. 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.

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