

Lab Services Agreement

This Lab Services Agreement (this "Agreement") is a legal agreement between Secure Data Technologies, Inc. ("Secure Data") and the Client identified on an order form ("Client") and governs any Statement of Work, quote, proposal, or other ordering document executed by Client ("Order Form") that references this Agreement. The Order Form will be issued to Client by Secure Data. This Agreement is effective on the date Client executes the Order Form or submits a matching purchase order to Secure Data (the "Effective Date").

This Agreement permits Client to purchase the lab and integration services defined herein and which are identified in the Order Form (collectively, the "Lab Services") and sets forth the terms and conditions under which those Lab Services will be delivered. The Agreement consists of the terms and conditions set forth below, the Master Agreement between the parties, and any Order Forms that reference this Agreement. If there is a conflict between the terms below, the Order Form, or the Master Agreement, the documents will control in the following order: The Master Agreement, the Order form (which may from time to time contain alterations to these standard terms and conditions), then this Agreement.

BY EXECUTING, WHETHER MANUALLY OR ELECTRONICALLY, AN ORDER FORM, DELIVERING A PURCHASE ORDER OR OTHER CONFIRMATION TO SECURE DATA, OR OPERATING, DOWNLOADING, INSTALLING, REGISTERING OR OTHERWISE USING THE PRODUCTS, OR CLICKING AN "I ACCEPT" OR "CONTINUE" BUTTON ASSOCIATED WITH THIS AGREEMENT, CLIENT (OR ITS AUTHORIZED AGENT, IF APPLICABLE) EXPRESSLY AND EXPLICITLY ACKNOWLEDGES AND AGREES THAT THIS IS A BINDING AGREEMENT AND CLIENT HEREBY AGREES TO THE TERMS OF THIS AGREEMENT AND ACCEPTS THE OFFER TO PURCHASE THE LAB SERVICES PURSUANT TO THE TERMS HEREIN.

In consideration of the mutual covenants and agreements contained herein, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. SCOPE

1.1 Lab Services; Service Levels. Client will purchase, and Secure Data will provide, the specific Lab Services identified in the applicable Order Form (the "Subscribed Lab Services"). Secure Data's Lab Services are organized into four standard service levels (each a "Service Level"):

- Level 1 – Inventory & Kitting
- Level 2 – Non-Powered Services
- Level 3 – Powered Services
- Level 4 – Integrated Rack Builds

The scope of each Service Level is described below. Secure Data will only perform those Lab Services that are expressly identified as Subscribed Lab Services in an Order Form or statement of work.

1.2 Level 1 – Inventory & Kitting.

1.2.1 Inclusions – Level 1. Unless otherwise specified in the Order Form, Level 1 Lab Services may include:

- Receipt of Client-owned or Secure Data–procured equipment at Secure Data facilities.
- Visual inspection of packaging for apparent shipping damage.
- Capture of serial numbers and basic device information and creation or update of asset records in Secure Data's systems.
- Assignment of bin, shelf, or pallet locations in Secure Data's warehouse and internal inventory systems.
- Secure storage of boxed equipment in a commercial environment suitable for typical IT hardware.
- Assembly of user or site kits (for example, PC + monitor + dock + keyboard/mouse + accessories) without powering on devices.
- Application of basic labels to cartons or kits (for example, user name, department, destination site, or project ID).

1.2.2 Exclusions – Level 1. Unless explicitly included in the Order Form, the parties agree the following are not included within the scope of Level 1 Lab Services:

- Any configuration, firmware updates, or powering on of devices.
- Long-term warehousing or archival storage beyond the periods or capacities stated in the Order Form.
- Packing or repacking with custom or specialized materials that Secure Data does not ordinarily stock.
- Insurance coverage beyond Secure Data's standard commercial property and liability insurance.
- Disposal, recycling, or destruction of hardware (which may be provided as separate billable services).

1.2.3 Client Responsibilities – Level 1. Client will:

- Ensure ownership of, and title to, all Client-supplied equipment and warrant that it may lawfully be stored and handled by Secure Data.
- Provide packing lists and equipment manifests sufficient for Secure Data to verify inbound shipments.
- Specify any special handling requirements (for example, unusually fragile, high-value, or environmentally sensitive devices) in advance and in writing.
- Acknowledge that risk of loss for equipment remains with Client except to the extent expressly allocated to Secure Data in this Agreement or the Master Agreement.

1.3 Level 2 – Non-Powered Services.

1.3.1 Inclusions – Level 2. Unless otherwise specified in the Order Form, Level 2 Lab Services may include:

- Application of Secure Data and/or Client-specified physical asset tags to devices or cartons.
- Creation or update of detailed asset records (serial, make/model, PO, project, location) in Secure Data's systems and, where agreed, in Client-provided systems.
- Product registration and warranty/entitlement activation with hardware and software vendors using serial numbers or license keys.
- Enrollment of devices into vendor or cloud management portals (for example, Cisco Smart Accounts, FortiCloud, Microsoft Autopilot/Intune) using serial numbers or equivalent identifiers.
- Labelling of boxes or devices to indicate enrollment status and any special handling instructions.

1.3.2 Exclusions – Level 2. Level 2 does not include:

- Powering on hardware, imaging, software installation, or any network configuration.
- Guarantee of acceptance or continued eligibility of serial numbers or devices by third-party portals or vendors.
- Responsibility for vendor platform outages, API changes, or policy changes that prevent registration or enrollment.
- Design or advisory services for Client's Autopilot/MDM/portal architecture (which may be scoped separately).

1.3.3 Client Responsibilities – Level 2. Client will:

- Provide accurate tenant, subscription, and portal access information in a timely manner.
- Maintain appropriate licenses and subscriptions with third-party vendors and cloud providers.
- Remain solely responsible for the configuration of its MDM, Autopilot, or cloud management policies beyond the enrollment actions described herein.

1.4 Level 3 – Powered Services.

1.4.1 Inclusions Endpoints (PCs, Laptops, Thin Clients, etc.) – Level 3. Unless otherwise specified, Level 3 endpoint Lab Services may include:

- Unboxing and bench setup of Client devices on ESD-safe lab benches.
- Installation of operating system images or execution of scripted build processes agreed with Client.
- Joining devices to Client's directory or identity systems (for example, Active Directory or Azure AD/Entra ID) as authorized by Client.
- Installation of standard and role-based software packages, including security agents.
- Application of current patches and updates in line with Client's documented standards.
- Basic security hardening, drive encryption (where specified), and verification that required agents are running.
- Functional testing (login, network connectivity, launch of key applications, basic hardware checks).
- Shutdown, repackaging, and external labeling for end user or destination site

1.4.2 Inclusions – Network & Security Infrastructure – Level 3. Where network and security devices are included at Level 3, services may include:

- Powering on and connecting devices in a lab environment.
- Upgrading or downgrading firmware to a Client-approved standard version.
- Applying Client-approved base configuration templates and making documented, Client-specific adjustments (for example, VLANs, IP addressing, base firewall policies).
- Performing basic smoke tests (for example, ping, interface status, HA/stack checks, sample policy tests where feasible).
- Saving and archiving configurations in Secure Data's configuration repository or other agreed system.

1.4.3 Exclusions – Level 3. Unless specifically included in an Order Form, Level 3 does not include:

- Full-scale performance, penetration, or security testing.
- Onsite installation, cutover, or production deployment (these are handled under Professional Services or Managed Services, as applicable).
- Design of new architectures, networks, or security policies (beyond applying provided templates).
- Guarantees that pre-deployment testing in the lab will identify all issues that may arise in Client's production environment.
- Data recovery from any device that arrives containing data; Level 3 work may overwrite or destroy existing data.

1.4.4 Client Responsibilities – Level 3. Client will:

- Provide, maintain, and approve golden images, configuration templates, naming conventions, and security standards.
- Ensure that any devices shipped to Secure Data with live or production data have been backed up; Client accepts that imaging and configuration tasks may irreversibly delete data.
- Provide and maintain necessary credentials and remote access to Client's identity, directory, and management systems.
- Review and approve representative sample builds and configurations as requested by Secure Data before large-scale production.

1.5 Level 4 – Integrated Rack Builds.

1.5.1 Inclusions – Level 4.

Unless otherwise specified, Level 4 Lab Services may include:

- Assembly of racks with predefined power, cable management, and mounting hardware.
- Installation of servers, switches, firewalls, storage, and other devices in the rack according to an agreed rack elevation and design.
- Power and network cabling within the rack, including labeling at both ends.
- Application of Client-approved configurations (typically building on Level 3 work).
- Functional testing of inter-device connectivity and core network behavior where feasible in the lab.
- Production of as-built documentation, including final rack elevation and cable maps.
- Preparation of racks for shipment, including strapping to pallets or shock-mount frames and basic protective wrapping.

1.5.2 Exclusions – Level 4.

Level 4 does not include:

- Site preparation (power circuits, cooling, physical infrastructure) at Client locations.
- Onsite installation, racking, cabling outside the rack, or final cutover activities (these are handled under Professional Services or Managed Services, as applicable).
- Responsibility for structural or environmental constraints at the destination site (doorway dimensions, floor loading, HVAC, and similar constraints).
- Any obligation to maintain or support the rack after shipment, except as otherwise covered by a separate managed or professional services agreement.

1.5.3 Client Responsibilities – Level 4.

Client will:

- Provide accurate and complete design documentation, power budgets, and IP addressing plans.
- Confirm that destination sites are physically able to receive and house the assembled racks (including elevator and doorway dimensions, floor ratings, power, and cooling).
- Assume responsibility for onsite installation, bolting, and integration with existing infrastructure, or contract separately with Secure Data for those activities.

1.6 General Client Responsibilities.

In addition to any responsibilities specific to a given Service Level, Client agrees to:

- Provide timely access to information, documentation, credentials, and approvals required for Secure Data to perform the Lab Services.
- Cooperate with Secure Data scheduling, including providing reasonable notice of required ship dates and deployment windows.
- Maintain active support agreements and warranties with hardware and software vendors where such agreements are required to perform Lab Services.
- Maintain insurance appropriate for its equipment while in transit and at Secure Data facilities, except to the extent coverage is expressly provided by Secure Data under the Master Agreement or this Agreement.
- Promptly notify Secure Data of any planned major deployments or changes that materially affect Lab Services (for example, large refresh projects, site openings, or design changes).

2. SERVICE REQUESTS, PRIORITIES, AND SCHEDULING.

2.1 Service Requests and Incidents.

A service request is any request by Client for Lab Services (for example, to receive new shipments, build devices, assemble kits, or ship equipment). An incident is a deviation from expected Lab Services performance, such as mis-labeled shipments, missing components in a kit, or build/configuration errors.

Secure Data will log Service Requests and Incidents in its ticketing system and classify them according to priority levels consistent with Secure Data's Managed Services response model.

2.2 Priority Levels and Response Targets.

Unless otherwise stated in an Order Form, Lab Services tickets will use the same priority classifications (P1-P4) and response targets defined in Secure Data's standard Managed Services Agreement (<https://www.securedatatech.com/msterms>), with the following clarifications:

- **P1 – Critical:** A Lab Services issue that is preventing or imminently threatening a major deployment or project go-live (for example, a critical rack build is missing, mis-built, or lost; or a large batch of devices has a serious configuration issue).
- **P2 – High/VIP:** A Lab Services issue that significantly affects a subset of users, locations, or project timelines but does not fully prevent operations.
- **P3 – Standard:** Normal Lab Services requests and minor issues, including routine builds, kit assembly, and non-urgent corrections.
- **P4 – Low.** Minor issues or requests with clear workarounds and no material impact on project timelines.

Response times will align with the Managed Services Agreement, but actual physical lab work requiring access to facilities will generally be performed during Normal Business Hours unless otherwise agreed in writing.

3. SERVICE LEVEL MEASUREMENT AND CREDITS.

3.1 Performance Measurement. Secure Data will measure its response performance for Lab Services tickets in the same way it measures performance for Managed Services tickets, based on its ticketing system data and the SLA definitions referenced above.

3.2 Service Credits. If Secure Data fails to meet agreed response targets for a material portion of P1-P3 Lab Services in any calendar month, Client may be eligible for service credits in the form of a percentage credit against the monthly recurring Lab Services charge (not to exceed 25% of regular monthly charges), as further detailed in the Order Form or Master Agreement. Service credits, if offered, will be Client's sole and exclusive remedy for failure to meet response SLAs.

The process for requesting and applying service credits (including notice periods and eligibility) will follow the same process set forth in Secure Data's Managed Services Agreement, unless otherwise specified in the applicable Order Form.

4. TERM AND TERMINATION.

4.1 Initial Term and Renewals. The onboarding period for Lab Services begins on the Effective Date of the first Order Form that references this Agreement. During onboarding, Secure Data and Client will establish images, configurations, standards, and operational procedures needed for Lab Services. Onboarding ends upon the earlier of (a) completion of these activities or (b) forty-five (45) days after the Effective Date, unless otherwise stated in the Order Form.

Following onboarding, Subscribed Lab Services will continue for the term specified in the Order Form (the "Initial Term"). If no term is specified, the default Initial Term will be thirty-six (36) months. After the Initial Term, the Agreement for the applicable Subscribed Lab Services will automatically renew for successive terms equal to the Initial Term, subject to any price adjustments specified in the Order Form or Master Agreement (for example, an automatic increase in the monthly contract amount at renewal). Either party may decline renewal by providing written notice at least sixty (60) days before the end of the current term.

4.2 Termination for Cause. Either party may terminate this Agreement (or any Order Form) upon written notice if the other party: (a) becomes insolvent or subject to bankruptcy proceedings; (b) makes an assignment for the benefit of creditors; or (c) materially breaches this Agreement or an Order Form and fails to cure such breach within thirty (30) days after written notice describing the breach.

4.3 Termination for Convenience. Client may terminate Subscribed Lab Services for convenience upon written notice, subject to payment of any early termination or minimum commitment fees set forth in the Order Form or Master Agreement (for example, a percentage of remaining contract value).

4.4 Effect of Termination. Upon termination or expiration of Subscribed Lab Services, Secure Data will cooperate with Client in the orderly transition of stored equipment and open Lab Services work, including coordinating shipment or pickup of Client equipment. Client will pay Secure Data for all Lab Services performed up to the effective termination date and any agreed termination or transition assistance costs. Client will arrange for prompt removal of its equipment from Secure Data facilities; if Client fails to remove equipment within a commercially reasonable period, Secure Data may charge ongoing storage fees or dispose of equipment in accordance with applicable law and any disposal terms in the Order Form.

5. ADDING, REMOVING, AND MODIFYING LAB SERVICES. Secure Data will typically scope and bill Lab Services based on some combination of: (a) the number and type of devices processed (per-device or per-rack fees); (b) the amount of storage space or number of stored devices; and (c) any recurring retainers or minimum monthly commitments.

Client's environment, device counts, and storage utilization may be reviewed periodically (for example, quarterly) and billing adjusted prospectively to reflect actual usage, subject to any minimum commitment specified in the Order Form. No retroactive billing or credits will be applied unless explicitly set out in the Order Form.

6. MINIMUM COMMITMENT. If an Order Form specifies a minimum monthly commitment for Lab Services, Client agrees that Secure Data may invoice Client for at least that minimum monthly amount during the applicable term, even if actual usage would otherwise result in lower fees. Reductions in device counts or storage volumes will not reduce monthly charges below the specified minimum commitment.

7. STORAGE, RISK OF LOSS, AND INSURANCE. Client retains all right, title, and interest in its equipment at all times. Secure Data's possession of Client equipment is solely for the purpose of performing Lab Services and does not transfer ownership.

Unless otherwise agreed in the Master Agreement or Order Form: (a) risk of loss for equipment in transit to Secure Data passes to Secure Data only upon Secure Data's signed receipt; (b) risk of loss for equipment in transit from Secure Data to Client or another destination passes to Client when Secure Data tenders the equipment to the carrier; and (c) while equipment is stored at Secure Data facilities, Secure Data will exercise commercially reasonable care to protect equipment from theft, damage, or misuse but does not assume the role of insurer.

Secure Data's total liability for loss of or damage to equipment arising from Lab Services (excluding gross negligence or willful misconduct) will be limited to the lesser of (a) the replacement cost of the affected equipment or (b) the total fees paid by Client for the specific Lab Services relating to that equipment, subject to any broader limitations of liability in the Master Agreement.

Client is encouraged to maintain property insurance covering its equipment while in transit and while at Secure Data facilities.

8. SHIPPING AND LOGISTICS. Secure Data may arrange shipping using Client's designated carrier accounts or Secure Data's preferred carriers, as specified in the Order Form. Unless explicitly included as part of Lab Services, freight and shipping charges will be passed through to Client or billed as separate line items.

Secure Data is not responsible for delays, damage, or loss caused by third-party carriers, customs authorities, or other factors beyond Secure Data's reasonable control. Client is responsible for inspecting shipments upon receipt and promptly notifying Secure Data and the carrier of any visible damage or shortages.

9. OUT-OF-SCOPE SERVICES AND RATES. Any services requested by Client that are outside the Subscribed Lab Services described in this Agreement and the applicable Order Form will be treated as "Out-of-Scope Services" and may be billed on a time-and-materials basis at Secure Data's then-current service rates.

Examples of Out-of-Scope Services include: onsite installation, cutover, or remediation work at Client locations; emergency or after-hours work outside normal lab operating hours (unless explicitly included); and major redesigns or rework driven by changes in Client requirements after initial approval.

10. UPDATES TO THIS AGREEMENT. Secure Data may update or modify this Agreement from time to time. Any updates will be posted at Secure Data's standard terms URL and will include an updated "Last Updated" date. Continued use of Lab Services after the effective date of such updates will constitute acceptance of the updated terms, subject to any rights Client may have under the Master Agreement to continue under existing terms until the end of the current term.

11. ATTORNEY'S FEES. If Secure Data must take legal action to enforce this Agreement and prevails, Secure Data will be entitled to recover its reasonable attorneys' fees and costs from Client, to the extent permitted by applicable law and consistent with the Master Agreement.

12. DEFINITIONS. Capitalized terms used but not defined in this Agreement have the meaning given to them in the Master Agreement or applicable Order Form. Without limiting the foregoing:

- **"Build"** means a single device or rack that Secure Data prepares under Level 3 or Level 4 Lab Services in accordance with Client's approved standards.
- **"Equipment"** means any IT hardware (including laptops, desktops, servers, storage, networking, and security appliances) owned or controlled by Client and handled by Secure Data in connection with Lab Services.
- **"Lab Services"** means the services described in Section 1 of this Agreement and any related tasks identified in an Order Form.
- **"Normal Business Hours"** means Monday through Friday, 8:00 a.m. to 5:00 p.m., Central Time, excluding Secure Data holidays.
- **"Order Form"** means any statement of work, quote, proposal, or ordering document executed by Client that references this Agreement.
- **"Service Request"** means a request by Client for Lab Services that does not arise from a service failure or Incident.
- **"Subscribed Lab Services"** means the Lab Services identified in an Order Form as being purchased by Client.