Sayers Technology Holdings, Inc.
Sayers Technology Services, LLC
Sayers Technology, LLC

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to Meet the Trust Services Criteria for the Security, Availability, and Confidentiality Categories for the Period of August 1, 2024, through July 31, 2025.

Table of Contents

Assertion of Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC Management

Assertion of Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's personalized hardware and software services system (system) throughout the period August 1, 2024, to July 31, 2025, to provide reasonable assurance that Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in section A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period August 1, 2024, to July 31, 2025, to provide reasonable assurance that Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in section B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period August 1, 2024, to July 31, 2025, to provide reasonable assurance that Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's service commitments and system requirements were achieved based on the applicable trust services criteria.

Independent Service Auditor's Report

Independent Service Auditor's Report

Chris Callahan
President and CEO
Sayers Technology, LLC
960 Woodlands Parkway
Vernon Hills, IL 60061

Scope

We have examined Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's accompanying assertion titled "Assertion of Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC Management" (assertion) that the controls within Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's personalized hardware and software services system (system) were effective throughout the period August 1, 2024, to July 31, 2025, to provide reasonable assurance that Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's service commitments and system requirements were achieved. Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's personalized hardware and software services system were effective throughout the period August 1, 2024, to July 31, 2025, to provide reasonable assurance that Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

August 29, 2025

Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's Description of Its Personalized Hardware and Software Services System

Section A: Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's Description of the Boundaries of Its Personalized Hardware and Software Services System

Services Provided

Sayers Technology Holdings, Inc., Sayers Technology Services, LLC, and Sayers Technology, LLC (collectively "Sayers") is a managed services provider that offers three categories of service:

- NexGen Firewall Lifecycle Services: A continuous, four-phase firewall lifecycle management service. Customers and Sayers co-manage the firewalls, and customers can select from a menu of services to offload responsibilities to Sayers, including patching, upgrades, security reviews, and design services. Customers receive reports on best practice assessments, policy and rule reviews, and monthly and quarterly environment reviews.
- Azure Cloud Services: Sayers is a Microsoft Cloud Solutions Provider and resells Azure services to customers. The Cloud Architecture team conducts monthly check-in calls with customers.
- Staff Augmentation: Customers look to Sayers as a trusted technology partner, including staff augmentation services to fill critical roles on a stop-gap basis. An on-staff recruiting team finds qualified candidates, which are interviewed and assessed by engineers, for six-to-12-month contracts. These contracts are not project-based and define, in general, expected tasks. Candidates filling these roles may be employees or contractors and report to and are managed by the customer.
- Professional Services: Project-based professional services are offered; these projects are mainly driven by the three previous services.

Marketing and Sales

Sayers' internal Marketing team uses the Sayers website, social media, email campaigns, industry events, and word of mouth to advertise. Marketing efforts are coordinated through HubSpot. HubSpot is integrated into Salesforce; leads are tracked as opportunities. Leads are then routed to the appropriate representative based on who the account is assigned to.

Sales representatives contact leads hold high-level discussions about each lead's organization and the problem to be solved. Potential solutions are proposed to leads, and a member of the Services team assigns an engineer or other technical resource to participate in additional calls with the potential client in order to refine Sayers' understanding of the problem and propose a solution and implementation plan.

Information from calls is used to create a Green Light Document (GLD). GLDs are used to confirm the scope of the engagement, services to be provided, and a cost estimate. Approved GLDs are used to create formal Statements of Work (SOWs). SOWs are

created from a template but are bespoke for the proposed solution specific to the client. SOWs include an executive summary of the services to be provided followed by a high-level phased implementation plan, a staffing plan, customer responsibilities and prerequisites, and itemized costs. SOWs are sometimes accompanied by a Sayers Master Services Agreement (MSA) that identifies Sayers' commitment to performance, assumption of risk of damages or injuries from providing services, reputable personnel with clear background checks and 10-panel drug testing, non-disclosure of sensitive information, and information security controls. SOWs are presented by the sales representative and engineer to the client. SOWs, MSAs, and mutual non-disclosure agreements (mNDAs) are signed by clients using DocuSign upon the start of an engagement and are returned to Sayers.

Project Setup

Signed agreements are stored by the Services team in a shared network folder and are submitted to the Project Management team by completing a client intake form. The form's fields are completed by Services and are used to populate a spreadsheet in a Software-as-a-Service (SaaS) based project management platform and to generate an alert to the Project Management team of a new project to be assigned. Information transferred to Project Management includes the SOW, rates, and assigned resources. A Project Manager is assigned based on availability and creates documents in the project management platform from templates including the project plan, status template, project & client dashboard, and project finance sheet used to track invoicing as defined in the SOW. The project plan is populated based on the scope and phased steps identified in the SOW; project plans track: Tasks/Milestones, Notes, Start/End Dates, and Status by Phases including Planning, Prerequisite, and Implementation. Data in the project plan is used to populate two dashboards: Project and Client.

Client Dashboards are client-facing and provide project information (project manager, primary engineer, account executive); project status (project health, start & target end dates), and project plan (tasks/milestones, status, start date, notes, health, duration).

Kickoff and Implementation

The Project Manager creates a draft kickoff presentation that is reviewed during the internal kickoff meeting, held as a team prior to meeting with the client to review the external kickoff draft. The meeting is attended by the Sales Representative, Services Director, Project Manager, and Delivery Engineers. The external kickoff meeting occurs with the client, and topics discussed include the project scope, deliverables, timeline, prerequisites, how often status calls will occur (if there will be status calls), and if any working sessions will be scheduled. A folder is created in Sayers' secure file sharing platform and is shared with the client contact and internal staff assigned to the project; this folder is used to securely share files between the client and Sayers. These files may include network diagrams and configuration information. Credentials provided by clients are stored in the SaaS based privileged access manager (PAM). Access to client credentials is limited to engineers assigned to the client project.

Changes to SOWs are addressed through change orders. Clients use the Change Order form, included as an appendix to the SOW, to submit changes to their project manager. The Project Manager discusses submitted changes at the next internal check-in and

presents a formal change to the client to sign and approve. Changes are tracked in project plans and are reflected in project information tracked in project dashboards.

When client dashboards are created, the client's project sponsors are invited by Project Management via Sayers SaaS project management platform email notification to register themselves and configure multi-factor authentication (MFA) to access the client dashboard. Clients can use this dashboard for the duration of a project for updates on tasks or milestones and any that are awaiting action. Project managers meet internally with engineers weekly to review project plans and dashboards; the Project Manager reviews the client dashboard with the client during status meetings. Progress in the project plan is updated by the Project Manager as tasks are reported as complete until completion. Project health is tracked on dashboards to represent an overall score of project progress.

Project Completion

Closeout calls are held both internally and externally. Internal calls are used to review the success of the project, lessons learned, and opportunities for additional business. Optional external calls are held with clients to review the success of the project and a review of deliverables. Clients are presented with a Certificate of Completion to sign. Upon signature of the certificate or following five days with no response, the project is closed. Upon project completion, folders in the secure file sharing platform used for information transfer are marked for deletion and are automatically purged after 90 days.

Support

Sayers provides support for Cloud and Firewall Lifecycle Services customers. Cloud customers receive first-call support as required in the Microsoft Partner agreement to address basic issues that can be resolved without escalation to Microsoft support. Firewall Lifecycle Services customers are provided support for firewalls included in their service agreements. Sayers does not provide other support beyond what is identified in SOWs. Issues with service delivery are addressed during client check-in calls and are documented as part of the project.

Infrastructure

Sayers segregates its network with two wireless local area networks (WLANs), the Sayers Guest and Sayers Technology wireless networks. The Guest WLAN uses a captive portal to authenticate visitors, and the Sayers Technology WLAN uses enterprise security levels to authenticate users and devices. Both WLANs use 2.4GHz and 5GHz transmission rates with ARP filtering to prevent gateway spoofing attacks. The Technology WLAN's Service Set Identifier (SSID) is tied to the corporate Entra ID instance, while the Sayers Guest WLAN is set to the captive portal.

A network diagram demonstrates the wide area network (WAN) environment and the virtual private network (VPN) connectivity between the organization's physical locations and Azure.

Software

The organization maintains a software inventory that lists the software used to provides its services, as well as the approved applications for end users. The software inventory includes a description, application version, vendor, distributor, and other relevant information.

People

Sayers is overseen by an independent board of directors comprised of one independent member serving as the chairman, two Sayers representatives, and two members representing outside investors. The board meets in person on a quarterly basis to discuss company strategy, operations, and financials.

The organization maintains a traditional hierarchical structure with defined leadership, departments, and reporting lines. Direct reports to the Chief Executive Officer (CEO) and President include the Chief Digital and Marketing Officer, the VP of IT, the COO, the Senior VP of Solutions, the Senior VP of Client Services, the Senior VP of Human Resources (HR), and the Chief Sales Officer. A Senior Leadership team is composed of the CEO and President as well as all Vice President (VP) roles within the organization, and the following departments are maintained:

- Pre-sales and Sales Architects
- Services
- Marketing
- Sales
- Human Resources
- Operations, Legal, and Project Management
- IT
- People

Data

Sayers maintains procedures for managing data securely. Data used to provide its services to clients is classified into the following categories: public, operational, and confidential. Guidance for the storage, transmission, consumption, and destruction of data in each category is provided within a Data Classification & Confidential Data Policy. Sayers also retains data as needed to conduct business and maintain compliance with applicable laws and regulations. Data is only retained when it is necessary to effectively conduct business activities, fulfill the organization's mission, and comply with regulatory requirements.

Data is protected both at rest and in transit using appropriate cryptographic algorithms. All servers and end-user computing devices are encrypted. For data in transit, site to site virtual private networks (VPNs) are established through the next generation firewalls at each site. Sayers uses a hub-and-spoke model, where every office is a spoke that connects to the Azure hub. Sayers offices can only communicate with Azure; they are not configured to pass traffic directly to another site or via Azure. Laptops use the VPN client that encrypts traffic via a symmetric AES-256 bit key. Logon sessions to Entra ID, firewall consoles, network switch consoles, and SaaS based security tools are secured with HTTPS or Transport Layer Security (TLS) 1.2.

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices

Section B: Principal Service Commitments and System Requirements

Regulatory Commitments

The organization complies with financial regulatory requirements; data is only retained when it is necessary to effectively conduct business activities, fulfill the mission, and comply with applicable laws and regulations including but not limited to:

- Providing an ongoing service or project
- Compliance with laws and regulations associated with financial and programmatic reporting by Sayers to funding agencies
- Security incidents and investigations
- Intellectual property preservation
- Litigation

Sayers undergoes both financial audits and annual SOC 2 audits.

Contractual Commitments

Sayers executes contractual agreements with its customers that outline its commitments related to the scope of work, security, confidentiality, availability, and other relevant service agreements. SOWs, MSAs, and non-disclosure agreements (NDAs) are maintained with customers depending on the services contracted for with Sayers.

System Design

Sayers designs its personalized hardware and software services system to meet its regulatory and contractual commitments. These commitments are based on the services that Sayers provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that Sayers has established for its services. Sayers establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in Sayers' system policies and procedures, system design documentation, and contracts with clients.