SEBONE TECHNOLOGIES
• COMPASSION • CREATIVITY • RELIABILITY

CONFIDENTIAL

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations™

SYSTEM AND ORGANIZATION CONTROLS

SOC 2® Type II

Report on the suitability of the design and operating effectiveness of controls relevant to *Security*.

Sebone System

Sebone Technologies Private Limited

SECURITY

REPORT PERIOD

April 1, 2026 – June 30, 2026

INDEPENDENT SERVICE AUDITOR

Accorp Partners CPA LLC

Contents

01

SECTION 01

Assertion of Sebone Technologies Management

Management's written assertion regarding the description of the Sebone System and the suitability of the design and operating effectiveness of its controls throughout the period.

Assertion of Sebone Technologies Management

We have prepared the accompanying description of the Sebone System (the "description") throughout the period April 1, 2026 to June 30, 2026, based on the criteria for a description of a service organization's system set forth in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, Description Criteria) (the "description criteria").

The description is intended to provide report users with information about the Sebone System that may be useful when assessing the risks arising from interactions with Sebone Technologies Private Limited's ("Sebone," "the Company") system, particularly information about system controls that Sebone has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (the "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).

Sebone uses Microsoft as a subservice organization to provide the cloud productivity, identity, endpoint-management, and email-security infrastructure on which the Sebone System operates. The description presents Sebone's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Sebone's controls. It does not disclose the actual controls at the subservice organization. The description also identifies certain complementary user entity controls that are necessary, in combination with Sebone's controls, to provide reasonable assurance that Sebone's service commitments and system requirements are achieved.

Assertion

We confirm, to the best of our knowledge and belief, that:

1. **Presentation of the description.** The description presents the Sebone System that was designed, implemented, and operated throughout the period April 1, 2026 to June 30, 2026 in accordance with the description criteria.
2. **Suitability of design.** The controls stated in the description were suitably designed throughout the period to provide reasonable assurance that Sebone's service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively and the subservice organization and user entities applied the complementary controls assumed in the design of Sebone's controls.
3. **Operating effectiveness.** The controls stated in the description operated effectively throughout the period to provide reasonable assurance that Sebone's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and user entity controls assumed in the design of Sebone's controls operated effectively throughout the period.

Ravi Vyas

Director & Chief Executive Officer, Sebone Technologies Private Limited

JULY 8, 2026

02

SECTION 02

Independent Service Auditor's Report

The independent service auditor's opinion on the fairness of the description and the suitability of the design and operating effectiveness of controls throughout the period.

To: The Management of Sebone Technologies Private Limited

Scope

We have examined Sebone Technologies Private Limited's ("Sebone's") accompanying description of the Sebone System throughout the period April 1, 2026 to June 30, 2026 (the "description"), based on the description criteria set forth in DC section 200, and the suitability of the design and operating effectiveness of the controls stated in the description throughout that period to provide reasonable assurance that Sebone's service commitments and system requirements were achieved based on the trust services criteria relevant to security (the applicable trust services criteria) set forth in TSP section 100.

Sebone uses Microsoft as a subservice organization to provide the cloud productivity, identity, endpoint-management, and email-security infrastructure supporting the Sebone System. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with the controls at Sebone, to achieve Sebone's service commitments and system requirements. The description presents Sebone's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Sebone's controls. It does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description also indicates that certain complementary user entity controls are necessary, in combination with Sebone's controls, to achieve Sebone's service commitments and system requirements. Our examination did not extend to such complementary user entity controls, and we have not evaluated their suitability of design or operating effectiveness.

Service Organization's Responsibilities

Sebone is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that its service commitments and system requirements were achieved. Sebone is also responsible for preparing the description and its assertion, including the completeness, accuracy, and method of presentation of the description and assertion. Sebone is further responsible for providing the services covered by the description, selecting the applicable trust services criteria and stating the related controls in the description, and identifying the risks that threaten the achievement of its service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of the controls stated in the description based on our examination. 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, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively throughout the period. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves performing procedures to obtain evidence about the presentation of the description, the suitability of the design, and the operating effectiveness of those controls. Our procedures included assessing the risks that the description is not presented in accordance with the description criteria and that the controls were not suitably designed or operating effectively. Our examination also included evaluating the overall presentation of the description. We did not perform procedures regarding the operating effectiveness of controls that are the responsibility of the subservice organization or user entities.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that each individual user may consider important. 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 commitments and system requirements were achieved. Also, the projection to the future of any conclusions about the suitability of the design or operating 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.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in Section 4 of this report, titled “Trust Services Criteria, Sebone’s Control Activities, Tests of Operating Effectiveness, and Results of Tests.” Our tests of operating effectiveness were designed to cover the period April 1, 2026 to June 30, 2026 and, depending on the nature of the control, included inquiry of appropriate personnel, inspection of relevant documentation and system configurations, and observation of the operation of the control.

Opinion

Opinion

In our opinion, in all material respects, throughout the period April 1, 2026 to June 30, 2026:

1. the description presents the Sebone System that was designed and implemented in accordance with the description criteria.
2. the controls stated in the description were suitably designed to provide reasonable assurance that Sebone's service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively and the subservice organization and user entities applied the complementary controls assumed in the design of Sebone's controls.
3. the controls stated in the description operated effectively to provide reasonable assurance that Sebone's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and user entity controls assumed in the design of Sebone's controls operated effectively throughout the period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Sebone, user entities of the Sebone System during some or all of the period April 1, 2026 to June 30, 2026, business partners of Sebone subject to risks arising from interactions with the Sebone System, and prospective user entities, independent auditors, and practitioners who have sufficient knowledge and understanding of the matters described. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Accorp Partners CPA LLC

Independent Service Auditor, License No. PAC-FIRM-LIC-47383

JULY 8, 2026

03

SECTION 03

Sebone's Description of the Sebone System

A description of the boundaries of the Sebone System and the controls designed and implemented to meet the applicable trust services criteria for Security throughout the period April 1, 2026 to June 30, 2026.

Overview of the Company and Services Provided

Sebone Technologies Private Limited ("Sebone" or "the Company") is an information-technology services company headquartered at Mahadevapura, Bengaluru, Karnataka, India. The Company provides IT consulting, custom software development, staff augmentation, and recruitment and managed-staffing services to enterprise clients in India and internationally, and maintains an information security management system certified to ISO/IEC 27001:2022.

Sebone delivers its services principally through skilled people — engineers, consultants, and recruitment specialists — supported by a corporate information environment built on Microsoft cloud services. The Company's principal service lines are summarized below.

- **Staff augmentation (Smart Team).** Skilled engineers and consultants are deployed to work within client teams and, frequently, within client-owned systems and environments, extending the client's delivery capacity under the client's direction.
- **IT consulting & custom software development.** Advisory, engineering, and delivery services across cloud, data and analytics, AI/ML, and digital transformation, delivered from Sebone-managed devices.
- **Recruitment & managed staffing.** End-to-end sourcing, screening, and placement of candidates for client organizations, including contract and managed-staffing arrangements, handling candidate personal data.
- **Management consulting.** Functional and technical consulting engagements aligned to client business objectives.

The Sebone System — the system that is the subject of this report — comprises the Company's corporate information environment and the people and processes through which these services are delivered and through which client, candidate, and personnel information is handled. The environment is built on Microsoft 365 and related Microsoft cloud services (Microsoft Entra ID, Microsoft Intune, Microsoft Defender for Business, and Microsoft Purview). The Company operates no self-managed production data-center infrastructure.

Sebone operates under a shared-responsibility model. Sebone is responsible for its corporate systems, the secure configuration and operation of its Microsoft 365 environment, the security of its managed endpoints, and the conduct and access of its personnel. Client (user) entities are responsible for administering their own systems and for provisioning, reviewing, and revoking the access they grant to deployed Sebone personnel, as described under Complementary User Entity Controls. Microsoft, as the subservice organization, is responsible for the physical and environmental security and the underlying infrastructure of the cloud services it provides.

Principal Service Commitments and System Requirements

Sebone designs and operates the Sebone System to meet the service commitments it makes to its clients and the system requirements established by management. These commitments are derived from client service agreements and statements of work, the Company's published service-level commitments, its information security policies, and applicable laws and regulations, including the Digital Personal Data Protection Act, 2023.

Security Commitments

Sebone commits to protecting client, candidate, and personnel information against unauthorized access and disclosure through the confidentiality obligations accepted by every employee and contractor, role-based and least-privilege access enforced through Microsoft Entra ID with multi-factor authentication, encryption of information in transit using TLS and at rest through BitLocker device encryption and the platform encryption of Microsoft 365, centrally managed and threat-protected endpoints, the logging and monitoring of security-relevant events, and the management of security incidents under a documented incident-management process, including client notification where required. The Company further commits to removing access promptly upon a personnel departure or an engagement roll-off, to retaining information in accordance with its Data Retention and Disposal Policy, and to sustaining the delivery of services through its business-continuity and backup arrangements.

System Requirements

System requirements are the specifications by which Sebone meets these commitments and complies with applicable laws and regulations. They include the identification and classification of information assets, role-based and least-privilege logical access, and the protection of information through encryption. They further include centralized endpoint management and threat protection, logging and monitoring, vulnerability, incident, and change management, and backup, business-continuity, and disaster-recovery planning. These requirements are documented and enforced through the Company's policy suite (31 information security policies), its Microsoft 365 configuration, and its operational procedures, and are described further under Components of the System below.

Components of the System

The Sebone System is bounded by the infrastructure, software, people, processes, and data that support the delivery of Sebone's in-scope services and the handling of client, candidate, and personnel information. Each component is described below.

Infrastructure

Sebone operates the Sebone System on Microsoft cloud services and maintains no on-premises or self-managed production infrastructure. Corporate identity, productivity, collaboration, endpoint management, email security, and information governance are delivered through Microsoft 365, Microsoft Entra ID, Microsoft Intune, Microsoft Defender for Business, and Microsoft Purview, and personnel operate Intune-managed Windows endpoints. The principal infrastructure components are summarized below.

SERVICE / COMPONENT	PROVIDER	BUSINESS FUNCTION AND SECURITY RELEVANCE
Microsoft 365 (Exchange Online, SharePoint, OneDrive, Teams)	Microsoft	Corporate email, document storage, and collaboration. Holds corporate, client-project, candidate, and personnel information, protected by external-sharing restrictions, email-threat policies, and Microsoft Purview retention.
Microsoft Entra ID	Microsoft	Corporate identity and access management for all personnel — authentication, Conditional Access, multi-factor authentication, password protection and smart lockout, and directory audit and sign-in logging.
Microsoft Intune	Microsoft	Endpoint and application management — device-compliance policies (BitLocker, Secure Boot, TPM, firewall, antivirus, minimum OS build, and password rules) and app-protection (MAM) policies for permitted personally-owned devices.
Microsoft Defender for Business	Microsoft	Endpoint detection and response in block mode with tamper protection, and Exchange Online anti-phishing and anti-malware policies protecting corporate email.
Microsoft Purview	Microsoft	Information-retention labelling and disposition and unified audit logging across the Microsoft 365 tenant.
Intune-managed Windows endpoints	Sebone / Microsoft	Corporate laptops used by personnel to deliver services, enrolled in Intune and evaluated against device-compliance and encryption policy.
Paybooks	Paybooks	Payroll and HR processing — handles employee payroll, bank, and personal data, managed as a critical vendor under the Company's third-party controls.
Recruitment tooling (Naukri, LinkedIn)	Info Edge / LinkedIn	Candidate sourcing for the recruitment and managed-staffing practice, handling candidate personal data.

SERVICE / COMPONENT	PROVIDER	BUSINESS FUNCTION AND SECURITY RELEVANCE
Trustflow GRC	Trustflow	Governance, risk, and compliance platform used to maintain the policy suite and control evidence.

> **IMPORTANT**
>
> Microsoft is presented as a subservice organization using the carve-out method. The controls expected to be implemented by Microsoft are described under Complementary Subservice Organization Controls and are not included within the boundaries of the Sebone System.

Network and Boundary Protection

The Sebone System is delivered through managed, internet-facing Microsoft cloud services rather than a self-managed corporate network. Its principal boundary controls are:

- **Identity boundary.** Access to Microsoft 365 is mediated by Microsoft Entra ID with Conditional Access and multi-factor authentication (via the Microsoft Authenticator application). Corporate sign-ins are captured in the Entra ID sign-in logs, and account lockout (smart lockout) and password protection are configured.
- **Device boundary.** Access is intended to originate from Intune-managed, compliance-evaluated endpoints. BitLocker disk encryption, firewall, antivirus, Secure Boot, and TPM are required by device-compliance policy, with non-compliant devices marked immediately.
- **Collaboration boundary.** External sharing in SharePoint and OneDrive defaults to “only people in your organization,” and Microsoft Teams external access is restricted to block all external domains.
- **Email boundary.** Exchange Online is protected by Microsoft Defender for Business anti-phishing and anti-malware policies operating in the tenant.
- **Administrative boundary.** Administrative roles in Microsoft Entra ID and Microsoft 365 are restricted to authorized personnel and are subject to quarterly access review.

Exhibit 1: Sebone System architecture — the Microsoft 365 corporate environment (Microsoft Entra ID, Intune, Defender for Business, and Purview) and the Intune-managed endpoints and personnel who deliver services into client-owned environments, with Microsoft as the carved-out subservice organization (Source: Sebone).

Software

The software component comprises the Microsoft 365 services and the operational and security tooling used to operate, secure, and monitor the environment. The principal software and tooling are summarized below.

SOFTWARE AND TOOLING

MICROSOFT 365 (EXCHANGE, SHAREPOINT, ONEDRIVE, TEAMS)	Email, document management, and collaboration for corporate and client-delivery work, and the primary store of corporate, project, candidate, and personnel information.
MICROSOFT ENTRA ID	Identity and access management — authentication, Conditional Access, multi-factor authentication, password protection, and audit and sign-in logging.
MICROSOFT INTUNE	Endpoint and application management — device-compliance and app-protection policies enforcing encryption and configuration baselines.
MICROSOFT DEFENDER FOR BUSINESS	Endpoint detection and response, tamper protection, and Exchange Online anti-phishing and anti-malware policies.
MICROSOFT PURVIEW	Retention labelling and disposition, and unified audit logging across the tenant.
TRUSTFLOW GRC	Maintenance of the policy suite and control evidence for the information security management system.
PAYBOOKS	Payroll and HR processing for personnel, managed as a critical third party.

People

Sebone operated with a workforce of approximately 57 employees and contractors during the period, the majority of whom are engineers and consultants deployed to client engagements, together with recruitment, delivery, human-resources, finance, and information-security personnel. The Company is led by the Director and Chief Executive Officer, who holds ultimate accountability for strategy, operations, and security posture. Information-security and IT responsibilities are assigned to a designated Information Security Lead and IT/Systems Lead. The security-relevant roles are summarized below.

ROLE	SECURITY-RELEVANT RESPONSIBILITIES
Director & Chief Executive Officer	Holds ultimate accountability for the Company, provides governance and oversight of the information security program, approves the policy suite and the risk assessment, and is the designated approver for the acceptance of residual risk.
Information Security Lead	Owns the information security management system, the risk assessment and risk register, incident coordination, and business-continuity coordination, and advises management on security and privacy matters.
IT / Systems Lead	Administers the Microsoft 365, Entra ID, Intune, and Defender environment, and performs user provisioning and deprovisioning, access reviews, patch and vulnerability management, and configuration change management.
HR & Delivery Management	Performs onboarding (background verification, confidentiality agreements, and training) and offboarding, and coordinates the deployment and roll-off of engineers on client engagements, including the removal of access.
Client Partnership	Manages client relationships and engagement scope and communicates the Company's security and confidentiality commitments to clients.
Delivery Engineers & Consultants	Deliver services from managed devices, including within client environments, and are responsible for adhering to security policy and to least-privilege access to client systems.
Talent Acquisition	Source, screen, and place candidates and handle candidate personal data in accordance with the Company's data-protection controls.

All employees and contractors are subject to the Company's human-resources security controls. Background verification is performed for personnel, and every employee and contractor accepts confidentiality and acceptable-use obligations before access is granted. New personnel receive least-privilege access, complete security-awareness training, and acknowledge the Company's policies. Access is reviewed quarterly and is removed promptly upon departure or upon roll-off from a client engagement.

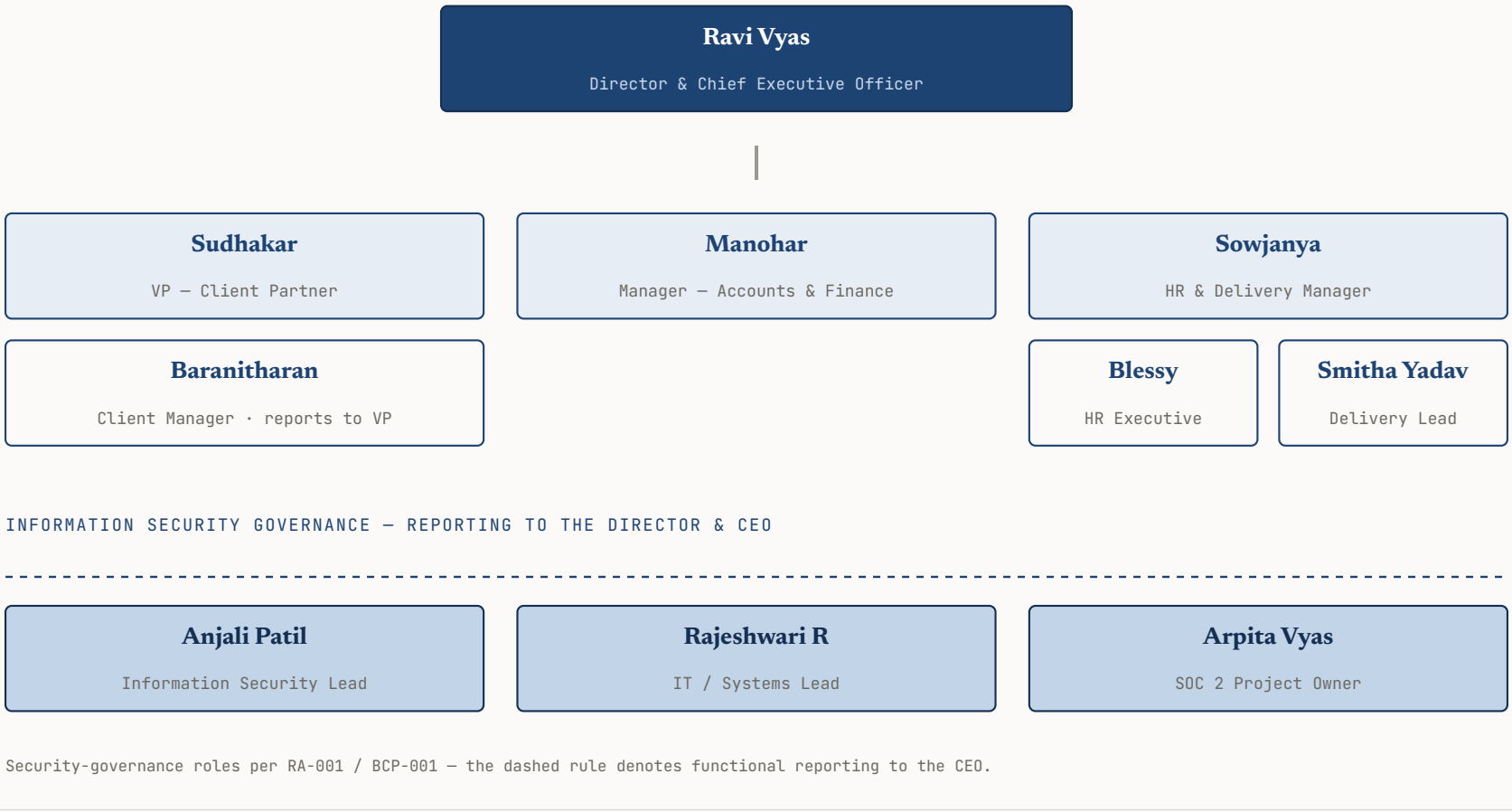

Exhibit 2: Sebone organizational structure — the Director & CEO over the client-partnership, finance, and HR & delivery functions, with the information-security governance roles (Information Security Lead, IT/Systems Lead, and SOC 2 Project Owner) reporting to the CEO (Source: Sebone organizational chart — security roles per RA-001 / BCP-001).

Processes and Procedures

Sebone's operation of the Sebone System is governed by a documented information security management system comprising a suite of 31 security policies (POL-001 to POL-031) approved by management, together with the operational registers through which the controls are executed and evidenced. The principal processes are described below.

Information Security Program and Policy Framework

Sebone maintains a documented information security program, certified to ISO/IEC 27001:2022, within which the controls for the Sebone System are defined, implemented, and maintained. The policy suite is versioned, approved by management, and made available to personnel, and personnel acknowledge the policies at onboarding. The framework is summarized by domain below.

INFORMATION SECURITY PROGRAM — POLICY DOMAINS

GOVERNANCE & PROGRAM	Information Security Policy, Continual Improvement Policy, and Risk Management Policy, within the ISO/IEC 27001:2022 management system.
HUMAN-RESOURCES SECURITY	Employee Screening Policy, Acceptable Use Policy, Information Security Awareness and Training Policy, and Disciplinary Policy.
ACCESS CONTROL & CRYPTOGRAPHY	Access Control Policy, Cryptographic Control and Encryption Policy, and Cryptographic Key Management Policy.
ASSET & INFORMATION MANAGEMENT	Asset Management Policy, Information Classification and Handling Policy, Data Retention and Disposal Policy, Data Protection and Privacy Policy, Information Transfer Policy, and Intellectual Property Rights Policy.
OPERATIONS & CHANGE	Change Management Policy, Secure Development Policy, Patch Management Policy, Logging and Monitoring Policy, Network Security Management Policy, and Cloud Security Policy.
THREAT & ENDPOINT	Malware and Anti-Malware Policy, Mobile and Teleworking Policy, and Clear Desk and Clear Screen Policy.
INCIDENT & CONTINUITY	Incident Management Policy, Significant Incident and Evidence Handling Policy, Backup and Recovery Policy, Business Continuity Policy, and Physical and Environmental Security Policy.

THIRD-PARTY Third Party and Supplier Security Policy.

Risk Assessment and Risk Management

Sebone manages information security risk in accordance with its Risk Management Policy and a documented risk assessment (RA-001). Risks to the confidentiality, integrity, and availability of client and corporate information within the SOC 2 boundary are identified and scored on a five-point likelihood-and-impact scale (inherent risk = likelihood × impact, 1–25), and each risk is assigned a treatment option — reduce, transfer, avoid, or accept — and a named owner. The current assessment records fifteen risks (R-01 to R-15), spanning unauthorized access to the Microsoft 365 environment, phishing and social engineering, exposure of client data within client systems, access not removed on exit or roll-off, malware and ransomware, critical-vendor failure, and regulatory (DPDP) non-compliance. The assessment explicitly considers fraud, insider misuse, and unauthorized access. It is owned by the Information Security Lead and approved by the Director, and is reviewed at least annually or upon material change. Residual High risks require documented Director approval.

Access Control and Identity Management

Logical access to the Sebone System is governed by the Access Control Policy on a role-based, least-privilege basis. Authentication to Microsoft 365 is provided by Microsoft Entra ID, with multi-factor authentication delivered through the Microsoft Authenticator application and enforced through Conditional Access. Account protection is reinforced by smart lockout (a lockout threshold of ten failed attempts and a sixty-second lockout duration) and Entra ID password protection. Access is requested and approved before provisioning, is granted on a least-privilege basis, and is reviewed quarterly through the Access Review Register. Administrative roles are restricted to authorized personnel. Access is removed promptly upon a personnel departure and, for deployed engineers, upon roll-off from a client engagement, with the offboarding process disabling the Entra ID account and coordinating the removal of, or notification to remove, access to client systems.

Change Management

Changes to the Microsoft 365, Entra ID, and Intune configuration are governed by the Change Management Policy and recorded in the Change Management Register. Standard changes are reviewed and approved before deployment, tested where applicable, and recorded with a rollback approach, while emergency changes are approved retrospectively within a defined window. The register captures the change, its type and environment, the requester and approver, testing, deployment, and status.

Vulnerability and Patch Management

Sebone identifies vulnerabilities through Microsoft Defender Vulnerability Management and Microsoft Secure Score and records them in the Vulnerability Management Register, tracking

each finding from discovery through remediation against severity-based timelines defined in the Patch Management Policy. Operating-system and application patches are deployed to managed endpoints through Microsoft Intune and Windows Update for Business.

Endpoint and Malware Protection

Corporate endpoints are enrolled in Microsoft Intune and evaluated against a device-compliance policy that requires BitLocker disk encryption, Secure Boot, a Trusted Platform Module, the Windows firewall, antivirus, a minimum operating-system build, and password controls (a minimum length of eight, expiry, and history), with non-compliant devices marked immediately. Microsoft Defender for Business provides endpoint detection and response operating in block mode with tamper protection, and an application-protection (MAM) policy governs permitted personally-owned devices. Exchange Online anti-phishing and anti-malware policies protect corporate email.

Security Monitoring and Incident Management

Security-relevant events are captured in the Microsoft Entra ID audit and sign-in logs and in Microsoft Purview unified audit logging, and Microsoft Defender for Business generates and surfaces security alerts. Findings and alerts are reviewed and, where material, escalated to management. Security events are managed under the Incident Management Policy and the Significant Incident and Evidence Handling Policy, which define identification, reporting, containment, escalation, root-cause analysis, and client notification where required, and incidents are recorded in the Incident Log.

Backup, Business Continuity, and Disaster Recovery

Corporate and client-related information resides primarily in Microsoft 365 and is retained and recoverable under the Data Retention and Disposal Policy and Microsoft Purview retention. Backup and recovery responsibilities are defined in the Backup and Recovery Policy, and continuity is governed by the Business Continuity Policy and the Business Continuity Plan (BCP-001), whose recovery objectives are derived from a Business Impact Analysis. The principal recovery objectives are summarized below.

BUSINESS FUNCTION	PRIORITY	RTO	RPO
Identity & access (Entra ID SSO + MFA)	Critical	≤ 4 hours	2 hours
Microsoft 365 environment (email / collaboration)	High	≤ 8 hours	4 hours
Client delivery — deployed engineers	High	≤ 8 hours	Depends on client systems
Payroll processing (Paybooks)	High (month-end)	≤ 1 business day	24 hours
Endpoint management (Intune / Defender)	Medium	≤ 1 business day	8 hours

Where engineers work within client environments, the backup and recovery of client-owned data is the responsibility of the client. Continuity arrangements are validated through a business-continuity tabletop exercise conducted at least annually.

Vendor and Third-Party Risk Management

Sebone manages its vendors and sub-processors under the Third Party and Supplier Security Policy. Vendors are inventoried and risk-rated in the Vendor Register according to the data they handle and their criticality, and assurance — such as a SOC 2 report or security questionnaire — is obtained and reviewed for critical vendors on at least an annual basis. Microsoft, as the subservice organization, is a High-criticality vendor whose SOC 2 reporting is reviewed. Other vendors include Paybooks (payroll), Naukri and LinkedIn (recruitment), the Company's banking provider, and Trustflow GRC.

Data

The Sebone System processes, transmits, and stores the following principal categories of information, each subject to the access, encryption, classification, and handling controls described in this report.

DATA CATEGORY	PRIMARY STORE	DESCRIPTION
Client & project data	Client-owned systems · Microsoft 365	Information handled by deployed engineers in the course of client engagements. Data held within client-owned systems is administered by the client. Project correspondence and documents held by Sebone reside in Microsoft 365.
Candidate & recruitment data	Microsoft 365 / recruitment tooling	Candidate personal data (resumes and contact details) processed by the recruitment and managed-staffing practice, retained under the recruitment retention labels.
Personnel & HR data	SharePoint (HR) / Paybooks	Employee records, onboarding and offboarding records, and payroll, bank, and personal data, access-restricted to HR, finance, and payroll roles.
Corporate & business data	Microsoft 365	Corporate email, contracts, and business documents, retained under Microsoft Purview retention labels.
Audit & system logs	Microsoft Entra ID / Purview	Directory audit and sign-in logs and unified audit logs of tenant activity, access-restricted to administrators.

Classification. Information is classified under the Information Classification and Handling Policy as Public, Internal, or Confidential. Client, candidate, and personnel data is treated as Confidential and is subject to the full scope of the Company's access, encryption, and handling controls.

Encryption. Data in transit is protected using TLS, data at rest on managed endpoints is protected using BitLocker, and data held in Microsoft 365 is protected by the platform's encryption.

Retention and disposal. Retention and disposal are governed by the Data Retention and Disposal Policy and enforced through Microsoft Purview retention labels — for example, HR records for seven years, financial records for eight years, employment and client contracts for ten years, project records for five years, recruitment data for three years, and SOC 2 audit evidence for seven years — with Microsoft 365 audit logs retained for one year.

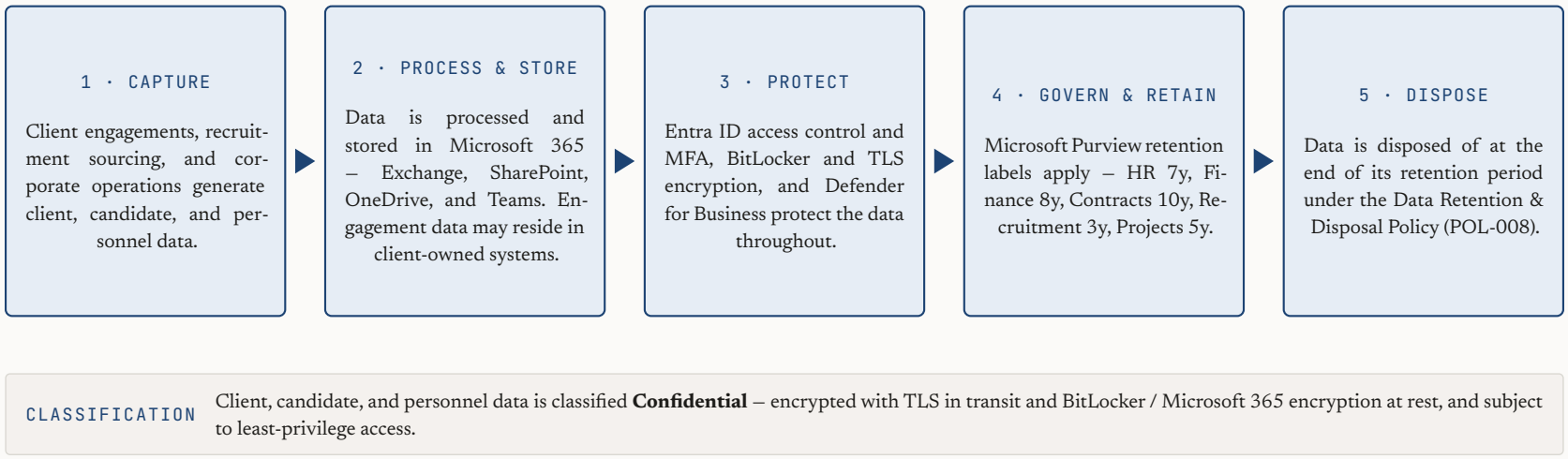

Exhibit 3: Data flow across the Sebone System – from capture through processing and storage in Microsoft 365 (and, for deployed engagements, within client-owned systems), through the access, encryption, and threat-protection controls, to retention and disposition under Microsoft Purview (Source: Sebone).

Boundaries of the System

The in-scope Sebone System is the Company's corporate Microsoft 365 environment (Exchange Online, SharePoint, OneDrive, Teams, Entra ID, Intune, Defender for Business, and Purview), the Intune-managed endpoints, and the people and processes that operate, secure, and monitor it and that deliver Sebone's IT-services, staff-augmentation, and recruitment services. Explicitly excluded from the boundaries of the in-scope system are the client-owned systems and environments into which Sebone personnel are deployed (which are administered by the client), Microsoft's underlying cloud infrastructure (addressed through the carve-out method), and the Company's public marketing website. The Availability, Confidentiality, Processing Integrity, and Privacy trust services categories were not selected by management and are outside the scope of this report.

Disclosures About Identified Security Incidents

There were no identified security incidents during the period April 1, 2026 to June 30, 2026 that were the result of controls that were not suitably designed or operating effectively and that (a) were significant to the achievement of Sebone's service commitments and system requirements, or (b) required notification to affected user entities under the terms of client agreements or applicable law.

Complementary User Entity Controls

Sebone's controls were designed with the assumption that certain controls would be implemented by user entities (clients). The following complementary user entity controls are necessary, in combination with Sebone's controls, to provide reasonable assurance that the applicable trust services criteria are achieved.

REF	CONTROL EXPECTED TO BE IMPLEMENTED
CUEC-1	User entities are responsible for provisioning, reviewing, and de-provisioning the access they grant to deployed Sebone personnel within the client's own systems, consistent with least privilege.
CUEC-2	User entities are responsible for promptly notifying Sebone, and for revoking access within their own systems, when a Sebone engineer rolls off an engagement or a change in personnel occurs.
CUEC-3	User entities are responsible for the security configuration of their own systems and networks into which Sebone personnel are deployed, including authentication, encryption, logging, and monitoring.
CUEC-4	User entities are responsible for promptly notifying Sebone of any actual or suspected security incident affecting their engagement or the systems accessed by Sebone personnel.
CUEC-5	User entities are responsible for defining the confidentiality, data-protection, and security obligations applicable to each engagement in the governing client agreement or statement of work.

Complementary Subservice Organization Controls

Sebone uses Microsoft as a subservice organization under the carve-out method. The controls below are the types of controls Sebone expects Microsoft to maintain. Sebone reviews Microsoft's SOC 2 report (or equivalent) at least annually. The physical and environmental security of the Company's office premises is provided by its managed-workspace facility provider.

SUBSERVICE ORGANIZATION	SERVICES PROVIDED	COMPLEMENTARY CONTROLS EXPECTED
Microsoft	Microsoft 365, Microsoft Entra ID, Microsoft Intune, Microsoft Defender for Business, and Microsoft Purview	Physical and environmental security of data-center facilities. Security, availability, and redundancy of the cloud infrastructure. Logical tenant isolation. Encryption of data at rest and in transit. Security of the identity service. Platform patching and vulnerability management. Microsoft maintains SOC 2 Type II and ISO 27001 attestations.
Managed-workspace facility provider	Physical office premises (Bengaluru)	Physical access control to the premises, environmental controls and power, and physical security of the workspace from which personnel operate.

Significant Changes During the Period

This is Sebone's initial SOC 2 examination, conducted as a Type II examination covering the period April 1, 2026 to June 30, 2026. During the period, Sebone formalized and operationalized its information security management system in support of the examination — including adopting its suite of 31 security policies, completing its information security risk assessment and risk register (RA-001), establishing its Business Continuity Plan (BCP-001) and Business Impact Analysis, and establishing its operational registers (access review, change, incident, vulnerability, vendor, and training). Sebone also maintained its ISO/IEC 27001:2022 certification and completed its review of the subservice organization's assurance reporting. Other than these enhancements to the control environment, there were no changes during the period that are likely to have significantly affected the Sebone System or the Company's ability to meet its service commitments and system requirements.

Applicable Trust Services Criteria Not Relevant to the System

The applicable trust services criteria for this examination are those relevant to Security (the common criteria). The categories of Availability, Confidentiality, Processing Integrity, and Privacy were not selected by management and are outside the scope of this examination and the boundaries of the in-scope system. Within the Security category, all of the applicable trust services criteria are relevant to the Sebone System. The specific criteria and the controls designed to meet them are presented in Section 4.

04

SECTION 04

Trust Services Criteria, Control Activities, Tests of Operating Effectiveness, and Results of Tests

The applicable trust services criteria for Security, the controls Sebone designed to meet them, the service auditor's tests of operating effectiveness, and the results of those tests, throughout the period April 1, 2026 to June 30, 2026.

The controls listed below were designed and operated by Sebone to meet the applicable trust services criteria for Security. For each control, the service auditor performed the tests described, which — depending on the nature of the control — included inquiry of appropriate personnel, inspection of policies, records, and system configurations, and observation of the operation of the control, throughout the period April 1, 2026 to June 30, 2026.

CRITERIA	CONTROL DESCRIPTION	SERVICE AUDITOR'S TEST PROCEDURES	RESULTS OF TESTS
CC1 | Control Environment			COMMON CRITERIA
CC1.1 *Integrity and Ethical Values*	Sebone maintains a Code of Conduct and Ethics Policy, an Anti-Bribery and Anti-Corruption Policy, a Whistleblower Policy, and an Acceptable Use Policy (POL-027) that set expectations for ethical behavior, conflicts of interest, and the acceptable use of Company assets. Confidentiality and acceptable-use obligations are accepted by all employees and contractors as a condition of engagement, and the Director is accountable for enforcement and escalation of violations.	1. Inspected the Code of Conduct and Ethics Policy, the Anti-Bribery and Anti-Corruption Policy, the Whistleblower Policy, and the Acceptable Use Policy (POL-027) to confirm existence, scope, and applicability to all personnel. 2. Inspected a sample of employment offer letters to confirm that confidentiality and acceptable-use obligations are accepted as a condition of engagement. 3. Inquired of management regarding the communication and enforcement of ethical requirements and the escalation of violations.	**No exceptions noted**
CC1.2 *Management Oversight*	The Director and Chief Executive Officer exercises oversight of the information security program, approves the Company's suite of 31 security policies and its information security risk assessment (RA-001), and is the designated approver for the acceptance of residual risk. The Company's ISO/IEC 27001:2022 management system provides for periodic management review.	1. Inspected the Information Security Policy (POL-001) and Risk Management Policy (POL-004) to confirm that governance and management-oversight responsibilities are defined and assigned to the Director. 2. Inspected the information security risk assessment (RA-001) to confirm that the Director is designated as the approver of the assessment and of residual-risk acceptance. 3. Inspected the ISO/IEC 27001:2022 certificate and inquired of management regarding oversight of the information security program during the period.	**No exceptions noted**
CC1.3 *Organizational Structure*	Sebone maintains a defined organizational structure with documented reporting lines, led by the Director & CEO. Security-relevant roles — including the Information Security Lead, the IT/Systems Lead, and HR & Delivery — are assigned to named individuals in the Company's risk assessment (RA-001), Business Continuity Plan (BCP-001), and policies.	1. Inspected the organizational chart to confirm defined reporting lines. 2. Inspected the risk assessment (RA-001) and Business Continuity Plan (BCP-001) to confirm that security-relevant roles and responsibilities are assigned to named individuals. 3. Inquired of management regarding role assignments for personnel with security responsibilities.	**No exceptions noted**

CRITERIA	CONTROL DESCRIPTION	SERVICE AUDITOR'S TEST PROCEDURES	RESULTS OF TESTS
CC1.4 *Commitment to Competence*	The Employee Screening Policy (POL-003) requires background verification of personnel prior to the granting of access, and the Information Security Awareness and Training Policy (POL-031) requires security-awareness training for personnel, tracked in the Training Register. Personnel are assigned responsibilities based on role and competence.	1. Inspected the Employee Screening Policy (POL-003) and the Information Security Awareness and Training Policy (POL-031). 2. Inspected a sample of background-verification records for personnel to confirm that screening was performed prior to the granting of access. 3. Inspected the security-awareness training materials and the Training Register used to record completion.	**No exceptions noted**
CC1.5 *Accountability*	Individual accountability for compliance with security policies is established in the Acceptable Use Policy (POL-027) and Disciplinary Policy (POL-029), with violations subject to disciplinary action. Microsoft Entra ID audit and sign-in logs attribute activity to named individual accounts, and account lockout (smart lockout) is configured with a lockout threshold of ten failed attempts and a sixty-second lockout duration.	1. Inspected the Acceptable Use Policy (POL-027) and Disciplinary Policy (POL-029) for provisions establishing individual accountability and disciplinary consequences. 2. Inspected the Microsoft Entra ID audit and sign-in logs to confirm that activity is attributed to named individual accounts. 3. Inspected the Entra ID password-protection configuration to confirm that smart-lockout settings (a lockout threshold of ten and a sixty-second duration) are enabled.	**No exceptions noted**
CC2 | Communication and Information			COMMON CRITERIA
CC2.1 *Quality Information*	Sebone maintains a policy suite, operational registers, and Microsoft 365 audit logging to support the operation of internal control. Microsoft Entra ID audit and sign-in logs and Microsoft Purview unified audit logging provide security-relevant operational information.	1. Inspected the Microsoft Entra ID audit and sign-in logs and the Microsoft Purview unified audit logging to confirm that security-relevant events are captured. 2. Inspected entries recorded during the period in the Company's operational registers (access review, change, incident, and vulnerability) evidencing the operation of controls. 3. Inquired of management regarding the use of logging and registers to support control operation.	**No exceptions noted**
CC2.2 *Internal Communication*	Security policies, objectives, and responsibilities are communicated to personnel through the Company's suite of 31 policies, the Employee Handbook, onboarding, and security-awareness training. Personnel are expected to acknowledge the Company's policies.	1. Inspected the security policy suite (POL-001 to POL-031) to confirm that security policies and personnel responsibilities are documented. 2. Inspected the Employee Handbook and security-awareness training materials used to communicate security expectations.	**No exceptions noted**

CRITERIA	CONTROL DESCRIPTION	SERVICE AUDITOR'S TEST PROCEDURES	RESULTS OF TESTS
		3. Inquired of management regarding the distribution and acknowledgement of policies by personnel.	
CC2.3 *External Communication*	Security and confidentiality commitments to clients are documented in service agreements and service-level documentation. The Incident Management Policy (POL-020) provides for the notification of clients where a security incident affects their engagement.	1. Inspected the Company's service-level agreement and service-commitment documentation to confirm confidentiality and security-commitment provisions. 2. Inspected the Incident Management Policy (POL-020) for client-notification provisions. 3. Inquired of management regarding channels for external security communication with clients.	**No exceptions noted**
CC3 | Risk Assessment			COMMON CRITERIA
CC3.1 *Objective Specification*	Sebone's service commitments and system requirements are documented in client agreements and service-level documentation and are reflected in the Company's security policies and this system description. The applicable trust services criteria define the security objectives against which risks are assessed.	1. Inspected the Company's service-level agreement and service-commitment documentation to confirm that security commitments are defined. 2. Inspected the Information Security Policy (POL-001) to confirm that commitments are reflected in policy and this description.	**No exceptions noted**
CC3.2 *Risk Identification and Analysis*	The Risk Management Policy (POL-004) defines a formal process for identifying and analyzing information security risks. The risk assessment (RA-001) records fifteen risks (R-01 to R-15), each scored on a five-point likelihood-and-impact scale, assigned a treatment option and a named owner, and reviewed at least annually and upon material change.	1. Inspected the Risk Management Policy (POL-004) to confirm a formal methodology covering identification, likelihood-and-impact scoring, ownership, and treatment. 2. Inspected the risk assessment and risk register (RA-001) to confirm that the fifteen recorded risks were identified, rated, and assigned owners and treatment options. 3. Inquired of management regarding the performance and approval of the risk assessment during the period.	**No exceptions noted**
CC3.3 *Fraud Consideration*	The Company's risk assessment (RA-001) explicitly considers fraud, insider misuse, and unauthorized access to client and corporate data — including the exposure of client data within client systems and access not removed on roll-off. Controls including least-privilege access, multi-factor authentication, logging, confidentiality agreements, and the Disciplinary Policy are designed to address these risks.	1. Inspected the risk register (RA-001) to confirm that insider misuse, unauthorized access, and fraud scenarios are considered. 2. Inspected the access-management and logging control configurations designed to mitigate these risks.	**No exceptions noted**

CRITERIA	CONTROL DESCRIPTION	SERVICE AUDITOR'S TEST PROCEDURES	RESULTS OF TESTS
CC3.4 *Change Assessment*	Significant changes to the Sebone System are assessed for security implications through the change-management and risk-assessment processes and are reviewed and approved before implementation, in accordance with the Change Management Policy (POL-024) and Secure Development Policy (POL-016).	1. Inspected the Change Management Policy (POL-024) and Secure Development Policy (POL-016) for provisions requiring assessment of significant changes. 2. Inspected the Change Management Register for records of configuration changes reviewed and approved during the period. 3. Inquired of management regarding the assessment of significant changes.	**No exceptions noted**
CC4 | Monitoring Activities			COMMON CRITERIA
CC4.1 *Ongoing Evaluations*	Sebone performs ongoing monitoring through Microsoft Entra ID audit and sign-in logging, Microsoft Defender for Business, Microsoft Secure Score and vulnerability tracking, and quarterly access reviews recorded in the Access Review Register. The subservice organization's assurance reporting is reviewed at least annually.	1. Inspected the Microsoft Entra ID logging and Microsoft Defender for Business configuration to confirm that monitoring is enabled. 2. Inspected findings tracked in the Vulnerability Management Register during the period, and completed quarterly access review records in the Access Review Register. 3. Inquired of management regarding the annual review of the subservice organization's assurance reporting.	**No exceptions noted**
CC4.2 *Deficiency Communication*	Control deficiencies, vulnerability findings, and security incidents are documented and communicated to the IT/Systems Lead and management, tracked in the Company's registers, and escalated to the Director where material, in accordance with the Continual Improvement Policy (POL-002).	1. Inspected the Vulnerability Management Register and Incident Log to confirm that findings identified during the period were recorded and tracked. 2. Inspected the Continual Improvement Policy (POL-002) for provisions on evaluating and communicating deficiencies. 3. Inquired of management regarding the escalation of material findings to the Director.	**No exceptions noted**
CC5 | Control Activities			COMMON CRITERIA
CC5.1 *Risk Mitigation Controls*	The Company's suite of 31 policies defines specific control activities for each key risk domain, implemented through a combination of technical controls in Microsoft 365 (Entra ID, Intune, and Defender) and procedural controls defined in policy.	1. Inspected the security policy suite to confirm that control activities are defined for key risk domains. 2. Inspected the technical control configurations in Microsoft 365 – Entra ID authentication, Intune device compliance, and Defender for Business – to confirm they are consistent with policy.	**No exceptions noted**

CRITERIA	CONTROL DESCRIPTION	SERVICE AUDITOR'S TEST PROCEDURES	RESULTS OF TESTS
CC5.2 *Technology Controls*	Technology controls deployed for the Sebone System include Microsoft Entra ID authentication with multi-factor authentication and Conditional Access, and a Microsoft Intune device-compliance policy requiring BitLocker encryption, Secure Boot, a Trusted Platform Module, the Windows firewall, antivirus, a minimum operating-system build, and password rules. They further include Microsoft Defender for Business endpoint detection and response in block mode, restricted external sharing in SharePoint, restricted external access in Teams, and Exchange Online email-threat policies.	1. Inspected the Microsoft Intune device-compliance policy to confirm the required baselines (BitLocker, Secure Boot, TPM, firewall, antivirus, minimum OS build, and password requirements). 2. Inspected the Microsoft Defender for Business configuration (endpoint detection and response in block mode, and tamper protection). 3. Inspected the SharePoint external-sharing restriction and the Microsoft Teams external-access restriction. 4. Inspected the Microsoft Entra ID Conditional Access policy requiring a compliant device (State: On) and the Microsoft Intune device inventory confirming enrolled Windows endpoints in a compliant state.	**No exceptions noted**
CC5.3 *Policy Deployment*	Sebone has deployed a formal suite of 31 policies defining control expectations for all key security domains. Policies are approved by management, versioned, reviewed at least annually, and made available to personnel, and policy acknowledgement is required as part of onboarding.	1. Inspected the complete policy suite (POL-001 to POL-031) to confirm that policies exist for all key control domains and are versioned and dated. 2. Inspected the policies to confirm management approval and effective dates. 3. Inquired of management regarding the acknowledgement of policies by personnel.	**No exceptions noted**
CC6 | Logical and Physical Access Controls			COMMON CRITERIA
CC6.1 *Logical Access Architecture*	Access to the Sebone System is provisioned on a role-based, least-privilege basis. Authentication to Microsoft 365 is managed through Microsoft Entra ID, with multi-factor authentication delivered through the Microsoft Authenticator application and enforced through Conditional Access, supported by smart lockout (a threshold of ten failed attempts and a sixty-second duration) and Entra ID password protection. Administrative roles are restricted to authorized personnel.	1. Inspected the Access Control Policy (POL-028) to confirm role-based, least-privilege access requirements. 2. Inspected the Microsoft Entra ID sign-in logs evidencing multi-factor authentication (via the Microsoft Authenticator application) for personnel sign-ins, and the Conditional Access and password-protection (smart-lockout) configuration establishing authentication requirements. 3. Inspected the Microsoft Entra ID Global Administrator role assignments to confirm that administrative access is restricted to the authorized administrator.	**No exceptions noted**
CC6.2	New access is requested and approved before provisioning, applying least-privilege	1. Inspected the Access Control Policy (POL-028) and Employee Screening	**No exceptions noted**

CRITERIA	CONTROL DESCRIPTION	SERVICE AUDITOR'S TEST PROCEDURES	RESULTS OF TESTS
Access Provisioning	defaults, and identities are created in Microsoft Entra ID. An application-protection (MAM) policy is applied to permitted personally-owned (BYOD) devices.	Policy (POL-003) for provisioning and prior-approval requirements. 2. Inspected the Microsoft Intune app-protection (MAM) policy applied to permitted BYOD devices. 3. Inquired of management regarding, and inspected the access and change registers evidencing, the provisioning of access during the period.	
CC6.3 *Access Modification and Removal*	Access is reviewed quarterly through the Access Review Register and removed promptly upon departure or engagement roll-off. The offboarding process disables the Microsoft Entra ID account and coordinates the removal of, or notification to remove, access to client systems.	1. Inspected the Access Control Policy (POL-028) and the HR onboarding/offboarding requirements for timely access removal on departure and engagement roll-off. 2. Inspected completed quarterly access reviews recorded in the Access Review Register during the period. 3. Inquired of management regarding the deprovisioning of personnel and the removal of client access on roll-off during the period.	**No exceptions noted**
CC6.4 *Physical Access*	Sebone operates no data-center infrastructure. Physical security of the Company's office premises is provided by its managed-workspace facility provider, and the physical and environmental security of the production cloud infrastructure is the responsibility of the subservice organization under the carve-out method, in accordance with the Physical and Environmental Security Policy (POL-025).	1. Inspected the Physical and Environmental Security Policy (POL-025). 2. Inquired of management regarding physical access controls at the office premises provided by the facility provider. 3. Confirmed, through the system description, that production-infrastructure physical security is the responsibility of the subservice organization.	**No exceptions noted**
CC6.5 *Asset and Data Disposal*	The Asset Management Policy (POL-006) and the Data Retention and Disposal Policy (POL-008) govern the secure handling and disposal of assets and information. Microsoft Purview retention labels enforce retention and disposition, and the data of departing personnel is handled in accordance with policy.	1. Inspected the Asset Management Policy (POL-006) and the Data Retention and Disposal Policy (POL-008). 2. Inspected the Microsoft Purview retention-label configuration enforcing the retention and disposition of information.	**No exceptions noted**
CC6.6 *Boundary Protection*	External access to the environment is restricted through Microsoft Entra ID Conditional Access, restricted external sharing in SharePoint and OneDrive (defaulting to "only people in your organization"), restricted external access in Microsoft Teams (blocking all external domains), and Exchange Online email-threat	1. Inspected the SharePoint external-sharing restriction and the Microsoft Teams external-access restriction (blocking external domains). 2. Inspected the Exchange Online anti-phishing and anti-malware policies.	**No exceptions noted**

CRITERIA	CONTROL DESCRIPTION	SERVICE AUDITOR'S TEST PROCEDURES	RESULTS OF TESTS
	policies, in accordance with the Network Security Management Policy (POL-014) and Cloud Security Policy (POL-015).	3. Inspected the Network Security Management Policy (POL-014) and Cloud Security Policy (POL-015).	
CC6.7 *Encryption in Transit and at Rest*	Data in transit is protected using TLS. Data at rest on managed endpoints is protected using BitLocker disk encryption enforced through Microsoft Intune, and data held in Microsoft 365 is protected by the platform's encryption. Cryptographic controls are governed by the Cryptographic Control and Encryption Policy (POL-012) and the Cryptographic Key Management Policy (POL-013).	1. Inspected the Cryptographic Control and Encryption Policy (POL-012) and the Cryptographic Key Management Policy (POL-013). 2. Inspected the Microsoft Intune device-compliance policy requiring BitLocker disk encryption. 3. Inspected the Information Security Controls Statement confirming the use of TLS/HTTPS in transit and encryption at rest.	**No exceptions noted**
CC6.8 *Malware and Endpoint Protection*	Corporate endpoints are protected by Microsoft Defender for Business endpoint detection and response operating in block mode with tamper protection. Microsoft Intune requires antivirus on managed devices, and an Exchange Online anti-malware policy protects corporate email, in accordance with the Malware and Anti-Malware Policy (POL-017) and Patch Management Policy (POL-019).	1. Inspected the Microsoft Defender for Business configuration (endpoint detection and response in block mode, and tamper protection). 2. Inspected the Microsoft Intune device-compliance policy requiring antivirus, and the Exchange Online anti-malware policy. 3. Inspected the Malware and Anti-Malware Policy (POL-017) and Patch Management Policy (POL-019).	**No exceptions noted**
CC7 | System Operations			COMMON CRITERIA
CC7.1 *Vulnerability and Configuration Management*	System vulnerabilities are identified through Microsoft Defender Vulnerability Management and Microsoft Secure Score and tracked to resolution in the Vulnerability Management Register against severity-based timelines. Patches are deployed to managed endpoints through Microsoft Intune and Windows Update for Business.	1. Inspected the Logging and Monitoring Policy (POL-018) and Patch Management Policy (POL-019). 2. Inspected the Vulnerability Management Register used to track Microsoft Defender and Secure Score findings from discovery to resolution. 3. Inspected the Microsoft Entra ID audit logging confirming the capture of operational events.	**No exceptions noted**
CC7.2 *Security Event Monitoring*	Security-relevant events are monitored through Microsoft Entra ID audit and sign-in logs and Microsoft Defender for Business alerting, in accordance with the Logging and Monitoring Policy (POL-018).	1. Inspected the Microsoft Entra ID sign-in and audit logs to confirm the capture of security-relevant events. 2. Inspected the Microsoft Defender for Business alerting configuration. 3. Inquired of management regarding the periodic review of security alerts.	**No exceptions noted**
CC7.3	Security events are evaluated and escalated in accordance with the Incident Management Policy (POL-020) and the Significant	1. Inspected the Incident Management Policy (POL-020) and Significant Incident and Evidence Handling Policy	**No exceptions noted**

CRITERIA	CONTROL DESCRIPTION	SERVICE AUDITOR'S TEST PROCEDURES	RESULTS OF TESTS
Security Event Evaluation	Incident and Evidence Handling Policy (POL-021), which define severity classification (P1 to P4) and escalation.	(POL-021) for evaluation and escalation procedures. 2. Inspected the Incident Log maintained during the period for the recording and classification of security events. 3. Inquired of management regarding the evaluation of security events during the period.	
CC7.4 *Incident Response*	Security incidents are managed under the Incident Management Policy (POL-020), which defines identification, reporting, containment, escalation, root-cause analysis, and client notification where required. Incidents are recorded in the Incident Log.	1. Inspected the Incident Management Policy (POL-020) for the defined incident-response lifecycle. 2. Inspected the Incident Log maintained for the period. 3. Inquired of management regarding security incidents during the period.	**No exceptions noted**
CC7.5 *Recovery*	Recovery of the environment is supported by the Backup and Recovery Policy (POL-022) and the Business Continuity Plan (BCP-001). Corporate and client-related information in Microsoft 365 is retained and recoverable through Microsoft Purview retention, and recovery objectives (RTO and RPO) are defined in the Business Impact Analysis.	1. Inspected the Backup and Recovery Policy (POL-022) and the Business Continuity Plan (BCP-001). 2. Inspected the Business Impact Analysis defining recovery-time and recovery-point objectives. 3. Inquired of management regarding backup and recovery arrangements through Microsoft 365 and Microsoft Purview.	**No exceptions noted**
CC8 | Change Management			COMMON CRITERIA
CC8.1 *Change Authorization and Testing*	Changes to the Microsoft 365, Entra ID, and Intune configuration are recorded, reviewed, and approved before deployment, with emergency changes approved retrospectively within a defined window, in accordance with the Change Management Policy (POL-024). Changes are recorded in the Change Management Register with the change, its type and environment, the requester and approver, testing, and rollback approach.	1. Inspected the Change Management Policy (POL-024) and Secure Development Policy (POL-016) for authorization, testing, and approval requirements. 2. Inspected the Change Management Register for configuration changes recorded, approved, and deployed during the period. 3. Inquired of management regarding the change-management process, including the handling of emergency changes.	**No exceptions noted**
CC9 | Risk Mitigation			COMMON CRITERIA
CC9.1 *Business Disruption Risk*	Sebone identifies and mitigates business-disruption risk through the Business Continuity Policy (POL-023), the Business Continuity Plan (BCP-001), and the Business Impact Analysis, which define critical functions, recovery strategies, and recovery	1. Inspected the Business Continuity Policy (POL-023) and the Business Continuity Plan (BCP-001). 2. Inspected the Business Impact Analysis identifying critical business functions	**No exceptions noted**

CRITERIA	CONTROL DESCRIPTION	SERVICE AUDITOR'S TEST PROCEDURES	RESULTS OF TESTS
	objectives and are reviewed at least annually and validated through a tabletop exercise.	and their recovery-time and recovery-point objectives. 3. Inquired of management regarding the testing of business-continuity arrangements.	
CC9.2 *Vendor and Third-Party Risk*	Third parties are inventoried and risk-assessed in the Vendor Register under the Third Party and Supplier Security Policy (POL-005). Assurance (such as SOC 2 reporting) is obtained and reviewed for critical vendors — including Microsoft, Paybooks, and the Company's banking provider — and the removal of access on client roll-off is addressed through the offboarding process.	1. Inspected the Third Party and Supplier Security Policy (POL-005). 2. Inspected the Vendor Register identifying vendors, the data they handle, criticality, and assurance status. 3. Inquired of management regarding the review of the subservice organization's SOC 2 report.	**No exceptions noted**

END OF REPORT

Sebone System

SOC 2 Type II · Security

Report on the suitability of the design and operating effectiveness of controls relevant to Security throughout the period

April 1, 2026 – June 30, 2026