Neurotek Ltd.’s

SOC 2 Type 1 Report on the description of the MOXO platform and on the Suitability of the Design Effectiveness of controls relevant to Security, Availability, Confidentiality, Processing Integrity Trust Service Criteria as of May 08, 2026.

Statement of Confidentiality

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of the Service Organization, User Entities of the Service Organization's system related to the MOXO platform relevant to Security, Availability, Confidentiality, Processing Integrity as of May 08, 2026, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties. Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

1. Independent Service Auditors' Report

Independent Service Auditors' Report on Description of Neurotek Ltd.'s System and the Suitability of the Design and Operating Effectiveness of Controls relevant to Security, Availability, Confidentiality, Processing Integrity trust service criteria.

To the Management of Neurotek Ltd.

Scope

We have examined Neurotek's accompanying description of its MOXO platform system found in Neurotek's MOXO platform system titled Neurotek's Description of the MOXO platform as of May 08, 2026 (description) based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022), in AICPA, Description Criteria, (description criteria) and the suitability of the design of controls stated in the description as of May 08, 2026, to provide reasonable assurance that Neurotek's service commitments and system requirements would be achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, Processing Integrity (applicable trust services criteria) set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022), in AICPA, Trust Services Criteria.

Neurotek uses a subservice organization to provide cloud and hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Neurotek, to achieve Neurotek's service commitments and system requirements based on the applicable trust services criteria. The description presents Neurotek's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Neurotek's controls. The description 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.

Service Organization's Responsibilities

Neurotek 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 Neurotek's service commitments and system requirements would be achieved. In Section 2, Neurotek has provided the accompanying assertion titled Management Assertion Provided By Service Organization (assertion) about the description and the suitability of design of controls stated therein. Neurotek is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; 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 the service organization's service commitments and system requirements.

The Description also indicates that Neurotek's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Neurotek's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls

stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. 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 to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion. We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

An examination of a description of a service organization's system and the suitability of the design of controls involves:

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the description.

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

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 individual users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects:

a. the description presents Neurotek's MOXO platform system that was designed and implemented as of May 08, 2026 in accordance with the description criteria.

b. the controls stated in the description were suitably designed as of May 08, 2026 to provide reasonable assurance that Neurotek's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organization applied the complementary controls assumed in the design of Neurotek's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Neurotek; user entities of Neurotek's MOXO platform system as of May 08, 2026 ; business partners of Neurotek subject to risks arising from interactions with the MOXO platform system; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Accorp Partners CPA LLC

Accorp Partners CPA LLC
PAC-FIRM-LIC-47383
Kalispell, Montana
May 18, 2026

SECTION 2

MANAGEMENT ASSERTION PROVIDED BY SERVICE ORGANIZATION

Assertion of the Management of Neurotek Ltd.

We have prepared the accompanying description of Neurotek's MOXO platform system titled Neurotek's Description of the MOXO platform as of May 08, 2026 (description) based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022) , in AICPA, Description Criteria (description criteria). The description is intended to provide report users with information about the MOXO platform system that may be useful when assessing the risks arising from interactions with Neurotek's system, particularly information about system controls that Neurotek 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, Availability, Confidentiality, Processing Integrity and Privacy (applicable trust services criteria) set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity and Privacy (With Revised Points of Focus—2022) , in AICPA, Trust Services Criteria.

Neurotek uses a Amazon Web Services (AWS) for hosting and cloud services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Neurotek, to achieve Neurotek's service commitments and system requirements based on the applicable trust services criteria. The description presents Neurotek's, controls the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Neurotek's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Neurotek, to achieve Neurotek's service commitments and system requirements based on the applicable trust services criteria. The description presents the service organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

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

1. The description presents Neurotek's MOXO platform system that was designed and implemented as of May 08, 2026 in accordance with the description criteria.

2. The controls stated in the description were suitably designed as of May 08, 2026 to provide reasonable assurance that Neurotek's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Neurotek's controls throughout that period.

For Neurotek Ltd.

Name: **Dr. Yaki Dayan**
Title: **CEO**
Date: **May 18, 2026**

80 Kokhav Ha-Yam St
Hofit, Israel
+972-8-6466107
info@neurotek.ai

SECTION 3

NEUROTEK'S DESCRIPTION OF THE MOXO PLATFORM

3. System Description Provided by Service Organization

3.1 Overview of the Company and Services Delivered by the Report

Neurotek Ltd. (hereinafter "Neurotek" or "the Organization") is headquartered at 80 Kohav HaYam St., Hofit, Israel. Neurotek develops and delivers innovative neuropsychological evaluation solutions aimed at unlocking the potential of every individual. The Organization employs 11 full-time employees and one contractor (CFO), operating from a single physical office of approximately 120 square meters. Neurotek has pursued ISO certification and is now pursuing SOC 2 Type 2 certification to formally demonstrate its commitment to security, availability, confidentiality, processing integrity, and privacy.

The core offering covered by this SOC 2 examination is the MOXO neuropsychological assessment platform. MOXO provides accurate diagnostic support and a scientifically validated assessment of human attention and executive functions. Key characteristics of the MOXO system include:

- Delivery Model: MOXO is delivered as a web-based Software-as-a-Service (SaaS) platform. No hardware installation or dedicated software installation is required. It operates via standard web browsers.
- Licensing & Payments: The MOXO software license is enforced at account registration. MOXO accounts require mandatory acceptance of the Software License, Terms of Use and Privacy statement. Clients purchase test packs directly within the application using credit card transactions.
- Target Clientele: Clinics, health service providers, educational institutions, and mental health or emotional well-being centers.
- Functionality: The platform administers standardized attention-profiling assessments, processes response data, generates diagnostic reports, and presents results to licensed practitioners via a secure online dashboard

3.1 Components of the System used to provide services

Infrastructure & Network Architecture

Hosting & Physical Environment

The MOXO production environment is hosted on Amazon Web Services (AWS), providing cloud-based compute, storage, and networking capabilities. Physical security of data center facilities (visitor logging, card access, CCTV, environmental controls) is the responsibility of AWS under their respective shared responsibility models.
Neurotek's corporate office is located at 80 Kohav HaYam St., Hofit, Israel. The office is a single-unit, ground-floor, 120 sqm physical space. Physical access controls at the office include locked doors and an alarm system whenever the office is unattended.There are no servers or digital storage / hard drives at the location. Employees's laptop computers are not stored at this physical location.

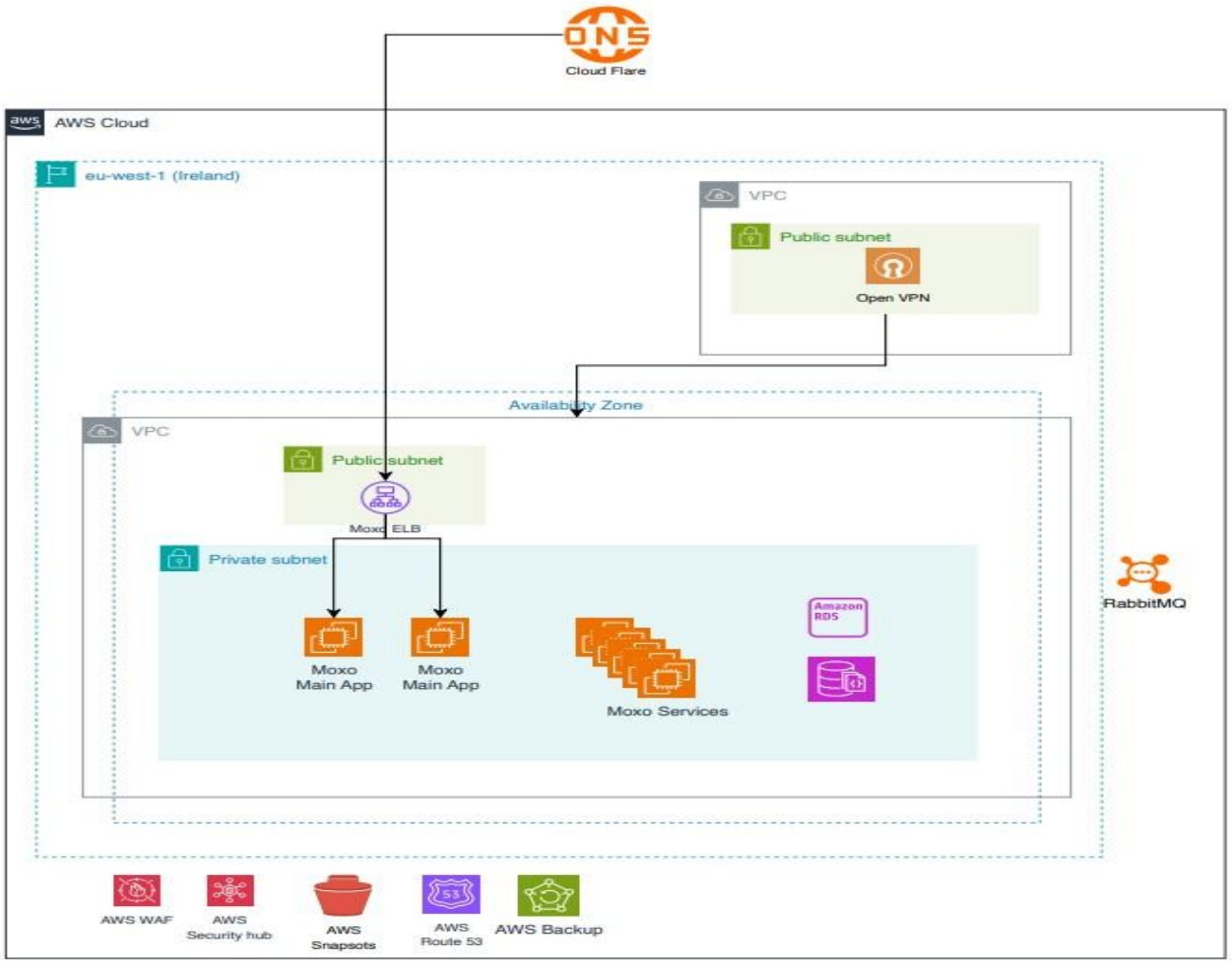
Network Architecture

The cloud production environment is accessible exclusively via VPN. Direct access to servers or databases is not possible without an active VPN connection. Cloudflare is used for CDN, DNS management, and DDoS mitigation. A high-level cloud architecture diagram has been prepared and is appended to this document.

Redundancy & Failover

AWS infrastructure provides redundancy and failover capabilities. Load balancing and multi- zone deployment practices are in place to maintain service continuity. Full architecture details are documented in the attached network diagram.

Network Diagram:



Software

- **Operating Systems & Key Tools**
  - MOXO is a web application developed entirely in-house by Neurotek's CTO/R&D team. No desktop, iOS, or Android native apps are in scope. The application handles the submission, processing, and reporting of neuropsychological assessments.
- **Internally Developed Software**
  - Source code is maintained in BitBucket. Code review, QA, and testing processes are managed internally prior to production deployment.
  - Jenkins is used for continuous integration and deployment pipelines. Sentry provides real-time error monitoring and alerting.
- **Monitoring & Logging**
  - Zabbix is used for infrastructure and system monitoring. CloudAMQP supports asynchronous messaging services. Monitoring alerts are reviewed by the R&D/DevOps team.
  - We use security information & event management (SIEM) to aggregate logs from key systems, generating alerts for anomalous behavior.

- Real-time and periodic scans for vulnerabilities are performed on application and infrastructure layers.

People

Organizational Structure

Neurotek's organizational structure is as follows:

- CEO: Strategic leadership and executive oversight of security and compliance commitments.
- CTO / R&D (including DBA and QA): Manages technical infrastructure, software development, database administration, and quality assurance. Primary accountable role for system security and availability.
- COO / CRO: Oversees operational processes and customer relationship management.
- Product Management: Drives product roadmap and coordinates between development and commercial teams.
- Sales (including Pre-sales and Training): Manages client onboarding, training, and commercial relationships.
- Marketing: Manages external communications and product promotion.
- Admin / Finance (Office Manager, CFO – contractor): Manages administrative and financial operations.
- Hiring & Training

All employees receive onboarding covering data protection policies and security expectations. Security awareness training is conducted on an ongoing basis.

Procedures

1. **Access Management**

   Access to production systems requires VPN authentication. Role-based access principles are applied. Privileged access is restricted to authorized personnel. Onboarding and offboarding procedures govern provisioning and deprovisioning of access rights.

2. **Change Management**

   Software changes follow a documented development, testing, QA review, and deployment process managed through GitHub and Jenkins. Changes are tested prior to production release. BrowserStack supports cross-browser testing. Postman is used for API testing.

3. **Incident Response**

   An incident management process is in place governing detection, escalation, and resolution of security and availability events. Zendesk is used as the customer support platform. Significant incidents are escalated to senior management and communicated to affected clients as required.

4. **Backup & Recovery**

   Data backups are performed on a Daily - nightly basis within the cloud environment. Restore procedures are periodically tested. Recovery time and recovery point objectives are defined in the business continuity documentation.

5. **Vendor Management**

   Third-party vendors are evaluated prior to onboarding. Annual review of vendor SOC 2 or

equivalent attestations is performed for critical vendors. A formal vendor list is maintained (see Section 4).

Data

Data Types & Classification

MOXO processes neuropsychological assessment data which may constitute Personally Identifiable Information (PII) and/or sensitive health-related data. Data categories include assessment inputs, response data, diagnostic results, and client (practitioner) account information.

Data Lifecycle

- Collection: Data is submitted by licensed practitioners via the MOXO web application.
- Storage: All data is stored in an encrypted cloud-based database. Both database-level and field- level encryption are applied, ensuring that users with direct database access cannot view sensitive information in cleartext.
- Transmission: Data in transit is encrypted using TLS. VPN is required for all administrative access.
- Retention & Deletion: Data retention periods are aligned with regulatory and contractual requirements. Secure deletion processes are applied when data reaches end-of-life.

Personal data storage is confirmed to be cloud-based. Employees are not permitted to download or store company or client data on personal devices or removable media. The organization does not issue or use external storage media. Encryption of local storage is enforced where personal computers are used under the hybrid work policy.

Subservice Organizations And Complementary Subservice Organization Controls

Neurotek may rely on certain third-party vendors or subservice organizations (SSOs) to provide critical components of our overall service. Examples may include AWS hosting providers, payment processors, identity verification services, or data analytics platforms. Their activities and controls can significantly impact our ability to meet the Trust Services Criteria in scope.

Carve-Out vs. Inclusive Method

Neurotek uses the carve-out method for all subservice organizations. Their individual controls are excluded from the scope of this SOC 2 report. Neurotek's control design assumes that subservice organizations have implemented the Complementary Subservice Organization Controls (CSOCs) described below. Neurotek reviews available attestation reports (SOC 2, ISO 27001, PCI-DSS) from critical vendors on an annual basis.

3.2 Relevant aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

The applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Although the applicable trust services criteria and related controls are included in Section IV, they are an integral part of Neurotek’s description of the system. This section provides information about the five interrelated components of internal control at Neurotek, including:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring controls

3.3 Control Environment

Tone at the Top and Ethical Values

Neurotek's senior leadership sets the tone for ethical conduct and security responsibility across the organization. Information security expectations are communicated to all staff at onboarding and reinforced through ongoing training and management communication.

Organizational Structure and Assignment of Authority

Clear reporting lines are defined across the organization (see Section 3.3). The CTO/R&D function bears primary accountability for technical security controls. The CEO provides executive oversight.

Segregation of duties is applied where feasible given organizational size, particularly between development, QA, and production release activities.

Competence and Human Resource Practices

Background checks are performed on new employees. Role-specific training is provided. Security awareness training is conducted on an ongoing basis. Employee performance expectations include adherence to Neurotek's security and data protection policies

Risk Assessment

Neurotek conducts periodic risk assessments covering security, availability, confidentiality, processing integrity, and privacy risks. Identified risks are assessed for likelihood and impact, and mitigation plans are assigned to appropriate owners. Risk assessments are revisited when significant system or organizational changes occur.

Risk Identification and Analysis

- Formal Risk Register: Neurotek maintains a living risk register, documenting threats, vulnerabilities, and potential business impacts. Risks are categorized (e.g., security, operational, compliance) and assigned risk owners.
- Annual Risk Assessment: At least once per year, cross-functional teams (including IT, Security, Compliance, and Executive Leadership) evaluate existing risks and identify new or emerging risks. Risks are prioritized based on likelihood, potential impact, and regulatory significance.
- Ad Hoc Risk Assessments: Additional reviews may be performed when significant changes occur (e.g., new system modules, major vendor transitions).

Response to Risks

- Mitigation Strategies: For each identified risk, mitigation plans are developed, which may include improving system controls, updating policies, adding monitoring tools, or reinforcing staff training.
- Acceptance, Transfer, or Avoidance: Management may choose to accept low-level risks, transfer them via contractual agreements or insurance, or avoid them by discontinuing certain activities if the residual risk is deemed too high.

Control Activities

Control activities are the policies, procedures, and mechanisms implemented to address risks identified in our risk assessment process and support the achievement of service commitments and system requirements.

Policies and Procedures

- Policy Framework: Key written policies include Information Security Policy, Access Control Policy, Acceptable Use Policy, Change Management Policy, Incident Response Policy, Business Continuity/DR Policy, etc.
- Periodic Reviews and Updates: These policies are reviewed annually to ensure continued relevance to evolving threats, technologies, and regulations.

IT General Controls

1. **Logical Access**

Production system access requires VPN authentication. Access is provisioned on a role-based, least-privilege basis. Access rights are reviewed during offboarding and on a periodic basis. Multi-factor authentication is in place for privileged access.

2. **Change Management**

All changes to the production environment follow a documented process: development, peer code review, QA testing (including automated and browser compatibility testing via BrowserStack), and deployment via Jenkins CI/CD pipeline. Production deployments are logged.

3. **System Operations and Availability**

- Scheduled Maintenance: Maintenance windows are predefined, with communication to stakeholders.
- Incident Response: Incidents are escalated based on severity, tracked in a centralized system, and resolved per documented procedures.

4. **Data Integrity and Confidentiality**

- Encryption: Data in transit is protected via TLS. Data at rest is encrypted at both the database level and field level. Local storage on employee devices is encrypted under the hybrid work policy. Zabbix provides infrastructure monitoring. Sentry provides application error monitoring and alerting. Penetration testing and vulnerability scanning are conducted on an annual basis.
- Data Retention: Neurotek follows retention periods aligned with regulatory and contractual requirements, removing or anonymizing data after end-of-life.

5. **Supporting Manual and Automated Controls**

- Review of Exception Reports: Automated monitoring alerts are reviewed by the operations team, who document findings and escalation in the ticketing system.
- Vendor Management: Controls are in place to evaluate third-party security posture (e.g., requiring SOC 2 or ISO 27001 attestations from critical vendors).

6. **Information & Communication**

- Updated policies and security communications are shared with relevant staff through internal channels. Management meetings address operational, security, and compliance matters.
- Customer-facing communications include notifications for material platform changes, planned maintenance, or incidents via email and support portal.

7. **Internal Communication**

- Policy Distribution: Updated policies are published in the intranet/knowledge base, with notifications sent to relevant staff.

- Management Meetings: Cross-departmental meetings occur weekly to share critical control updates, discuss incidents, and address identified issues.
- Security Awareness: Regular bulletins or micro-trainings keep staff informed of emerging threats (e.g., phishing campaigns, zero-day exploits).

8. External Communication

- Customer Notifications: Major platform changes, planned downtimes, or incident disclosures are communicated via email and support portal.
- Regulatory Disclosures: If an incident or breach triggers a legal reporting obligation, we follow established processes to promptly notify authorities and affected parties.
- Feedback Channels: Clients and partners can submit complaints or suggestions through customer support or a dedicated feedback form. Such feedback is triaged, logged, and addressed accordingly.

Monitoring Activities

Ongoing monitoring is performed through Zabbix (infrastructure), Sentry (application errors), and Cloudflare (network/traffic). Periodic internal reviews assess control effectiveness. External assessments (e.g., penetration testing) are conducted annually. Control deficiencies are tracked to remediation.

1. Ongoing Monitoring

- System Performance and Security Tools: We use a centralized SIEM (such as AWS native tools), Cloudflare (for IDS/IPS and WAF), and Zabbix and Sentry as monitoring dashboards to track real-time system performance and security events. Alerts are escalated to on-call resources for prompt investigation.
- Performance Metrics: Key metrics (e.g., system uptime, response times, incident resolution time) are tracked and reviewed by senior management.

2. Periodic Evaluations

- Internal Audits: The internal audit team or designated personnel periodically evaluate the effectiveness of internal controls. Results are documented, with action items assigned to process owners.
- External Assessments: Third-party penetration tests and vulnerability scans are conducted annually, with results documented in a remediation plan.
- Risk Reassessments: Findings from audits and scans are factored into risk assessment updates to ensure continuous improvement.

3. Deficiency Management and Remediation

- Issue Tracking: Control deficiencies or noncompliance issues are documented in Jira, assigned an owner, and monitored to resolution.
- Remediation Action Plans: Significant issues require a formal plan, outlining steps and deadlines to address underlying causes. Corrective action progress is reported to executive leadership or relevant committees.

3.4 Principal Service Commitments and System Requirements

Service Commitments

Neurotek makes formal service commitments to its customers (user entities). These commitments are established through Master Service Agreements (MSAs), Terms of Service, Privacy Statements, and applicable regulatory disclosures. The commitments address:

- Security: Neurotek implements administrative, technical, and physical controls designed to protect client data from unauthorized access, disclosure, or destruction.
- Availability: Neurotek commits to maintaining system uptime sufficient for clinical and educational operations, backed by cloud redundancy and timely incident response.
- Confidentiality: Neurotek safeguards confidential client and patient data, including restricting access and applying field-level encryption.
- Processing Integrity: Neurotek ensures that assessment data is processed completely, validly, accurately, and in an authorized manner.
- Privacy: Neurotek collects, uses, retains, and disposes of personal information consistent with applicable data protection regulations (including GDPR, where applicable) and contractual obligations.

System Requirements

To fulfill our service commitments, Neurotek defines and maintains policies, procedures, and technology requirements. For example:

- Regulatory Compliance: The system is designed to align with GDPR requirements for EU data subjects, and with applicable Israeli data protection law. Neurotek has engaged Mednet as an EU regulatory authority contact.
- Information Security Policies: Access control, encryption, vulnerability management, and acceptable use policies are documented and enforced.
- Technical Specifications: Cloud architecture is designed for redundancy, encrypted data storage (at-rest and in-transit), VPN-restricted server access, and continuous monitoring.

Together, these commitments and requirements shape how we design, implement, and monitor controls across our infrastructure and applications.

3.5 Complementary User Entity Controls (CUECs)

- Neurotek has designed its system and control environment to meet the applicable trust services criteria under the assumption that certain controls (referred to as Complementary User Entity Controls, or CUECs) will be implemented by our customers ("user entities"). These CUECs are essential for fully achieving the trust services criteria relevant to the services we provide.
- Neurotek's system is designed under the assumption that user entities (licensed practitioners and their organizations) will implement the following Complementary User Entity Controls (CUECs):
- Account Management: User entities are responsible for managing their own user accounts within the MOXO platform, including provisioning access for their staff and revoking access promptly upon role changes or departures.
- Credential Security: User entities must maintain the confidentiality of their login credentials and enforce password policies within their own environments.
- Endpoint Security: User entities are responsible for maintaining secure configurations on the devices used to access MOXO, including up-to-date anti-malware and operating system patches.
- Data Classification: User entities must ensure that only authorized and appropriately classified data is submitted to the MOXO platform. Submission of data outside the intended scope is the responsibility of the user entity.
- Incident Reporting: User entities must promptly report any suspected unauthorized access, account compromise, or anomalous activity to Neurotek support via Zendesk.
- Regulatory Compliance: While Neurotek supports GDPR-aligned practices, user entities are responsible for ensuring that their own use of MOXO data complies with applicable local laws, professional regulations, and consent requirements governing patient or subject data in their jurisdiction.

- Periodic Access Review: User entities should periodically review and certify the access rights of their staff within the MOXO platform.

3.6 Complementary Subservice Organization Controls (CSOCs)

To fully achieve the trust services criteria relevant to our system and services, Neurotek relies on the proper design and operation of certain controls performed by subservice organizations. Complementary subservice organization controls (CSOCs) are controls that we assume would be implemented by subservice organizations and are necessary, in combination with controls at our organization to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved. Below is a table where we outline:

- **Subservice Organization & Services:** The name of the subservice org and a brief description of the functions or services they provide.
- **Applicable Trust Services Criteria (TSC):** Reference the criteria numbers (e.g., CC6.1, CC7.2) that the subservice organization's controls address.
- **Required Controls:** A concise summary of the control(s) we expect the subservice org to perform.

Subservice Organization	Services Performed	Applicable Criteria	Complementary Controls Required
AWS	Cloud hosting & infrastructure services	CC6.3, CC6.4 , CC7.1	Maintain physical security; ensure uptime per SLA; provide SOC 2 report annually
HubSpot	CRM platform	CC6.1 , CC9.2	Enforce access controls; maintain data confidentiality; provide SOC 2 report
Tranzila	Payment processing (credit card transactions)	CC6.6 , CC9.2	Maintain PCI-DSS compliance; encrypt payment data; notify of any breaches
Mailgun	Transactional email delivery	CC6.7 , CC9.2	Secure email transmission; protect message content; maintain availability
Cloudflare	CDN, DDoS protection, DNS	CC6.6 , CC7.2	Monitor and block malicious traffic; maintain firewall rules; provide uptime

Monitoring of Subservice Organization

Neurotek performs the following activities to monitor subservice organization performance and compliance:

- Annual review of vendor SOC 2, ISO 27001, or equivalent attestation reports for critical vendors.
- Periodic review of vendor service outputs and comparison against SLA commitments.
- Tracking of customer complaints or incidents attributable to subservice organization performance.
- Escalation to vendor account management when issues are identified.

Incidents And Significant Events

During the examination period, Neurotek did not experience any system incidents that materially impacted its ability to meet service commitments. Minor operational events were managed through the standard incident response process. No material breaches or extended outages occurred that required mandatory customer or regulatory notification.

Changes To The System

During the period covered by this examination, the following significant changes were made to the MOXO system:

- Application & Feature Enhancements (March 2026, v26.4.0): Introduced a new 'Client Report' feature enabling direct sharing with test subjects. The update also included a redesigned Profile page, free-text capabilities for medication entries, and registration flow optimizations to reduce user friction.
- Platform Expansion (August 2025, v19.2.0): Launched a dedicated Dashboard for distributors and corporate clients, expanded the supported testing age range, and integrated new localized payment options for Israeli customers.
- Policy Updates (April 2025): Updated the MOXO License & Terms of Service to reflect current licensing and operational requirements.
- No material changes to the core underlying cloud architecture or infrastructure were made that impacted the scope or performance of the system during the examination period.

Specific Criterion Not Relevant To The System

All Common Criteria of the applicable Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy apply to Neurotek's MOXO platform. No criteria have been identified as entirely not applicable.

Other Disclosures Or Forward-Looking Notes (Optional)

Neurotek is actively pursuing SOC 2 Type 2 certification and ISO certification as part of its commitment to demonstrating security and compliance maturity to its client base of healthcare providers and educational institutions. No other significant disclosures or forward-looking notes are applicable at this time.

3.7 Applicable Trust Services Criteria and Related Controls

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	C-TC.6	Monitor system performance, conduct regular capacity planning, and implement scaling solutions.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	C-OP.15	ICT readiness and information security must be maintained to ensure immediate recovery and minimal operational disruption.
		C-PC.2	Adequate security controls must be implemented and maintained for offices, rooms, and other facilities to protect against physical and environmental threats. This includes the secure siting and protection of equipment, secure cabling, and appropriate controls for supporting utilities.
		C-PC.4	Environmental controls such as fire extinguishers, fire sprinklers, smoke detectors, and UPS devices must be installed and regularly checked. Fire drills must be conducted annually. Mantraps or other physical devices must be used for controlling access to highly sensitive facilities.
		C-PC.7	Facilities, operations, and admin personnel must monitor the status of physical and environmental protections regularly. Maintenance checklists and reports must be used where applicable, including monitoring server room temperature daily and ensuring compliance with vendor warranty specifications.
		C-TC.13	Maintain regular backups to prevent data loss and ensure quick recovery.
		C-TC.14	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	C-OP.15	ICT readiness and information security must be maintained to ensure immediate recovery and minimal operational disruption.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	C-OP.19	Intellectual property rights must be protected to safeguard valuable organizational assets from unauthorized use.
		C-OP.20	Controls must be in place to protect organizational records from unauthorized access, modification, loss, or destruction.
		C-OP.39	Procedures must be established and implemented for labelling information in accordance with the organization's classification scheme, ensuring secure handling and transmission of sensitive information.
		C-OP.9	Information must be classified according to its sensitivity and importance to the organization, ensuring appropriate protection based on confidentiality, integrity, availability, and relevant stakeholder requirements.
		C-TC.11	Implement data masking to protect sensitive information during testing and development.
		C-TC.12	Deploy data leakage prevention measures to prevent unauthorized data transfers.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	C-OP.37	Procedures are in place to remove data from production based on retention schedules, contract requirements, and deletion rules that are applied to specific forms of data; disposals are tracked; a data disposal process is in place. These procedures are reviewed, updated, and approved as needed.
		C-PC.5	Appropriate controls for the security of assets off-premise and the secure disposal of media once it reaches its end of life must be implemented to ensure information is not leaked.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
		C-TC.10	Ensure secure deletion of information to prevent unauthorized access to residual data.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	C-HR.3	The Company must have a code of conduct within the Employee Handbook(or documented anywhere) that establishes standards and guidelines for personnel ethical behaviour. These would include security and privacy clauses. Personnel are required to read and accept the entity's code of conduct
		C-HR.7	All new employees and contractors must have to read and sign the Confidentiality Agreement (NDA) or Non-Disclosure Agreement upon joining.
		C-OP.1	Information security policies must be documented and followed to ensure the protection of sensitive information within the organization.
		C-OP.18	Compliance with all legal, statutory, regulatory, and contractual requirements must be ensured to protect the organization and avoid penalties.
		C-OP.8	Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	C-OP.34	The board of directors operates independently of management and meets quarterly to oversee the organization's internal control objectives OR Company founders and department leads meet quarterly to assess organizational objectives.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	C-OP.2	Roles and responsibilities, including management duties, must be clearly defined and followed to protect organizational information assets and ensure smooth operations, with top management reviewing and driving the information security culture.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	C-HR.1	External third party background verification checks must be carried out for all hires. This would include education qualification verification, employment verification, address check and where necessary criminal checks. Negative BGV reports require further management action. Internal HR Reference checks must be conducted by HR team or hiring manager through document verification and other reference checks with the former colleagues or managers provided in the resume.
		C-HR.10	The company must provide thorough and structured job training and onboarding programs for all new employees to ensure they are fully equipped to fulfil their responsibilities and duties competently. This training should cover job-specific skills, company policies and procedures, compliance requirements, and any other relevant information necessary for effective performance in their role. The onboarding process should include regular check-ins and assessments to gauge the employee's understanding and readiness. Employees are required to complete all designated training modules and formally acknowledge their completion. Documentation of completed training and acknowledgments should be retained in the employee's personnel file. Regular reviews and updates to training materials should be conducted to ensure ongoing relevance and effectiveness, with refresher courses provided as needed.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
		C-HR.2	The company must ensure that all employees and contractors are provided with a clear and comprehensive document outlining the terms of their employment. This document should include job responsibilities, compensation details, benefits, work hours, termination conditions, and other relevant employment conditions. Employees and contractors are required to read, understand, and formally acknowledge their agreement to these terms. The acknowledgment should be documented and retained in the employee's or contractor's personnel file. Regular reviews and updates to the terms of employment should be communicated to and re-acknowledged by all relevant personnel.
		C-HR.3	The Company must have a code of conduct within the Employee Handbook(or documented anywhere) that establishes standards and guidelines for personnel ethical behaviour. These would include security and privacy clauses. Personnel are required to read and accept the entity's code of conduct
		C-HR.4	The induction training given by HR must include information security training. In this training the HR must provide training on physical access, security policies and other security related do's and don'ts.
		C-HR.5	Performance appraisals must be performed by the management team on an annual basis at least. Disciplinary process to be communicated and acknowledged by personnel associated with the organization.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
		C-OP.2	Roles and responsibilities, including management duties, must be clearly defined and followed to protect organizational information assets and ensure smooth operations, with top management reviewing and driving the information security culture.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	C-HR.2	The company must ensure that all employees and contractors are provided with a clear and comprehensive document outlining the terms of their employment. This document should include job responsibilities, compensation details, benefits, work hours, termination conditions, and other relevant employment conditions. Employees and contractors are required to read, understand, and formally acknowledge their agreement to these terms. The acknowledgment should be documented and retained in the employee's or contractor's personnel file. Regular reviews and updates to the terms of employment should be communicated to and re-acknowledged by all relevant personnel.
		C-HR.3	The Company must have a code of conduct within the Employee Handbook(or documented anywhere) that establishes standards and guidelines for personnel ethical behaviour. These would include security and privacy clauses. Personnel are required to read and accept the entity's code of conduct
		C-HR.5	Performance appraisals must be performed by the management team on an annual basis at least. Disciplinary process to be communicated and acknowledged by personnel associated with the organization.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
		C-HR.6	The company must clearly communicate the post-employment responsibilities to all employees during the offboarding process. This includes, but is not limited to, confidentiality obligations, non-compete agreements, return of company property, and any other relevant post-employment conditions. Employees are required to read, understand, and formally acknowledge their agreement to these responsibilities. The acknowledgment should be documented and retained in the employee's personnel file. Regular reviews and updates to post-employment responsibilities should be communicated to and re-acknowledged by all relevant personnel upon their departure from the company.
		C-HR.7	All new employees and contractors must have to read and sign the Confidentiality Agreement (NDA) or Non-Disclosure Agreement upon joining.
		C-OP.2	Roles and responsibilities, including management duties, must be clearly defined and followed to protect organizational information assets and ensure smooth operations, with top management reviewing and driving the information security culture.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	C-OP.33	The data flow diagram is maintained and highlights the systems that require logical access controls per data classification level. The data flow diagram is updated annually or as business needs require.
		C-OP.7	Information and asset inventory must be maintained to effectively track the use of all assets owned by the organization.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	C-HR.4	The induction training given by HR must include information security training. In this training the HR must provide training on physical access, security policies and other security related do's and don'ts.
		C-OP.1	Information security policies must be documented and followed to ensure the protection of sensitive information within the organization.
		C-OP.24	SOPs must be documented and followed for each department and role to ensure streamlined operations and information security.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	C-OP.26	The organization must implement a structured process to handle customer grievances and take prompt corrective actions.
		C-OP.28	The organization must report any changes or deviations in people, processes, or system architecture to customers and relevant stakeholders to ensure transparency and alignment.
		C-OP.29	The organization must ensure that all externally communicated terms and policies, including Terms of Service (ToS), Master Service Agreements (MSA), Privacy Policy, and consent for data usage, are clearly documented, regularly reviewed, and properly communicated to customers and stakeholders. These commitments must be updated as necessary to reflect changes in legal, regulatory, and operational requirements. The organization must ensure that these documents are accessible and that any revisions are communicated transparently to the affected parties.
		C-OP.3	Contact with relevant authorities must be in place to ensure streamlined communication regarding various concerns/events/updates both internally and externally.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	C-OP.25	Regular risk management exercises must be conducted to ensure awareness of risks and to implement mitigation plans, thereby maintaining operational hygiene.
		C-OP.6	Information security within project management must ensure the safe and secure onboarding and delivery of projects both internally and externally.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	C-OP.25	Regular risk management exercises must be conducted to ensure awareness of risks and to implement mitigation plans, thereby maintaining operational hygiene.
		C-OP.5	Threat intelligence controls must be implemented to ensure the organization receives regular updates on the latest information security attacks, trends, and analysis to avoid cyber-attacks and ensure data security.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	C-OP.25	Regular risk management exercises must be conducted to ensure awareness of risks and to implement mitigation plans, thereby maintaining operational hygiene.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.		Regular risk management exercises must be conducted to ensure awareness of risks and to implement mitigation plans, thereby maintaining operational hygiene.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	C-OP.22	Independent reviews of information security must be conducted to ensure continuous compliance with relevant laws and standards.
		C-TC.22	Conduct regular security testing to detect and mitigate vulnerabilities in the development life cycle.
		C-TC.27	Protect information systems during audit testing to prevent system disruptions and unauthorized access.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	C-OP.23	Compliance with information security policies and standards must be ensured to maintain a secure environment and drive security practices within the organization.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	C-OP.1	Information security policies must be documented and followed to ensure the protection of sensitive information within the organization.
		C-OP.20	Controls must be in place to protect organizational records from unauthorized access, modification, loss, or destruction.
		C-OP.38	Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.
		C-OP.39	Procedures must be established and implemented for labelling information in accordance with the organization's classification scheme, ensuring secure handling and transmission of sensitive information.
		C-OP.6	Information security within project management must ensure the safe and secure onboarding and delivery of projects both internally and externally.
		C-OP.7	Information and asset inventory must be maintained to effectively track the use of all assets owned by the organization.
		C-OP.9	Information must be classified according to its sensitivity and importance to the organization, ensuring appropriate protection based on confidentiality, integrity, availability, and relevant stakeholder requirements.
CC5.2	The entity also selects and develops general control activities over technology to	C-OP.17	Zero Trust principles must be followed to ensure ultimate security by not trusting any entity implicitly.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
	support the achievement of objectives.	C-TC.1	Endpoint protection, including antivirus software, firewalls and encryption, is configured appropriately on all devices.
		C-TC.15	Implement logging and monitoring to detect security incidents and ensure accountability.
		C-TC.18	Implement network security measures to prevent attacks and unauthorized access.
		C-TC.2	Implement a role-based access control system, regularly review and update access privileges, and monitor privileged user activities.
		C-TC.20	Maintain strong cryptographic controls to protect data integrity and confidentiality.
		C-TC.21	Implement secure development practices to prevent vulnerabilities in applications.
		C-TC.25	Implement change management to prevent unauthorized changes and ensure system stability.
		C-TC.3	Configure access control lists (ACLs), use multi-factor authentication (MFA), and enforce least privilege access principles.
		C-TC.5	Implement MFA, enforce strong password policies, and use single sign-on (SSO) solutions.
		C-TC.7	Deploy and update antivirus/anti-malware software, perform regular malware scans, and educate users on safe practices.
		C-TC.9	Maintain consistent configuration management to prevent security vulnerabilities.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	C-HR.8	The company must establish and implement a comprehensive security policy specifically for remote working and work-from-home (WFH) arrangements. This policy should cover all aspects of information security, including secure access to company systems, data protection measures, use of company-approved devices, and guidelines for maintaining a secure work environment at home. Employees must receive training on these security policies as part of their onboarding process and on a regular basis thereafter. The training should ensure that employees understand the importance of adhering to these policies and the potential risks associated with remote work. Employees are required to acknowledge their understanding and agreement to comply with the remote working/WFH security policies. This acknowledgment should be documented and retained in the employee's personnel file. Regular reviews and updates to the remote working security policy should be communicated to and re-acknowledged by all relevant personnel.
		C-OP.1	Information security policies must be documented and followed to ensure the protection of sensitive information within the organization.
		C-OP.24	SOPs must be documented and followed for each department and role to ensure streamlined operations and information security.
		C-OP.8	Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.
		C-PC.6	Clear desk and clear screen controls must be implemented and followed by all employees/associate personnel of the organization, both on-premise and off-premise.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	C-OP.11	Access control measures must be implemented to protect physical and logical assets, ensuring only authorized personnel can access information and systems.
		C-OP.41	Allocate, manage, and secure authentication information, ensuring personnel understand proper handling and usage practices.
		C-TC.2	Implement a role-based access control system, regularly review and update access privileges, and monitor privileged user activities.
		C-TC.20	Maintain strong cryptographic controls to protect data integrity and confidentiality.
		C-TC.3	Configure access control lists (ACLs), use multi-factor authentication (MFA), and enforce least privilege access principles.
		C-TC.4	Use version control systems with access controls, conduct regular access reviews, and require MFA for source code repositories.
		C-TC.5	Implement MFA, enforce strong password policies, and use single sign-on (SSO) solutions.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	C-OP.40	The full lifecycle of identities, including creation, modification, and de-provisioning, must be managed securely to ensure only legitimate users access organizational resources.
		C-TC.30	A user's logical (and physical) access to IT systems is revoked within 24 hours of termination or transfer and all assets are returned to the organization when employment ends or their contract terminates. Exceptions are documented in an offboarding checklist and/or offboarding ticket.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities,	C-OP.11	Access control measures must be implemented to protect physical and logical assets, ensuring only authorized personnel can access information and systems.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
	or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	C-OP.42	Access rights must be provisioned, regularly reviewed, modified, and removed in accordance with organizational access control policies and business requirements.
		C-TC.2	Implement a role-based access control system, regularly review and update access privileges, and monitor privileged user activities.
		C-TC.3	Configure access control lists (ACLs), use multi-factor authentication (MFA), and enforce least privilege access principles.
		C-TC.4	Use version control systems with access controls, conduct regular access reviews, and require MFA for source code repositories.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	C-OP.11	Access control measures must be implemented to protect physical and logical assets, ensuring only authorized personnel can access information and systems.
		C-PC.1	Physical security perimeters must be appropriately marked. All entry and exit points must be adequately secured with physical access controls, monitored through CCTV, and restricted to authorized personnel only. This includes delivery and loading areas.
		C-PC.10	Physical access to the onsite server room is restricted to authorized individuals who have the key; access is approved by the head of IT.
		C-PC.2	Adequate security controls must be implemented and maintained for offices, rooms, and other facilities to protect against physical and environmental threats. This includes the secure siting and protection of equipment, secure cabling, and appropriate controls for supporting utilities.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
		C-PC.3	A physical access control system must be implemented to secure facilities. All visitors must enter their details in a visitor logbook, be issued temporary visitor ID cards, and be escorted by a company employee/security. ID cards with employee pictures must be worn at all times, and access must be deactivated upon termination.
		C-PC.6	Clear desk and clear screen controls must be implemented and followed by all employees/associate personnel of the organization, both on-premise and off-premise.
		C-PC.9	Physical access to the onsite server room/data center is restricted to authorized individuals only. All new access requests and changes to access permissions are appropriately approved and documented. Management performs at least an annual review of physical user access to the data center. During this review, inactive users are identified and removed, with the removal process being documented. The review is formally documented, including system-generated user listings and sign-off by management to ensure accountability and compliance.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	C-OP.37	Procedures are in place to remove data from production based on retention schedules, contract requirements, and deletion rules that are applied to specific forms of data; disposals are tracked; a data disposal process is in place. These procedures are reviewed, updated, and approved as needed.
		C-PC.5	Appropriate controls for the security of assets off-premise and the secure disposal of media once it reaches its end of life must be implemented to ensure information is not leaked.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
		C-TC.10	Ensure secure deletion of information to prevent unauthorized access to residual data.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	C-OP.13	Cloud security controls must be implemented to ensure secure usage of cloud environments, preventing data leaks and unauthorized access.
		C-OP.17	Zero Trust principles must be followed to ensure ultimate security by not trusting any entity implicitly.
		C-TC.1	Endpoint protection, including antivirus software, firewalls and encryption, is configured appropriately on all devices.
		C-TC.12	Deploy data leakage prevention measures to prevent unauthorized data transfers.
		C-TC.18	Implement network security measures to prevent attacks and unauthorized access.
		C-TC.19	Deploy web filtering controls to prevent access to malicious websites and inappropriate content.
		C-TC.20	Maintain strong cryptographic controls to protect data integrity and confidentiality.
		C-TC.5	Implement MFA, enforce strong password policies, and use single sign-on (SSO) solutions.
		C-TC.8	Regularly assess and manage vulnerabilities to prevent exploits.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	C-OP.10	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.
		C-PC.5	Appropriate controls for the security of assets off-premise and the secure disposal of media once it reaches its end of life must be implemented to ensure information is not leaked.
		C-TC.10	Ensure secure deletion of information to prevent unauthorized access to residual data.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
		C-TC.12	Deploy data leakage prevention measures to prevent unauthorized data transfers.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	C-TC.1	Endpoint protection, including antivirus software, firewalls and encryption, is configured appropriately on all devices.
		C-TC.17	Manage software installation to prevent unauthorized software and ensure system stability.
		C-TC.29	Threat detection tools are utilized to monitor and log possible or actual network breaches and other anomalous security events. Alerting occurs on threats and results are actioned as appropriate.
		C-TC.7	Deploy and update antivirus/anti-malware software, perform regular malware scans, and educate users on safe practices.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	C-OP.5	Threat intelligence controls must be implemented to ensure the organization receives regular updates on the latest information security attacks, trends, and analysis to avoid cyber-attacks and ensure data security.
		C-TC.15	Implement logging and monitoring to detect security incidents and ensure accountability.
		C-TC.22	Conduct regular security testing to detect and mitigate vulnerabilities in the development life cycle.
		C-TC.25	Implement change management to prevent unauthorized changes and ensure system stability.
		C-TC.29	Threat detection tools are utilized to monitor and log possible or actual network breaches and other anomalous security events. Alerting occurs on threats and results are actioned as appropriate.
		C-TC.8	Regularly assess and manage vulnerabilities to prevent exploits.
CC7.2	The entity monitors system components and the operation of those components for	C-TC.15	Implement logging and monitoring to detect security incidents and ensure accountability.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
	anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	C-TC.29	Threat detection tools are utilized to monitor and log possible or actual network breaches and other anomalous security events. Alerting occurs on threats and results are actioned as appropriate.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	C-HR.9	The company must provide comprehensive training to all employees and contractors on the procedures for reporting security incidents and events. This training should cover the types of incidents that need to be reported, the appropriate channels and contacts for reporting, and the steps to be taken immediately following the discovery of a security incident. The training should emphasize the importance of prompt and accurate reporting to mitigate potential risks and ensure swift resolution. Employees and contractors are required to acknowledge their understanding of the security incident/event reporting procedures. This acknowledgment should be documented and retained in their personnel file. Regular refresher training sessions should be conducted to reinforce the reporting procedures and update personnel on any changes.
		C-OP.14	Incident management controls must be followed to address incidents appropriately, reducing repeated occurrences and improving security.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
CC7.4	The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.	C-HR.9	The company must provide comprehensive training to all employees and contractors on the procedures for reporting security incidents and events. This training should cover the types of incidents that need to be reported, the appropriate channels and contacts for reporting, and the steps to be taken immediately following the discovery of a security incident. The training should emphasize the importance of prompt and accurate reporting to mitigate potential risks and ensure swift resolution. Employees and contractors are required to acknowledge their understanding of the security incident/event reporting procedures. This acknowledgment should be documented and retained in their personnel file. Regular refresher training sessions should be conducted to reinforce the reporting procedures and update personnel on any changes.
		C-OP.14	Incident management controls must be followed to address incidents appropriately, reducing repeated occurrences and improving security.
		C-OP.35	A Data Breach Policy and related procedures are in place. Procedures contain supporting processes to receive, track, address, resolve, and respond to incidents involving user data, and to communicate incidents to affected parties and data subjects. This policy is reviewed, updated, and approved annually.
		C-OP.36	Procedures are in place for breach notification. Procedures include who must be notified, under what circumstances breach notifications must be prepared, the timing of the notification, how the notification is to be sent, and the required elements of the notification.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	C-OP.14	Incident management controls must be followed to address incidents appropriately, reducing repeated occurrences and improving security.
		C-OP.15	ICT readiness and information security must be maintained to ensure immediate recovery and minimal operational disruption.
		C-OP.29	The organization must ensure that all externally communicated terms and policies, including Terms of Service (ToS), Master Service Agreements (MSA), Privacy Policy, and consent for data usage, are clearly documented, regularly reviewed, and properly communicated to customers and stakeholders. These commitments must be updated as necessary to reflect changes in legal, regulatory, and operational requirements. The organization must ensure that these documents are accessible and that any revisions are communicated transparently to the affected parties.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	C-TC.17	Manage software installation to prevent unauthorized software and ensure system stability.
		C-TC.21	Implement secure development practices to prevent vulnerabilities in applications.
		C-TC.24	Development, testing and production environments should be separated and secured to prevent cross-contamination and data leaks.
		C-TC.25	Implement change management to prevent unauthorized changes and ensure system stability.
		C-TC.9	Maintain consistent configuration management to prevent security vulnerabilities.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	C-OP.15	ICT readiness and information security must be maintained to ensure immediate recovery and minimal operational disruption.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
		C-OP.16	Business insurance must be in place to ensure financial recovery from incidents or disasters.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	C-OP.13	Cloud security controls must be implemented to ensure secure usage of cloud environments, preventing data leaks and unauthorized access.
		C-OP.30	A policy and procedures are in place which govern the vendor management lifecycle. The policy is reviewed and re-approved by management annually. Procedures are defined for assessing vendor risk.
		C-OP.31	Due diligence activities are performed over new vendors and service providers prior to contract execution. Due diligence activities include an assessment of information security practices based on the assessed level of vendor risk.
		C-OP.32	Critical IT vendors and service providers are annually reviewed to update their risk profiles, assess performance against contracts, re-assess the vendors' security controls, and manage change in supplier information security practices and service delivery.
		C-TC.23	Implement controls for outsourced development to ensure quality and security compliance.
P1.1	The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.	C-OP.21	Controls for the privacy and protection of PII must be implemented to prevent unauthorized access, use, or modification of sensitive information.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
P2.1	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.		Controls for the privacy and protection of PII must be implemented to prevent unauthorized access, use, or modification of sensitive information.
P3.1	Personal information is collected consistent with the entity's objectives related to privacy.		Controls for the privacy and protection of PII must be implemented to prevent unauthorized access, use, or modification of sensitive information.
P3.2	For information requiring explicit consent, the entity communicates the need for such consent as well as the consequences of a failure to provide consent for the request for personal information and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.		Controls for the privacy and protection of PII must be implemented to prevent unauthorized access, use, or modification of sensitive information.
		C-OP.29	The organization must ensure that all externally communicated terms and policies, including Terms of Service (ToS), Master Service Agreements (MSA), Privacy Policy, and consent for data usage, are clearly documented, regularly reviewed, and properly communicated to customers and stakeholders. These commitments must be updated as necessary to reflect changes in legal, regulatory, and operational requirements. The organization must ensure that these documents are accessible and that any revisions are communicated transparently to the affected parties.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
P4.1	The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.	C-OP.21	Controls for the privacy and protection of PII must be implemented to prevent unauthorized access, use, or modification of sensitive information.
		C-TC.11	Implement data masking to protect sensitive information during testing and development.
P4.2	The entity retains personal information consistent with the entity's objectives related to privacy.	C-OP.37	Procedures are in place to remove data from production based on retention schedules, contract requirements, and deletion rules that are applied to specific forms of data; disposals are tracked; a data disposal process is in place. These procedures are reviewed, updated, and approved as needed.
P4.3	The entity securely disposes of personal information to meet the entity's objectives related to privacy.		Procedures are in place to remove data from production based on retention schedules, contract requirements, and deletion rules that are applied to specific forms of data; disposals are tracked; a data disposal process is in place. These procedures are reviewed, updated, and approved as needed.
		C-TC.10	Ensure secure deletion of information to prevent unauthorized access to residual data.
P5.1	The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	C-OP.21	Controls for the privacy and protection of PII must be implemented to prevent unauthorized access, use, or modification of sensitive information.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
P5.2	The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.		Controls for the privacy and protection of PII must be implemented to prevent unauthorized access, use, or modification of sensitive information.
P6.1	The entity discloses personal information to third parties with the explicit consent of data subjects and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.		Controls for the privacy and protection of PII must be implemented to prevent unauthorized access, use, or modification of sensitive information.
		C-OP.31	Due diligence activities are performed over new vendors and service providers prior to contract execution. Due diligence activities include an assessment of information security practices based on the assessed level of vendor risk.
		C-OP.32	Critical IT vendors and service providers are annually reviewed to update their risk profiles, assess performance against contracts, re-assess the vendors' security controls, and manage change in supplier information security practices and service delivery.
P6.2	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.	C-OP.21	Controls for the privacy and protection of PII must be implemented to prevent unauthorized access, use, or modification of sensitive information.
P6.3	The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.	C-OP.35	A Data Breach Policy and related procedures are in place. Procedures contain supporting processes to receive, track, address, resolve, and respond to incidents involving user data, and to communicate incidents to affected parties and data subjects. This policy is reviewed, updated, and approved annually.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
P6.4	The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.	C-OP.30	A policy and procedures are in place which govern the vendor management lifecycle. The policy is reviewed and re-approved by management annually. Procedures are defined for assessing vendor risk.
		C-OP.31	Due diligence activities are performed over new vendors and service providers prior to contract execution. Due diligence activities include an assessment of information security practices based on the assessed level of vendor risk.
		C-OP.32	Critical IT vendors and service providers are annually reviewed to update their risk profiles, assess performance against contracts, re-assess the vendors' security controls, and manage change in supplier information security practices and service delivery.
P6.5	The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident-response procedures to meet the entity's objectives related to privacy.		Critical IT vendors and service providers are annually reviewed to update their risk profiles, assess performance against contracts, re-assess the vendors' security controls, and manage change in supplier information security practices and service delivery.
P6.6	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.	C-OP.35	A Data Breach Policy and related procedures are in place. Procedures contain supporting processes to receive, track, address, resolve, and respond to incidents involving user data, and to communicate incidents to affected parties and data subjects. This policy is reviewed, updated, and approved annually.

TSC Ref#	Criteria Description	Control#	Control Activity as specified by Neurotek
		C-OP.36	Procedures are in place for breach notification. Procedures include who must be notified, under what circumstances breach notifications must be prepared, the timing of the notification, how the notification is to be sent, and the required elements of the notification.
P6.7	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.	C-OP.21	Controls for the privacy and protection of PII must be implemented to prevent unauthorized access, use, or modification of sensitive information.
P7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.		Controls for the privacy and protection of PII must be implemented to prevent unauthorized access, use, or modification of sensitive information.
P8.1	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.	C-OP.26	The organization must implement a structured process to handle customer grievances and take prompt corrective actions.
PI1.5	The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.	C-TC.26	Protect test information to prevent unauthorized access and data breaches.

[Space intentionally left blank]

SECTION 4

TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

4. Trust Services Category, Criteria, Related Controls, and Tests of Controls

4.1 Objective of Our Examination

This report is intended to provide interested parties with information about the controls at Neurotek that may affect the processing of user organizations' transactions and also to provide users with information about the operating effectiveness of the controls that were tested. This report, when combined with an understanding and assessment of the controls at user organizations, is intended to assist user auditors in (1) planning the audit of user organizations' financial statements and (2) assessing control risk for assertions in user organizations' financial statements that may be affected by controls at Neurotek.

Our testing of Neurotek controls was restricted to the control objectives and related controls listed in the matrices in this section of the report and was not extended to controls described in the system description but not included in the aforementioned matrices, or to controls that may be in effect at user organizations. It is each user auditor's responsibility to evaluate this information about the controls in place at each user organization. If certain complementary controls are not in place at user organizations, Neurotek controls may not compensate for such weaknesses.

4.2 Control Environment Elements

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for other components of internal control, providing discipline and structure. In addition to the tests of design, implementation, and operating effectiveness of controls identified by Neurotek our procedures included tests of the following relevant elements of the Neurotek control environment:

1. Environment
2. Internal Risk Assessment
3. Information and Communication
4. Control Activities
5. Monitoring

Such tests included inquiry of the appropriate management, supervisory, and staff personnel; observation of Neurotek activities and operations, inspection of Neurotek documents and records, and re-performance of the application of Neurotek controls. The results of these tests were considered in planning the nature, timing, and extent of our testing of the control activities described in this section.

4.3 Applicable Trust Services Criteria, Controls, Tests of Operating Effectiveness, and Results of Tests

Our tests were designed to examine Neurotek description of the system related to Neurotek as well as the suitability of the design effectiveness of controls for a representative number of samples as of May 08, 2026.

In selecting particular tests of the operational effectiveness of controls, we considered (a) the nature of the items being tested, (b) types of available evidential matter, (c) the nature of the trust services principles and criteria to be achieved, and (d) expected efficiency and effectiveness of the test.

Testing the accuracy and completeness of the information provided by Neurotek is also a component of the testing procedures performed. Information we are utilizing as evidence may include but is not limited to:

1. Standard 'out of the box' reports as configured within the system
2. Parameter-driven reports generated by Neurotek
3. Custom-developed reports that are not standard to the application such as scripts, report writers, and queries
4. Spreadsheets that include relevant information utilized for the performance or testing of a control
5. Neurotek-prepared analyses, schedules, or other evidence manually prepared and utilized by the Company

While these procedures are not specifically called out in the test procedures listed in this section, they are completed as a component of our testing to support the evaluation of whether or not the information is sufficiently precise and detailed for purposes of fully testing the controls identified by Neurotek.

Description of Testing Procedures Performed

Our examination included inquiry of management, supervisory, and staff personnel; inspection of documents and records; observation of activities and operations; and re-performance of controls surrounding and provided by Neurotek Our tests of controls were performed on controls as they existed for the period from as of May 08, 2026, and were applied to those controls relating to the trust services principles and criteria.

Tests performed on the operational effectiveness of controls are described below:

Test	Description
Inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the reporting period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.
Observation	Observed the performance of the control multiple times throughout the reporting period to evidence the application of the specific control activity.
Examination of Documentation/Inspection	If the performance of the control is documented, inspected documents and reports indicate the performance of the control.
Re-performance of Monitoring Activities or Manual Controls	Obtained documents used in the monitoring activity or manual control activity and independently re-performed the procedures. Compare any exception items identified with those identified by the responsible control owner.
Re-performance of Programmed Processing	Input test data, manually calculated expected results, and compared actual results of processing to expectations.

4.4 Testing Procedures Performed by Independent Service Auditor

In addition to the tests listed below for each control specified by Neurotek, ascertained through inquiry with management and the controlling owner that each control activity listed below operated as described as of May 08, 2026.

TSC Ref	Control#	Control Activities as specified by Neurotek	Results of Test
CC1.1 CC2.2 CC5.1 CC5.3	C-OP.1	Information security policies must be documented and followed to ensure the protection of sensitive information within the organization.	No Exceptions Noted.
CC1.1 CC5.3	C-OP.8	Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.	No Exceptions Noted.
CC1.1	C-OP.18	Compliance with all legal, statutory, regulatory, and contractual requirements must be ensured to protect the organization and avoid penalties.	No Exceptions Noted.
CC1.1 CC1.4 CC1.5	C-HR.3	The Company must have a code of conduct within the Employee Handbook(or documented anywhere) that establishes standards and guidelines for personnel ethical behaviour. These would include security and privacy clauses. Personnel are required to read and accept the entity’s code of conduct	No Exceptions Noted.
CC1.1 CC1.5	C-HR.7	All new employees and contractors must have to read and sign the Confidentiality Agreement (NDA) or Non-Disclosure Agreement upon joining.	No Exceptions Noted.
CC1.2	C-OP.34	The board of directors operates independently of management and meets quarterly to oversee the organization's internal control objectives OR Company founders and department leads meet quarterly to assess organizational objectives.	No Exceptions Noted.
CC1.3 CC1.4 CC1.5	C-OP.2	Roles and responsibilities, including management duties, must be clearly defined and followed to protect organizational information assets and ensure smooth operations, with top management reviewing and driving the information security culture.	No Exceptions Noted.
CC1.4	C-HR.1	External third party background verification checks must be carried out for all hires. This would include education qualification verification, employment verification, address check and where necessary criminal checks. Negative BGV reports require further management action. Internal HR Reference checks must be conducted by HR team or hiring manager through document verification and other reference checks with the former colleagues or managers provided in the resume.	No Exceptions Noted.
CC1.4 CC1.5	C-HR.2	The company must ensure that all employees and contractors are provided with a clear and comprehensive document outlining the terms of their employment. This document should include job responsibilities, compensation details, benefits, work hours, termination conditions, and other relevant employment conditions. Employees and contractors	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Neurotek	Results of Test
		are required to read, understand, and formally acknowledge their agreement to these terms. The acknowledgment should be documented and retained in the employee's or contractor's personnel file. Regular reviews and updates to the terms of employment should be communicated to and re-acknowledged by all relevant personnel.	
CC1.4 CC2.2	C-HR.4	The induction training given by HR must include information security training. In this training the HR must provide training on physical access, security policies and other security related do's and don'ts.	No Exceptions Noted.
CC1.4 CC1.5	C-HR.5	Performance appraisals must be performed by the management team on an annual basis at least. Disciplinary process to be communicated and acknowledged by personnel associated with the organization.	No Exceptions Noted.
CC1.4	C-HR.10	The company must provide thorough and structured job training and onboarding programs for all new employees to ensure they are fully equipped to fulfill their responsibilities and duties competently. This training should cover job-specific skills, company policies and procedures, compliance requirements, and any other relevant information necessary for effective performance in their role. The onboarding process should include regular check-ins and assessments to gauge the employee's understanding and readiness. Employees are required to complete all designated training modules and formally acknowledge their completion. Documentation of completed training and acknowledgments should be retained in the employee's personnel file. Regular reviews and updates to training materials should be conducted to ensure ongoing relevance and effectiveness, with refresher courses provided as needed.	No Exceptions Noted.
CC1.5	C-HR.6	The company must clearly communicate the post-employment responsibilities to all employees during the offboarding process. This includes, but is not limited to, confidentiality obligations, non-compete agreements, return of company property, and any other relevant post-employment conditions. Employees are required to read, understand, and formally acknowledge their agreement to these responsibilities. The acknowledgment should be documented and retained in the employee's personnel file. Regular reviews and updates to post-employment responsibilities should be communicated to and re-acknowledged by all relevant personnel upon their departure from the company.	No Exceptions Noted.
CC2.1 CC5.1	C-OP.7	Information and asset inventory must be maintained to effectively track the use of all assets owned by the organization.	No Exceptions Noted.
CC2.1	C-OP.33	The data flow diagram is maintained and highlights the systems that require logical access controls per data classification level. The data flow diagram is updated annually or as business needs require.	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Neurotek	Results of Test
CC2.2 CC5.3	C-OP.24	SOPs must be documented and followed for each department and role to ensure streamlined operations and information security.	No Exceptions Noted.
CC2.3	C-OP.3	Contact with relevant authorities must be in place to ensure streamlined communication regarding various concerns/events/updates both internally and externally.	No Exceptions Noted.
CC2.3 P8.1	C-OP.26	The organization must implement a structured process to handle customer grievances and take prompt corrective actions.	No Exceptions Noted.
CC2.3	C-OP.28	The organization must report any changes or deviations in people, processes, or system architecture to customers and relevant stakeholders to ensure transparency and alignment.	No Exceptions Noted.
CC2.3 CC7.5 P3.2	C-OP.29	The organization must ensure that all externally communicated terms and policies, including Terms of Service (ToS), Master Service Agreements (MSA), Privacy Policy, and consent for data usage, are clearly documented, regularly reviewed, and properly communicated to customers and stakeholders. These commitments must be updated as necessary to reflect changes in legal, regulatory, and operational requirements. The organization must ensure that these documents are accessible and that any revisions are communicated transparently to the affected parties.	No Exceptions Noted.
CC3.1 CC5.1	C-OP.6	Information security within project management must ensure the safe and secure onboarding and delivery of projects both internally and externally.	No Exceptions Noted.
CC3.1 CC3.2 CC3.3 CC3.4	C-OP.25	Regular risk management exercises must be conducted to ensure awareness of risks and to implement mitigation plans, thereby maintaining operational hygiene.	No Exceptions Noted.
CC3.2 CC7.1	C-OP.5	Threat intelligence controls must be implemented to ensure the organization receives regular updates on the latest information security attacks, trends, and analysis to avoid cyber-attacks and ensure data security.	No Exceptions Noted.
CC4.1	C-OP.22	Independent reviews of information security must be conducted to ensure continuous compliance with relevant laws and standards.	No Exceptions Noted.
CC4.1 CC7.1	C-TC.22	Conduct regular security testing to detect and mitigate vulnerabilities in the development life cycle.	No Exceptions Noted.
CC4.1	C-TC.27	Protect information systems during audit testing to prevent system disruptions and unauthorized access.	No Exceptions Noted.
CC4.2	C-OP.23	Compliance with information security policies and standards must be ensured to maintain a secure environment and drive security practices within the organization.	No Exceptions Noted.
CC5.1 C1.1	C-OP.9	Information must be classified according to its sensitivity and importance to the organization, ensuring appropriate protection based on confidentiality, integrity, availability, and relevant stakeholder requirements.	No Exceptions Noted.
CC5.1	C-OP.20	Controls must be in place to protect organizational records	No Exceptions

TSC Ref	Control#	Control Activities as specified by Neurotek	Results of Test
C1.1		from unauthorized access, modification, loss, or destruction.	Noted.
CC5.1	C-OP.38	Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	No Exceptions Noted.
CC5.1 C1.1	C-OP.39	Procedures must be established and implemented for labeling information in accordance with the organization's classification scheme, ensuring secure handling and transmission of sensitive information.	No Exceptions Noted.
CC5.2 CC6.6	C-OP.17	Zero Trust principles must be followed to ensure ultimate security by not trusting any entity implicitly.	No Exceptions Noted.
CC5.2 CC6.6 CC6.8	C-TC.1	Endpoint protection, including antivirus software, firewalls and encryption, is configured appropriately on all devices.	No Exceptions Noted.
CC5.2 CC6.1 CC6.3	C-TC.2	Implement a role-based access control system, regularly review and update access privileges, and monitor privileged user activities.	No Exceptions Noted.
CC5.2 CC6.1 CC6.3	C-TC.3	Configure access control lists (ACLs), use multi-factor authentication (MFA), and enforce least privilege access principles.	No Exceptions Noted.
CC5.2 CC6.1 CC6.6	C-TC.5	Implement MFA, enforce strong password policies, and use single sign-on (SSO) solutions.	No Exceptions Noted.
CC5.2 CC6.8	C-TC.7	Deploy and update antivirus/anti-malware software, perform regular malware scans, and educate users on safe practices.	No Exceptions Noted.
CC5.2 CC8.1	C-TC.9	Maintain consistent configuration management to prevent security vulnerabilities.	No Exceptions Noted.
CC5.2 CC7.1 CC7.2	C-TC.15	Implement logging and monitoring to detect security incidents and ensure accountability.	No Exceptions Noted.
CC5.2 CC6.6	C-TC.18	Implement network security measures to prevent attacks and unauthorized access.	No Exceptions Noted.
CC5.2 CC6.1 CC6.6	C-TC.20	Maintain strong cryptographic controls to protect data integrity and confidentiality.	No Exceptions Noted.
CC5.2 CC8.1	C-TC.21	Implement secure development practices to prevent vulnerabilities in applications.	No Exceptions Noted.
CC5.2 CC7.1 CC8.1	C-TC.25	Implement change management to prevent unauthorized changes and ensure system stability.	No Exceptions Noted.
CC5.3	C-HR.8	The company must establish and implement a comprehensive security policy specifically for remote working and work-from-home (WFH) arrangements. This policy should cover all aspects of information security, including secure access to company systems, data protection measures, use of company-approved devices, and guidelines for maintaining a secure work environment at home.	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Neurotek	Results of Test
		Employees must receive training on these security policies as part of their onboarding process and on a regular basis thereafter. The training should ensure that employees understand the importance of adhering to these policies and the potential risks associated with remote work. Employees are required to acknowledge their understanding and agreement to comply with the remote working/WFH security policies. This acknowledgment should be documented and retained in the employee's personnel file. Regular reviews and updates to the remote working security policy should be communicated to and re-acknowledged by all relevant personnel.	
CC5.3 CC6.4	C-PC.6	Clear desk and clear screen controls must be implemented and followed by all employees/associate personnel of the organization, both on-premise and off-premise.	No Exceptions Noted.
CC6.1 CC6.3 CC6.4	C-OP.11	Access control measures must be implemented to protect physical and logical assets, ensuring only authorized personnel can access information and systems.	No Exceptions Noted.
CC6.1	C-OP.41	Allocate, manage, and secure authentication information, ensuring personnel understand proper handling and usage practices.	No Exceptions Noted.
CC6.1 CC6.3	C-TC.4	Use version control systems with access controls, conduct regular access reviews, and require MFA for source code repositories.	No Exceptions Noted.
CC6.2	C-OP.40	The full lifecycle of identities, including creation, modification, and de-provisioning, must be managed securely to ensure only legitimate users access organizational resources.	No Exceptions Noted.
CC6.2	C-TC.30	A user's logical (and physical) access to IT systems is revoked within 24 hours of termination or transfer and all assets are returned to the organization when employment ends or their contract terminates. Exceptions are documented in an offboarding checklist and/or offboarding ticket.	No Exceptions Noted.
CC6.3	C-OP.42	Access rights must be provisioned, regularly reviewed, modified, and removed in accordance with organizational access control policies and business requirements.	No Exceptions Noted.
CC6.4	C-PC.1	Physical security perimeters must be appropriately marked. All entry and exit points must be adequately secured with physical access controls, monitored through CCTV, and restricted to authorized personnel only. This includes delivery and loading areas.	No Exceptions Noted.
CC6.4 A1.2	C-PC.2	Adequate security controls must be implemented and maintained for offices, rooms, and other facilities to protect against physical and environmental threats. This includes the secure siting and protection of equipment, secure cabling, and appropriate controls for supporting utilities.	No Exceptions Noted.
CC6.4	C-PC.3	A physical access control system must be implemented to secure facilities. All visitors must enter their details in a visitor logbook, be issued temporary visitor ID cards, and be	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Neurotek	Results of Test
		escorted by a company employee/security. ID cards with employee pictures must be worn at all times, and access must be deactivated upon termination.	
CC6.4	C-PC.9	Physical access to the onsite server room/data center is restricted to authorized individuals only. All new access requests and changes to access permissions are appropriately approved and documented. Management performs at least an annual review of physical user access to the data center. During this review, inactive users are identified and removed, with the removal process being documented. The review is formally documented, including system-generated user listings and sign-off by management to ensure accountability and compliance.	No Exceptions Noted.
CC6.4	C-PC.10	Physical access to the onsite server room is restricted to authorized individuals who have the key; access is approved by the head of IT.	No Exceptions Noted.
CC6.5 C1.2 P4.2 P4.3	C-OP.37	Procedures are in place to remove data from production based on retention schedules, contract requirements, and deletion rules that are applied to specific forms of data; disposals are tracked; a data disposal process is in place. These procedures are reviewed, updated, and approved as needed.	No Exceptions Noted.
CC6.5 CC6.7 C1.2 P4.3	C-TC.10	Ensure secure deletion of information to prevent unauthorized access to residual data.	No Exceptions Noted.
CC6.5 CC6.7 C1.2	C-PC.5	Appropriate controls for the security of assets off-premise and the secure disposal of media once it reaches its end of life must be implemented to ensure information is not leaked.	No Exceptions Noted.
CC6.6 CC9.2	C-OP.13	Cloud security controls must be implemented to ensure secure usage of cloud environments, preventing data leaks and unauthorized access.	No Exceptions Noted.
CC6.6 CC7.1	C-TC.8	Regularly assess and manage vulnerabilities to prevent exploits.	No Exceptions Noted.
CC6.6 CC6.7 C1.1	C-TC.12	Deploy data leakage prevention measures to prevent unauthorized data transfers.	No Exceptions Noted.
CC6.6	C-TC.19	Deploy web filtering controls to prevent access to malicious websites and inappropriate content.	No Exceptions Noted.
CC6.7	C-OP.10	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.	No Exceptions Noted.
CC6.8 CC8.1	C-TC.17	Manage software installation to prevent unauthorized software and ensure system stability.	No Exceptions Noted.
CC6.8 CC7.1 CC7.2	C-TC.29	Threat detection tools are utilized to monitor and log possible or actual network breaches and other anomalous security events. Alerting occurs on threats and results are actioned as appropriate.	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Neurotek	Results of Test
CC7.3 CC7.4 CC7.5	C-OP.14	Incident management controls must be followed to address incidents appropriately, reducing repeated occurrences and improving security.	No Exceptions Noted.
CC7.3 CC7.4	C-HR.9	The company must provide comprehensive training to all employees and contractors on the procedures for reporting security incidents and events. This training should cover the types of incidents that need to be reported, the appropriate channels and contacts for reporting, and the steps to be taken immediately following the discovery of a security incident. The training should emphasize the importance of prompt and accurate reporting to mitigate potential risks and ensure swift resolution. Employees and contractors are required to acknowledge their understanding of the security incident/event reporting procedures. This acknowledgment should be documented and retained in their personnel file. Regular refresher training sessions should be conducted to reinforce the reporting procedures and update personnel on any changes.	No Exceptions Noted.
CC7.4 P6.3 P6.6	C-OP.35	A Data Breach Policy and related procedures are in place. Procedures contain supporting processes to receive, track, address, resolve, and respond to incidents involving user data, and to communicate incidents to affected parties and data subjects. This policy is reviewed, updated, and approved annually.	No Exceptions Noted.
CC7.4 P6.6	C-OP.36	Procedures are in place for breach notification. Procedures include who must be notified, under what circumstances breach notifications must be prepared, the timing of the notification, how the notification is to be sent, and the required elements of the notification.	No Exceptions Noted.
CC7.5 CC9.1 A1.2 A1.3	C-OP.15	ICT readiness and information security must be maintained to ensure immediate recovery and minimal operational disruption.	No Exceptions Noted.
CC8.1	C-TC.24	Development, testing and production environments should be separated and secured to prevent cross-contamination and data leaks.	No Exceptions Noted.
CC9.1	C-OP.16	Business insurance must be in place to ensure financial recovery from incidents or disasters.	No Exceptions Noted.
CC9.2 P6.4	C-OP.30	A policy and procedures are in place which govern the vendor management lifecycle. The policy is reviewed and re-approved by management annually. Procedures are defined for assessing vendor risk.	No Exceptions Noted.
CC9.2 P6.1 P6.4	C-OP.31	Due diligence activities are performed over new vendors and service providers prior to contract execution. Due diligence activities include an assessment of information security practices based on the assessed level of vendor risk.	No Exceptions Noted.
CC9.2 P6.1 P6.4 P6.5	C-OP.32	Critical IT vendors and service providers are annually reviewed to update their risk profiles, assess performance against contracts, re-assess the vendors' security controls, and manage change in supplier information security practices	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Neurotek	Results of Test
		and service delivery.	
CC9.2	C-TC.23	Implement controls for outsourced development to ensure quality and security compliance.	No Exceptions Noted.
A1.1	C-TC.6	Monitor system performance, conduct regular capacity planning, and implement scaling solutions.	No Exceptions Noted.
A1.2	C-TC.13	Maintain regular backups to prevent data loss and ensure quick recovery.	No Exceptions Noted.
A1.2	C-TC.14	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	No Exceptions Noted.
A1.2	C-PC.4	Environmental controls such as fire extinguishers, fire sprinklers, smoke detectors, and UPS devices must be installed and regularly checked. Fire drills must be conducted annually. Mantraps or other physical devices must be used for controlling access to highly sensitive facilities.	No Exceptions Noted.
A1.2	C-PC.7	Facilities, operations, and admin personnel must monitor the status of physical and environmental protections regularly. Maintenance checklists and reports must be used where applicable, including monitoring server room temperature daily and ensuring compliance with vendor warranty specifications.	No Exceptions Noted.
C1.1	C-OP.19	Intellectual property rights must be protected to safeguard valuable organizational assets from unauthorized use.	No Exceptions Noted.
C1.1 P4.1	C-TC.11	Implement data masking to protect sensitive information during testing and development.	No Exceptions Noted.
PI1.5	C-TC.26	Protect test information to prevent unauthorized access and data breaches.	No Exceptions Noted.
P1.1 P2.1 P3.1 P3.2 P4.1 P5.1 P5.2 P6.1 P6.2 P6.7 P7.1	C-OP.21	Controls for the privacy and protection of PII must be implemented to prevent unauthorized access, use, or modification of sensitive information.	No Exceptions Noted.

[End of the report]

◆ CERTIFICAT ◆ CERTIFICADO ◆ СЕРТИФИКАТ ◆ CERTIFICATE ◆ ZERTIFIKAT

CERTIFICATE

This is to Certify that the Management System of

NEURO - TECHNOLOGY SOLUTIONS LTD.

80 Kohav HaYam St., Hofit, Israel

has been found to conform to the Medical Device - Quality Management System standard:

ISO 13485:2016

This certificate is valid for the following scope of operations:

Development of the MOXO(™) Product Suite used in neuropsychological Diagnosis which provides an objective and detailed assessment for ADHD (Attention-Deficit/Hyperactivity Disorder) screening and diagnostic support

:: Certificate No :: IL62998H

Date of initial registration	*Date of this Certificate*	*Surv. audit on or before / Certificate expiry*	*Recertification Due*
30 May 2026	*30 May 2026*	*29 May 2027*	*29 May 2029*

This Certificate remains valid subject to satisfactory surveillance audits.

Director

For verification and updated information concerning the present certificate visit to https://www.staunchlyservices.com/search_certified_client_php

STAUNCHLY MANAGEMENT AND SYSTEM SERVICES LIMITED

International Office: Labrynth Business Centre, 43 Middle Hill Gate, Stockport Great Manchester, England-SK1 3DG
Phone: +44-7404823687
(Company Registered in England with Company Number 11488683

STAUNCHLY MANAGEMENT AND SYSTEM SERVICES PVT. LTD.

Corporate Office: 303, U-60, 3rd Floor Shakarpur, Delhi-110019, India
Phone: +91-6389519394
Web :- www.staunchlyservices.com
E-mail :- info@staunchlyservices.com

EGAC Accredited MSCB CAB # 011804

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT IAF

CERTIFICATE

This is hereby certified that the Health informatics of

NEURO - TECHNOLOGY SOLUTIONS LTD.

80 Kohav HaYam St., Hofit, Israel

Has been found to comply with the requirements of

ISO 27799:2025

This certificate is applicable for the following scope:

Manufacturing of MOXO(™) Product Suite

Certificate Number: KAHIS202605004

Date of initial registration:	29 May 2026
Surveillance audit on/before:	29 April 2027
Certificate Expiry:	29 May 2027
Recertification due:	28 May 2029

Authorised Signatory
KVQA Assesment Pvt. Ltd.

MANAGEMENT SYSTEM CERTIFICATE

Website: www.iso-registration.com | Email: info@iso-registration.com

The certificate is valid subject to successful completion of surveillance audits. Verify validity/status on www.iso-registration.com or on email at info@iso-registration.com