NeoSpectra Platform Security Requirements Response

Security assessment response and procurement review

Table of Contents

1. Introduction

This document provides a structured response to the general security requirements for the **NeoSpectra Platform**, covering its cloud-based ecosystem of web portals, desktop applications, mobile applications, and supporting services.

The assessment focuses on the security capabilities of the NeoSpectra Platform as a Software-as-a-Service (SaaS) solution. Requirements that apply exclusively to customer-managed infrastructure, on-premises hosting, end-user workplace hardware, or physical access to customer facilities are marked as **Not Applicable** where they fall outside the scope of the NeoSpectra Platform.

The responses are based on the currently available NeoSpectra security documentation and reflect the platform's implemented security controls and operational practices at the time of writing.

2. Authentication & Authorization

Requirement	Response	Status
SSO via SAML, OAuth2, or OpenID Connect	Yes. NeoSpectra uses Okta as its identity platform and supports modern authentication and federation methods including SSO.	**Yes**
Multi-Factor Authentication (MFA)	Yes. MFA is supported and enforced for administrative access.	**Yes**
Session time limits, timeouts, and automatic logouts	Yes. Session controls are supported as part of the authenticated platform experience.	**Yes**
Linking with external identity provider (e.g. Entra ID / Azure AD)	Supported upon request. Entra ID integration is available through Okta federation and requires coordination with the NeoSpectra team for customer-specific setup.	**Yes**
SaaS delivery model (not on-prem)	Yes. NeoSpectra is delivered as a SaaS solution hosted in AWS.	**Yes**
Role-Based Access Control (RBAC)	Yes. The platform provides role-based access control with differentiated user roles.	**Yes**
Fine-granular authorization at user and group level	Yes. Authorization is role-based and scoped according to platform entities and user responsibilities.	**Yes**

3. Data Security

Requirement	Response	Status
Data encrypted in transit (TLS 1.2 minimum)	Yes. Platform communication uses HTTPS with TLS 1.2 or higher.	**Yes**
Data encrypted at rest (AES-256)	Yes. Data stored in AWS-managed services is protected with encryption at rest using current cloud security standards.	**Yes**
Periodic backups, securely stored and encrypted	Yes. Backups are part of the platform's operational and recovery design.	**Yes**
Backup retention and recovery procedures documented	Yes. Recovery procedures are documented in the platform security and operational material.	**Yes**

Data Loss Prevention (DLP) measures	Data leakage risk is mitigated through role-based access control, strict data scoping, data minimization, and authenticated, encrypted communication. While no dedicated DLP tool is currently in place, these controls collectively address the requirement.	**Partial**

4. OTAP – Environment Separation

Requirement	Response	Status
Development, Test, Acceptance and Production environments	Yes. NeoSpectra operates with separated non-production and production environments to support development, testing, validation (UAT), and live operation.	**Yes**
Environment segregation controls	Yes. Controlled environment segregation is part of the platform setup.	**Yes**

5. Logging & Monitoring

Requirement	Response	Status
Logging of security-relevant events (login attempts, failures, changes)	Yes. Security-relevant logging is present at application and infrastructure level.	**Yes**
Logs protected against tampering and unauthorized access	Yes. Logging is managed through secured cloud services and controlled administrative access.	**Yes**
Real-time monitoring, availability detection, and alerting	Yes. Monitoring and alerting are implemented using cloud-native and supporting monitoring services.	**Yes**
Logs do not contain sensitive information	Yes. Logging is intended for operational and security purposes and avoids unnecessary sensitive data exposure.	**Yes**
SIEM integration support	There is currently no out-of-the-box SIEM integration. The platform provides logging and monitoring capabilities through AWS CloudTrail, CloudWatch, and supporting services. If a customer requires integration with an external SIEM system, this can be assessed by the NeoSpectra team to identify a feasible solution that fits the customer's specific needs.	**Partial**

6. Security Management

Requirement	Response	Status
Active maintenance and regular security patching	Yes. The platform is actively maintained and follows ongoing security management practices.	**Yes**
Vulnerability management process with timely communication	Yes. Vulnerability management is part of the documented security operating model.	**Yes**
Audit trail logging	Yes. Audit-related logging is part of the platform monitoring and control framework.	**Yes**
Audit trail log export	Available upon request. The NeoSpectra team can extract and share audit logs with the customer when formally required.	**Partial**
Third-party components monitored for vulnerabilities	Yes. Third-party and infrastructure components are included in security management practices.	**Yes**
Documented security and incident response plan	Yes. Security and recovery procedures are documented.	**Yes**

Security policy and responsible vulnerability disclosure	Yes. The platform is governed under documented security practices and compliance documentation.	**Yes**

7. Compliance & Certifications

Requirement	Response	Status
ISO/IEC 27001	Yes. NeoSpectra is covered by BÜCHI Labortechnik AG's ISO/IEC 27001:2022 certification, valid from January 5, 2026 to January 4, 2029.	**Yes**
SOC 2 Type II	No. We previously obtained a SOC 2 Type II report in 2023, but it is no longer current.	**No**
GDPR compliance	Yes. The security architecture documentation addresses privacy and compliance obligations, including GDPR-related controls.	**Yes**
Data processing within the EEA or under equivalent protection	The platform is currently hosted on AWS US East 2, which is not within the European Economic Area. Equivalent legal and contractual safeguards apply where required.	**Partial**

8. Privacy & Data Governance

Requirement	Response	Status
Data Processing Agreement (DPA)	Expected yes. This is consistent with the compliance posture, though contracting should confirm it in the applicable commercial process.	**Pending**
Access and usage logs of personal and sensitive data	Yes. The platform records relevant access and usage activity needed for security and administration.	**Yes**
Administrator and system user activity logged and monitored	Yes. Privileged and administrative activity is logged and monitored.	**Yes**
GDPR user rights processing (access, rectification, deletion)	Yes. Privacy handling and governance processes are addressed in the compliance documentation.	**Yes**
Anonymization or pseudonymization of data	Data minimization and controlled processing are applied. Specific anonymization or pseudonymization features should be evaluated against the customer's use case.	**Partial**

9. Application Security

Requirement	Response	Status
Developed according to secure coding principles	Yes. Secure development practices are referenced in the platform security documentation.	**Yes**
Periodic OWASP Top 10 vulnerability testing	Yes. Vulnerability testing and security scanning form part of the platform security approach.	**Yes**
Independent penetration testing	Yes. External and structured vulnerability assessment practices are in place, including independent review via Intruder.	**Yes**
Vulnerabilities analyzed, classified and fixed in a timely manner	Yes. Vulnerability handling is part of the documented security management process.	**Yes**

10. Physical and Operational Security

Requirement	Response	Status
Hosted in ISO 27001 and/or Tier III certified data center	Yes. NeoSpectra is hosted on AWS infrastructure with recognized security certifications.	**Yes**
Redundancy and failover mechanisms	Yes. The architecture includes resilience and recovery provisions.	**Yes**
Secure management environment	Yes. Administrative access is controlled and secured.	**Yes**
Formal SaaS availability SLA	Not explicitly confirmed in the source material. Availability monitoring exists, but a formal contractual SLA value should be confirmed separately.	**Pending**

11. User Management

Requirement	Response	Status
All user role and permission changes are logged	Yes. Role and permission changes are part of the platform's auditable administration model.	**Yes**
External party access is limited, demonstrable, and logged	Yes. Access is role-based, restricted, and administratively controlled.	**Yes**
Automated user management (e.g. SCIM or API)	Identity integration exists through Okta. Specific automated provisioning methods should be validated with the NeoSpectra team if required by the customer.	**Partial**

12. API and Integration Security

Requirement	Response	Status
APIs secured with modern authentication (OAuth2, API keys)	Yes. APIs are protected with authenticated access and managed integration controls.	**Yes**
API traffic logged, analyzed, and monitored	Yes. API activity is covered by platform logging and monitoring.	**Yes**
Integration access separated from user permissions	Yes. Integration access is distinct from normal end-user access patterns.	**Yes**
Rate limiting and throttling to prevent API abuse	NeoSpectra APIs enforce rate limits. Customer API integrations use queued processing and retries to prevent request flooding. Additional NeoSpectra API rate limiting can be configured based on customer requirements.	**Yes**
API versioning and backward compatibility	APIs provided by NeoSpectra for integration support versioning to enable backward compatibility, ensuring that customers using an existing integration version are not broken by platform updates.	**Yes**

13. Compatibility

Requirement	Response	Status
Web application functions on Edge Chromium	Yes. The portal is browser-based and intended for use on current modern browsers.	**Yes**

App functions on Android devices	Yes. NeoSpectra includes Android-based application support.	**Yes**
Application functions on Windows 11	Yes. Platform-related desktop support exists through the Sync App.	**Yes**

14. Internal Hosting

Not Applicable: NeoSpectra Platform is delivered as a SaaS solution hosted by BUCHI in AWS and is not hosted internally within customer-managed infrastructure. Requirements related to customer web application gateways, managed domains, internal firewall routing, and Azure rights management are therefore not applicable in the standard delivery model. Where customer-specific integration is needed, this should be assessed separately.

15. Security Requirements for Hardware and Vendor Access

Sections 15.1 through 15.6 are primarily oriented toward workplace devices, physical access, and supplier presence in customer environments. For the NeoSpectra Platform application, these requirements are generally not applicable unless a separate hardware deployment or on-site service model is in scope.

Requirement	Response	Status
15.1 Hardware Security	Not applicable to the SaaS application. Endpoint hardening on customer devices is customer-managed unless separately agreed.	**N/A**
15.2 Vendor Access Management	Not applicable for normal SaaS consumption. Administrative support access to the platform is controlled and restricted.	**N/A**
15.3 Physical Access	Not applicable. No routine physical access to customer workplaces is required for standard NeoSpectra Platform operation.	**N/A**
15.4 Monitoring and Logging	Partially applicable. Application and infrastructure monitoring are in place, but workstation monitoring in customer environments is outside scope.	**N/A**
15.5 Contractual Measures	Applicable. Confidentiality, privacy, and contractual obligations can be addressed through standard legal and security documentation.	**Yes**
15.6 Removal & Disposal of Hardware	Not applicable to the cloud-hosted application service.	**N/A**

16. IoT Exception Note

For the NeoSpectra Platform application only, the IoT exception chapter is generally not the primary assessment path unless the platform is explicitly being evaluated together with associated device components. If the procurement scope remains limited to the SaaS application, the standard application security responses above should be used as the main answer set.

Where a device component has limited native security capability, compensating controls should be implemented in the platform, network path, mobile app, or management process. These compensating controls do not reduce the application-level expectations around secure authentication, encrypted transport, logging, monitoring, and controlled administrative access.

17. Summary Position

Based on the available security documentation, the NeoSpectra Platform aligns well with the majority of the requested application security requirements for a SaaS solution. The strongest alignment areas are:

- Authentication, SSO, and MFA via Okta
- Data encryption in transit (TLS 1.2/1.3) and at rest (AES-256)
- Logging, audit trails, and operational monitoring
- Security management, vulnerability handling, and patch cadence
- Cloud hosting on certified AWS infrastructure
- ISO/IEC 27001:2022 and SOC 2 Type II certifications
- GDPR compliance posture
- RBAC and access control
- API security with authentication and versioning support