SECURITY AS A COMPANY VALUE

Paradigm Software Technologies, Inc. DBA Nexelus’ security & compliance principles guide how we deliver our products and services, enabling people to simply and securely access our products.

**Secure Personnel**

Nexelus takes the security of its data and that of its customers seriously and ensures that only vetted personnel are given access to their resources.

* Nexelus contractors and employees undergo background checks prior to being engaged or employed by us in accordance with local laws and industry best practices.
* Confidentiality or other types of Non-Disclosure Agreements (NDAs) are signed by all employees, and contractors.
* We embed the culture of security into our business by conducting employee security training & testing using current and emerging techniques and attack vectors.

**Secure Development**

* All development projects at Nexelus, including software products, support & implementation services follow secure development lifecycle principles.
* All development of new products, tools, and services, and major changes to existing ones, undergo a design review to ensure security requirements are incorporated into proposed development.
* All team members that are regularly involved in any system development undergo periodic training to ensure the highest security standards in the codebase.
* Software development is conducted in line with [OWASP Top 10](https://owasp.org/www-project-top-ten/)recommendations for web application security.

**Secure Testing**

Nexelus deploys third party penetration testing and vulnerability scanning of all Internet facing production systems on a regular basis.

* All new systems and services are scanned prior to being deployed to production.
* We perform periodic penetration testing external penetration testing companies on systems and products to ensure a comprehensive and real-world view of our products & environment from multiple perspectives.
* We perform regular vulnerability security testing of all code, including 3rd party libraries, as part of our software development process.

**Cloud Security**

Nexelus provides maximum security for cloud architecture. Nexelus Cloud leverages the native physical and network security features of the cloud service, and relies on the providers to maintain the infrastructure, services, and physical access policies and procedures.

* All data is also encrypted in transmission to prevent any unauthorized access and to prevent data breaches. Our entire platform is also continuously monitored by dedicated, highly trained Nexelus experts.
* Client’s data protection complies with SOC 2 standards ensuring customer and company data is always protected.
* We implement role-based access controls and the principles of least privileged access, and review/-revoke access as needed.

**Compliance**

Nexelus is committed to providing secure products and services to many customers across the globe. Our external certifications provide independent assurance of Nexelus’ dedication to protecting our customers by regularly assessing and validating the protections and effective security practices that Nexelus has in place.

**SOC 2 Type 1**

Paradigm Software Technologies, Inc. DBA Nexelus successfully completed the AICPA Service Organization Control (SOC) 2 Type I audit. The audit confirms that Paradigm Software Technologies, Inc. DBA Nexelus’ information security practices, policies, procedures, and operations meet the SOC 2 standards for security, confidentiality and availability.

Nexelus was audited by [Prescient Assurance](https://www.prescientassurance.com/) , a leader in security and compliance certifications for B2B and SAAS companies worldwide. Prescient Assurance is a registered public accounting in the US and Canada and provide risk management and assurance services which includes but not limited to SOC 2, PCI, ISO, NIST, GDPR, CCPA, HIPAA, CSA STAR etc. For more information about Prescient Assurance, you may reach out to them at [info@prescientassurance.com](mailto:info@prescientassurance.com)

An unqualified opinion on a SOC 2 Type I audit report demonstrates to Nexelus’ current and future customers that they manage their data with the highest standard of security and compliance. Customers can request access to the audit report by contacting [support@nexelus.net](mailto:support@nexelus.net)

**SOC 2 Type 2**

Carrying on its mission to embed all the practices and procedures that are in-line with the Service Organization Control Type 2 (SOC 2) and Nexelus business goals, Nexelus earned SOC 2 Type II compliance in 2023. The company has secured operations that totally align with the requirements of SOC 2, which includes establishing, implementing, operating, monitoring, reviewing, maintaining, and improving security procedures and policies. By operating in such an environment, we ensure that we protect the information of our clients, supplier, staff, or any given interested business party.

Nexelus was audited by [Prescient Assurance](https://www.prescientassurance.com/), a leader in security and compliance certifications for B2B and SAAS companies worldwide. Prescient Assurance is a registered public accounting in the US and Canada and provide risk management and assurance services which includes but not limited to SOC 2, PCI, ISO, NIST, GDPR, CCPA, HIPAA, CSA STAR etc. For more information about Prescient Assurance, you may reach out to them at [info@prescientassurance.com](mailto:info@prescientassurance.com)

Achieving SOC 2 Type 2 compliance has helped Nexelus to:

* Develop consistency in providing its products and services to its clients.
* Demonstrate our design, transition, delivery, and improvement of services to ensure reliability and high quality of service.
* Provide assurance to our customers, through industry standard processes and procedures, that all their service requirements will be fulfilled in an efficient and secure manner.
* Provide assurance to customers that their financial and business data is completely secure and protected using stringent industry standard security controls.

 