SYSTEM DESCRIPTION

Table of Contents

1. Company Background.

Nuclei, Inc. ("Nuclei") is a privately held company established in January 2019 that provides a comprehensive platform enabling capture, analysis, and archival of human communication. Nuclei democratizes access to data and helps empower organizations to understand and leverage their data to improve business outcomes while mitigating risks.

Nuclei is a Delaware corporation headquartered in Holmdel, New Jersey, USA.

2. Services Provided.

Nuclei provides customers with a comprehensive, cloud-native platform that enables capture, analysis, and archival of human communication across various communication modalities, including customer engagement, meeting applications, messaging applications, social media, video marketing, voice communication platforms, and more.

The Nuclei Compliance Platform is composed of the following components:

- **Nuclei AI**: A broad set of machine learning services and supporting cloud infrastructure, enabling:
  - Automatic audio transcription for rapid discovery and search
  - Automatic language translation of text-based communications
  - Automatic classification of text-based communications
- **Nuclei Capture**: A highly scalable platform designed to capture, enrich, and consolidate data from a wide range of sources, enabling seamless data portability and providing a single pane of glass for monitoring and surveillance of communication data.
- **Nuclei Recording**: A Microsoft Teams recording application that automatically records voice and video communications within Microsoft Teams, ensuring compliance with regulatory and legal requirements.
- **Nuclei Archive**: A comprehensive platform designed to help organizations meet regulatory and legal requirements for preserving and storing electronic communications, providing long-term storage, search, retrieval, and management of archived data.
- **Nuclei Surveillance**: A real-time monitoring and surveillance platform that uses advanced analytics and artificial intelligence to identify and flag potential compliance violations, proactively detecting and preventing compliance issues before they occur.

Our services are used primarily by organizations operating in highly regulated industries (financial services) to identify risks, meet their record keeping requirements, and to maintain the highest levels of regulatory compliance.

3. Principal Service Commitments and System Requirements.

Nuclei designs its processes and procedures related to the platform with the aim of meeting its objectives, which are rooted in service commitments made to customers, adherence to applicable laws and regulations, and the financial, operational, and compliance requirements that Nuclei has established for its services. Our comprehensive platform, including Nuclei Capture, Nuclei Recording, Nuclei Archive, and Nuclei Surveillance, is developed to align with our mission of unlocking access to valuable knowledge and data through seamless capture, archival, and analysis of human communication. The platform services are subject to the Security, Confidentiality, and Availability commitments established internally to ensure the highest levels of customer satisfaction, regulatory compliance, and protection of sensitive data.

Nuclei communicates our system and service commitments to customers through various channels, ensuring transparency and clarity in our offerings. The key channels we use to convey our commitments include:

- **Service Level Agreements (SLAs)**: We establish clear SLAs that outline our performance standards, availability, and support commitments. The SLAs are shared with customers during the onboarding process and are incorporated into our contractual agreements.
- **Product Documentation**: Comprehensive product documentation, including user guides, feature descriptions, and technical specifications, is made available to customers through our online knowledge base. This documentation provides detailed information on the capabilities, functionality, and performance of our platform components.
- **Sales and Marketing Materials**: Our sales and marketing materials, such as brochures, case studies, and presentations, highlight the benefits of our platform, its features, and the value it brings to customers in meeting their compliance and data analysis needs.
- **Customer Support**: Our dedicated customer support team is available to assist customers with any questions or concerns they may have about our services, ensuring that they have a clear understanding of our system and service commitments.
- Training and Webinars: We offer training sessions and webinars to educate customers on the functionality and capabilities of our platform, as well as best practices for using our services to achieve their desired business outcomes.

By utilizing these channels, we ensure that our customers have a thorough understanding of our system and service commitments, enabling them to make informed decisions and derive maximum value from our platform.

3.1. Security Commitments.

Nuclei's security commitments encompass the following measures:

- System features and configuration settings designed to authorize user access while preventing unauthorized users from accessing information beyond their role requirements.
- Utilization of intrusion detection systems to identify and prevent potential security attacks originating outside the system boundaries.
- Conducting regular vulnerability scans across the system and network, as well as penetration tests within the production environment.
- Implementing operational procedures for managing security incidents and breaches, including established notification procedures.
- Employing encryption technologies to safeguard customer data both in transit and at rest.
- Adhering to data retention and disposal policies.
- Ensuring the uptime and availability of production systems.

3.2. Confidentiality Commitments.

Nuclei's confidentiality commitments comprise the following:

- Employing encryption technologies to secure system data, both at rest and in transit.
- Establishing confidentiality and non-disclosure agreements with employees, contractors, and third parties.
- Ensuring that confidential information is used solely for purposes explicitly stated in agreements between Nuclei and user entities.

3.3. Availability Commitments.

Nuclei's availability commitments include:

- Utilizing system performance and availability monitoring mechanisms to maintain consistent delivery of the platform and its components.
- Responding to customer requests in a reasonably timely manner.
- Developing and maintaining business continuity and disaster recovery plans that encompass detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities.
- Implementing operational procedures that support the achievement of availability commitments to user entities.

4. Components of the System.

The System description is comprised of the following components:

- **Software**: The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- **People**: The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- **Data**: The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- **Procedure**s: The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

4.1. Infrastructure.

The Nuclei Compliance Platform is deployed as a multi-tenant, software as a service architecture. Nuclei's application infrastructure is hosted on Amazon Web Services (AWS) or Microsoft Azure, which provide scalable computing capacity on cloud infrastructure as sub-service organizations.

Each subservice organization provides the physical security, network security, and environmental protection controls, as well as managed services for Nuclei's infrastructure. Each subservice organization provides network security using advanced network firewalls and other network security capabilities.

Nuclei does not operate physical servers or other types of infrastructure. All services in AWS are serverless, and do not include virtual servers or related infrastructure. All services in Microsoft Azure (Microsoft Teams Recording) are run in a managed Kubernetes environment with standard Docker images provided by Microsoft.

4.2. Software.

Nuclei maintains an inventory of critical software in use within its organization and production environments, which includes the following:

Primary Software	Purpose
AWS API Gateway	API gateway services for our serverless infrastructure
AWS DynamoDB	Database services for our infrastructure
AWS Lambda	Runtime for our serverless infrastructure
AWS GuardDuty	Security application used for automated intrusion detection (IDS)
AWS S3	Storage services for our infrastructure
AWS Secrets Manager	Secrets management for our production infrastructure
AWS SES	Email delivery services for our infrastructure
AWS SQS	Simple queue services for our serverless infrastructure
Azure Blob Storage	Storage services for our Microsoft Teams Recording infrastructure
Azure Kubernetes Services	Runs and managers our Microsoft Teams Recording infrastructure
Checkr	Background checks for prospective and current Nuclei employees
GitHub	Version control and code hosting
Google Workspace	Identity and access management. Productivity and collaboration
Gusto	Payroll and human resources automation
Hubspot	Customer relationship management
Linear	Agile tools and workflow collaboration
Lumigo	Cloud-based application monitoring
Slack	Collaboration tool
Stripe	Payment processing API
Vanta	Automated surveillance of our organizational and endpoint compliance with information security controls
Zendesk	Customer communications

4.3. People.

The Nuclei organization is structured into several functional teams, each responsible for specific aspects of our business operations and services. These teams collaborate to ensure the seamless delivery of our platform and maintain the high standards of customer satisfaction and regulatory compliance that we strive for.

- **Executive Leadership**: Responsible for setting the vision, mission, and values of Nuclei, as well as overseeing the strategic direction, governance, and compliance of the organization.
- **Compliance**: The Compliance team oversees adherence to applicable laws, regulatory requirements, norms and industry best practices. They collaborate with other teams to ensure that our platform and services remain compliant, and they provide guidance on legal matters affecting our operations and services.
- **Customer Experience**: This team provides exceptional support and assistance to our customers. They help with onboarding, training, issue resolution, and platform optimization, ensuring that customers can fully leverage the benefits of our platform and achieve their desired outcomes.
- **Design**: The Design team is responsible for designing the platform architecture, application interface, and overall user experience of our platform. They collaborate closely with the Engineering team to ensure that our platform is well designed, visually appealing, and easy to use.
- **Engineering**: This team is responsible for the development, maintenance, and ongoing improvement of our platform components, including Nuclei Capture, Nuclei Recording, Nuclei Archive, and Nuclei Surveillance. They work closely with customers, stakeholders, and other teams to ensure that our products meet the evolving needs of our clients and stay up to date with industry trends and regulatory requirements.
- **Growth**: The Growth team focuses on promoting our platform and services to potential customers, as well as maintaining and strengthening relationships with existing clients. They develop sales and marketing materials, conduct market research, and identify opportunities for growth and expansion.
- **Operations**: This team manages the day-to-day operations of our organization, including financial management, human resources, and administrative functions. They ensure that our business runs smoothly and efficiently while supporting the growth and success of our company.
- **Partnerships**: The Partnerships team is responsible for establishing and maintaining strategic relationships with industry partners, vendors, and other stakeholders. They work closely with other teams to identify opportunities for collaboration and integration that can enhance the value and capabilities of our platform.
- **People**: The People team oversees talent acquisition, employee development, and company culture. They focus on attracting, retaining, and nurturing top talent to ensure that our organization has the skills and resources necessary to achieve our mission and strategic objectives.

By organizing our teams in this manner, we can effectively meet the diverse needs of our customers and maintain a high level of operational efficiency, product quality, and regulatory compliance across our organization.

4.4. Data.

Nuclei defines Customer Data as the electronic data or information submitted by the Customer or Authorized Parties to Nuclei's service. Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements. Customer Data is utilized by Nuclei in delivering its services. Customer Data is stored according to industry best practices, and access to said data is restricted to employees whose job function requires it and in accordance with Nuclei's Privacy Policy and Terms of Use.

The Nuclei platform collects various types of data to effectively capture, archive, and analyze human communication across multiple channels. The following are the primary data types collected by our product and a brief description of each, along with information on where they are stored in our system:

- **Communication Data**: This includes text, voice, and video communications from various sources such as customer engagement, meeting applications, messaging applications, social media, video marketing, and voice communications. Communication data is captured and enriched by Nuclei Capture and stored in our secure, cloud-based data storage system, ensuring seamless portability and access for monitoring and surveillance.
- **Meta Data**: Meta Data refers to contextual information about the communication data, such as timestamps, sender and receiver details, conversation threads, and unique identifiers. This data is crucial for effective organization, analysis, and retrieval of communication records. Meta Data is also stored in our secure, cloud-based data storage system, alongside the associated communication data.
- **User Data**: This includes information about the users of our platform, such as names, email addresses, job titles, and organizational affiliations. User data is essential for managing access controls, personalizing user experiences, and providing relevant insights and analytics. User data is securely stored in our cloud-based user management system.
- **Archived Data**: Nuclei Archive stores long-term communication records and Meta Data to meet regulatory and legal requirements for preserving and storing electronic communications. Archived data is securely stored in our cloud-based storage system, with access controls and encryption measures in place to protect data integrity and confidentiality.
- **Compliance Violation Alerts**: These are generated by Nuclei Surveillance when potential compliance violations, such as insider trading or market manipulation, are identified. The alerts contain information about the suspected violation, including the relevant communication data, involved parties, and a summary of the suspicious activity. Compliance violation alerts are stored in a dedicated database within our secure cloud infrastructure, accessible only to authorized personnel.
- **Application Logs**: This includes application logging from the various services that together compose the Nuclei Compliance Platform.

By collecting and managing these types of data, our platform enables organizations to effectively monitor, analyze, and maintain compliance with regulatory requirements while leveraging their communication data to drive business outcomes.

All data managed, processed, or stored by Nuclei is subject to the following internal classification system:

Category	Description	Examples
Confidential	Highly sensitive data requiring the highest levels of protection; access is restricted to specific employees or departments, and these records can only be passed to others with approval from the data owner, or a company executive.	Customer data Company financial data Source code
Internal	Nuclei proprietary information requiring thorough protection	Legal documents Meeting minutes Slack message E-mail
Public	Documents intended for public consumption which can be freely distributed outside Nuclei	Marketing materials Product descriptions Release notes

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by the company in delivering its services.

All employees and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Nuclei has policies and procedures in place to proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

4.5. Processes and Procedures.

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

4.5.1. Physical Security

Nuclei's office buildings include publicly accessible reception areas with on-site, armed security guards 24x7. The office entrance is secured by keycard access. Visitors are required to be registered with on the building's guest list and confirmed by building staff members. Visitors are issued a temporary ID badge to be worn throughout their visit and are required to be escorted at all times while they are in the office.

AWS and Microsoft Azure, as the sub-service organization providing hosting services, are responsible for implementing physical security controls over their respective data centers for in-scope systems. Nuclei reviews the attestation reports and performs a risk analysis for each sub-service organization on an at least annual basis.

4.5.2. Logical Access

Nuclei provides employees and contractors access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and reportable user provisioning and deprovisioning processes.

Access to these systems are split into admin roles, user roles, and no access roles. User access and roles are reviewed on a quarterly basis to ensure least privilege access.

Asset owners are responsible for provisioning access to the system based on the employee's role. The Compliance team is responsible for completing background checks on our prospective and current employees. Employees are responsible for reviewing Nuclei's policies and completing all required security trainings. These steps must be completed within 72 hours of hire.

When an employee is terminated, Asset owners are responsible for deprovisioning access to all in scope systems within 1 business day for that employee's termination, under the supervision of the Compliance team.

4.5.3. Computer Operations – Backups

Customer data is continuously protected and monitored by the Engineering team, utilizing DynamoDB Point-in-Time Recovery (PITR) and Amazon S3's versioning and compliance mode features. These technologies ensure data protection and preservation against accidental deletion or application errors. In case of any exceptions, the Engineering team will perform troubleshooting to identify the root cause and take the necessary steps to restore the data using the available backup technologies.

The backup infrastructure is maintained across Microsoft Azure and AWS, with access restricted according to the Operations Security and related policies. This multi-cloud approach enhances the security and resilience of our data backup and recovery processes.

4.5.4. Computer Operations – Availability

Nuclei maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting, and acting upon breaches or other incidents.

Nuclei internally monitors all applications, including the web UI, application runtime environment, databases, and cloud storage to ensure that service delivery matches SLA requirements.

Nuclei utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

4.5.5. Change Management

Nuclei maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

4.5.6. Data Communications

Nuclei has chosen to adopt a serverless architecture for its production infrastructure, which eliminates the complexity of network monitoring, configuration, and related operations. This approach cripples traditional attack vectors that are used to exploit other applications and streamlines our logical network configuration by leveraging the AWS Shared Responsibility Model for security in the cloud. This model ensures that AWS is responsible for the security of the underlying cloud infrastructure, while Nuclei is responsible for securing the data and application components hosted within the AWS environment.

The serverless architecture also automates the provisioning and deprovisioning of resources to align with the desired configuration. In the event of an application component failure, whether due to the application itself or underlying hardware, the architecture ensures the automatic replacement of the affected component in real-time. This enhances the overall resilience and reliability of our platform.

For select services that run in Microsoft Azure (Microsoft Teams Recording), Nuclei has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the Nuclei application containers, with the only ingress from the network via HTTPS connections to designated endpoints.

The PaaS provider also automates the provisioning and deprovisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on underlying hardware.

Our process for identifying new vulnerabilities is comprehensive and combines automated scanning tools, regular vulnerability scans, and external assessments to ensure the security of our systems and infrastructure.

- Automated Scanning Tools: We use Dependabot and other related technologies to automatically scan our codebase and dependencies for known security vulnerabilities. These tools help us identify and remediate vulnerabilities in real-time by providing notifications and suggesting updates or patches when necessary.
- Regular Vulnerability Scans: We continuously monitor our systems and infrastructure for potential security vulnerabilities using GitHub Dependabot, an industry-standard scanning tool integrated with our GitHub repositories. Dependabot automatically identifies outdated or insecure dependencies and creates pull requests to update them, ensuring that our software remains secure and up to date. By leveraging GitHub Dependabot's automated scanning capabilities, we gain actionable insights for improving our overall security posture and maintain the integrity of our systems.

- External Assessments: In addition to our internal vulnerability management processes, we engage third-party security firms to conduct annual penetration tests. These external assessments help us identify and address potential security vulnerabilities from an outsider's perspective, ensuring that our systems remain resilient against potential attacks.
- Cross-functional Security Collaboration: Our approach to security involves coordinating resources across the Executive Leadership, Compliance, and Engineering teams. These teams collaborate closely to review vulnerability reports and prioritize remediation efforts. By fostering cross-functional collaboration, we ensure that security vulnerabilities are addressed promptly, and our systems remain secure and compliant.

By combining these processes, we maintain a robust vulnerability detection and remediation program that helps us stay proactive in addressing potential security threats and ensuring the ongoing security and integrity of our platform and customer data.

4.5.7. Risk Assessment

Our organization conducts regular risk assessments to identify, analyze, and evaluate potential threats and vulnerabilities within our systems and infrastructure. This process helps us prioritize risks based on their likelihood and potential impact, allowing us to make informed decisions about implementing appropriate controls and mitigation strategies. Risk assessments are performed at least annually or whenever significant changes occur in our environment, ensuring that our risk management approach remains effective and up-to-date.

4.5.8. Data Retention

We have established data retention policies and procedures to ensure that customer data is securely stored and retained only for as long as necessary to fulfill the purposes for which it was collected. Our data retention policy outlines the specific retention periods for various types of data, taking into account legal, regulatory, and operational requirements. We perform regular audits to verify compliance with our data retention policies, and any data that is no longer required is securely deleted or anonymized in accordance with industry best practices.

4.5.9. Vendor Management

Our organization is committed to maintaining a robust vendor management program to ensure that third-party service providers meet our security and compliance requirements. We conduct thorough due diligence on potential vendors, evaluating their security controls, certifications, and track records before entering into any agreements. Throughout our relationships with vendors, we monitor their performance and adherence to our security standards, conducting periodic reviews and assessments as necessary. This approach enables us to maintain a secure and compliant supply chain and effectively manage risks associated with outsourcing critical services.

4.5.10. Boundaries of the System

The boundaries of the Nuclei Compliance Platform are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Nuclei Compliance Platform.

5. Control Environment.

5.1. Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Nuclei's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Nuclei's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process to the extent permitted by applicable law.

5.2. Commitment to Competence

Nuclei's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

5.3. Management's Philosophy and Operating Style

The Nuclei management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly-sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way Nuclei can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Nuclei to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

5.4. Organizational Structure and Assignment of Authority and Responsibility

Nuclei's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Nuclei's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

5.5. HR Policies and Practices

Nuclei's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Nuclei's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

5.6. Risk Assessment Process

Nuclei's risk assessment process identifies and manages risks that could potentially affect Nuclei's ability to provide reliable and secure services to our customers. As part of this process, Nuclei maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are

incorporated into the regular Nuclei product development process so they can be dealt with predictably and iteratively.

5.7. Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Nuclei's system; as well as the nature of the components of the system result in risks that the criteria will not be met. Nuclei addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Nuclei's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

5.8. Information and Communication Systems

Information and communication are an integral component of Nuclei's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

Nuclei uses several information and communication channels internally to share information with management, employees, contractors, and customers. Nuclei uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, Nuclei uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

5.9. Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Nuclei's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

5.10. On-going Monitoring

Nuclei's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Nuclei's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Nuclei's personnel.

5.11. Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective

actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

5.12. Changes to the System

There have been no significant changes that have impacted our business. Nuclei has not undergone any acquisitions, mergers, or major changes to our system environment, such as switching key vendors. Our focus has been on maintaining the stability and security of our platform, while continuously working to enhance our product offerings and provide the best possible experience to our customers.

5.13. Incidents

There have been no significant security incidents in our organization. This includes any breaches or leaks of data or major security incidents. We remain committed to maintaining a strong security posture and continuously investing in measures that protect our platform, customer data, and overall system integrity.

5.14. Criteria not applicable to the System

All Common Criteria/Security, Security, Confidentiality, and Availability criteria were applicable to the Nuclei Compliance Platform system.

5.15. Subservice Organizations (aka Sub-Processors)

This report does not include the Cloud Hosting Services provided by AWS and Microsoft Azure at multiple facilities.

5.16. Subservice description of services

The Cloud Hosting Services provided by AWS and Microsoft Azure support the physical infrastructure of the entity's services.

6. Complementary Subservice Organization Controls.

Nuclei's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Nuclei's services to be solely achieved by Nuclei control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Nuclei.

The following subservice organization controls have been implemented by Microsoft Azure and AWS, and are included in this report to provide additional assurance that the trust services criteria are met.

6.1. Azure

Category	Criteria	Control
Security	CC 6.4	Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established.
Security	CC 6.4	Security verification and check-in for personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors, are required.
Security	CC 6.4	Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
Security	CC 6.4	Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
Security	CC 6.4	The datacenter facility is monitored 24x7 by security personnel.
Availability	A 1.2	Datacenter Management team maintains and tests data center managed environmental equipment within the facility according to documented policy and maintenance procedures.
Availability	A 1.2	Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.

6.2. AWS

Category	Criteria	Control
Security	CC 6.4	Physical access to data centers is approved by an authorized individual.
Security	CC 6.4	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
Security	CC 6.4	Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
Security	CC 6.4	Closed circuit television camera (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
Security	CC 6.4	Access to server locations is managed by electronic access control devices.
Availability	A 1.2	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment.
Availability	A 1.2	AWS has a process in place to review environmental and geo-political risks before launching a new region.
Availability	A 1.2	Amazon-owned data centers are protected by fire detection and suppression systems.

Availability	A 1.2	Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
Availability	A 1.2	Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon owned data centers
Availability	A 1.2	Amazon-owned data centers have generators to provide backup power in case of electrical failure.
Availability	A 1.2	Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies. Contracts also include provisions requiring communication of incidents or events that impact Amazon assets and/or customers to AWS.

Nuclei management, along with the subservice provider, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Nuclei performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organization(s)
- Making regular site visits to vendor and subservice organization(s') facilities
- Testing controls performed by vendors and subservice organization(s)
- Reviewing attestation reports over services provided by vendors and subservice organization(s)
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

7. Complementary User Entity Controls.

Nuclei's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to Nuclei's services to be solely achieved by Nuclei control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Nuclei's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

- User entities are responsible for understanding and complying with their contractual obligations to Nuclei.
- User entities are responsible for notifying Nuclei of changes made to technical or administrative contact information.
- User entities are responsible for maintaining their own system(s) of record.
- User entities are responsible for ensuring the supervision, management, and control of the use of Nuclei services by their personnel.

- User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Nuclei services.
- User entities are responsible for providing Nuclei with a list of approvers for security and system configuration changes for data transmission.
- User entities are responsible for immediately notifying Nuclei of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

8. Responsibility & Approval.

It is the responsibility of Compliance to ensure this Service Description is continuously updated. The CEO approved this Service Description at the revision date indicated below.