Kleene

ISMS Policy V3

29 August 2024

Purpose of the ISMS

This document is designed to provide an overview of the Information Security Management System (ISMS) Kleene AI has been put in place in order to assure the integrity, availability and confidentiality of our own and our suppliers' and clients' information.

The ISMS as a whole comprises various policies, plans & reports, and operational procedures, for example: the Information Security Policy, the Business Continuity Plan and the Risk Assessment Standard.

This Overview acts as the framework that brings all these components together to form a single cohesive management system. It provides a summary of the ISMS and refers to specific, more detailed, documents where appropriate (e.g. the Business Continuity Plan).

Information Security Objectives

The following objectives support the ISMS:

ISMS Objectives

Objective	Ownership	Measurement
Maintain ISO 27001 certification	Chief Executive Officer	Recommended for certification to ISO 27001
Enhance risk management processes	Chief Executive Officer	Risk register contents - what is reported, how is it assessed and timeframe for mitigation
Strengthen third-party and supplier management	Chief Operations Officer	Completed annual review of critical suppliers
Improve incident detection and response	Chief Executive Officer	Incident Register contents - what is reported, treatment plan and timeframe until resolution
Expand and deepen employee security training and awareness	Chief Operations Officer	Completion rates of security training and number of reported phishing or social engineering attempts by employees

External and Internal Issues

Please see PESTLE Analysis.

This section identifies internal and external issues that are relevant to the organization and can negatively impact the ability to achieve objectives of the organization. There is a close link between these issues and risk identified in the Risk Assessment. The analysis of these issues should include the following:

1. How the scope of the ISMS is impacted
2. Context of the issues to determine the risks and opportunities; and
3. Adapting the ISMS to changing internal and external issues

Internal Issues

The organization has identified the following dependencies and other factors that may contribute to an increase or decrease in issues. These include:

1. Major organizational changes
2. Business Continuity related issues
3. Mergers and acquisitions
4. Failure of ISMS or an inability to maintain operational security controls
5. Lack of management commitment to security and other operational best practices
6. Consistent issues identified as part of the ISMS Management Reviews.

External Issues

The external environment in which the organization operates inherently includes a number of possible factors that can create uncertainty in the amount of external issues. As such there are dependencies and other factors that may contribute to an increase or decrease in issues. These include:

1. Supply chain
2. Strategic Partners
3. Regulatory changes
4. Changes to standards of operation

These internal and external issues are reviewed regularly (at least annually) as part of the risk assessment process because both the internal and external issues will change over time and their influence on the scope, constraints, and requirements of the ISMS may be impacted.

Interested Parties

Internal and external parties have been identified, which might impact upon the ISMS’s ability to deliver its intended results, or those that might influence Kleene AI’s strategic direction. These interested parties are both internal and external as follows:

- Internal - founders, senior management and advisory board, employees and contractors
- External - investors and shareholders, suppliers, contractors, customers, competitors, and regulators

Please see interested parties register.

These identified interested parties generate the following requirements:

1. Operate in accordance with applicable and relevant laws where Kleene AI operates
2. Implement ISO 27001 frameworks best practices to further strengthen its ISMS efforts.
3. Obtain and maintain ISO 27001 certifications
4. Maintain availability of the CUSTOMER’s platform
5. Ensure accuracy of the methodology used by Kleene AI in the provision of its product
6. Continued development and growth of the company
7. Protection of the reputation of Kleene AI as a company and its product
8. Periodic review by the Information Security Team regarding the needs and expectations of interested parties.

Communication and Management Commitment

The ISMS is annually approved by management and published and communicated to all Employees and relevant external parties bound to a Mutual Non-Disclosure Agreement. This ISMS is available to appropriate users, in a form that is relevant, accessible and understandable to the intended reader.

This Policy demonstrates the commitment of executive management to the Information Security Program documented within the ISMS.

It is mandatory that all Kleene AI Employees and Vendors adhere to this ISMS and the policies, procedures, standards, guidelines, and processes derived from this

Policy. The Kleene AI ISMS and supporting policies and procedures include all information technology, virtual and physical systems and facilities used in connection with the Assets. The details set out in this document, while comprehensive, are not exhaustive and are provided for guidance.

If you are unsure of whether a contemplated use or action is permitted, it is your responsibility to determine whether the use is allowed by checking with your line manager and contacting the owner of the ISMS.

Compliance

Kleene AI establishes a baseline for its Information Security Policies from the ISO 27001 framework.

Additionally, the ISMS, Policies, and Procedures were designed with industry security standards in mind and often exceed those standards including OWASP and meeting or exceeding the legal, statutory, and regulatory compliance obligations.

ISMS Scope

Information Security Roles and Responsibilities

The implementation of this Policy and Information Security Program requires a clear definition of security roles and responsibilities. Kleene AI establishes and maintains the Information Security Program for managing information security across the Kleene AI Information Security Program including this Policy, Kleene AI policies and procedures and Kleene AI System-Specific (“Product” or “Application”) Information Security policies and procedures.

ISMS Roles and Responsibilities

Ownership and Enforcement

The COO is the owner of this policy and is responsible for its approval. The COO in conjunction with a member of the Kleene AI Risk Committee approves any exceptions to this policy.

Kleene AI must have an organizational structure that establishes, approves, implements, and monitors adherence to an Information Security Program through clear lines of authority and responsibilities. Every Employee and Vendor is responsible for identifying and mitigating risks associated with the protection of Confidential Information, and must comply with additional policies that support this Policy including, but not limited to:

- Information Security Policy
- Configuration and Change Management Policy
- Data Protection and Handling Policies
- Incident Response Policy and Plan
- Supplier Risk Management Policy
- Hiring Policy

Additionally, in conjunction with this Policy, based on Employee's and Vendor's level of access, job duties, and scope of work is required, where applicable, Employees and Vendors must comply with the following Kleene AI System-Specific (“Product” or “Application”) Information Security policies and procedures; that are applicable to Customer Information:

- Configuration and Change Management Policy includes Operating System, and Change Management Procedures
- Software Development Life Cycle Policy that includes QA process 🎯 QA Process, System and component architecture.
- Business Continuity & Disaster Recovery Plan

Maintenance of Policies

The COO has responsibility for the development, maintenance and updating of this Policy and Information Security Program policies and procedures including Kleene AI System-Specific (“Product” or “Application”) Information Security policies and procedures (hereby referred to as “Governance Set”) to ensure relevance, quality and completeness.

Requests for Change ("RFC") are reported to the COO, which is responsible for analyzing the impact of the change from the business, security and financial perspectives. Significant changes approved by the Kleene AI Information Security Team will be sent to the COO or an approved delegate for review prior to implementation.

Review of Policies

The COO and the Kleene AI Information Security Team will review and approve this Policy and all Kleene AI Information Security Program policies and procedures including Kleene AI System-Specific (“Product” or “Application”) Information Security policies and procedures (hereby referred to as “Governance Set”) at least annually.

Security Principles

Kleene adopts the following core security principles to ensure the protection of its information assets:

1. **Confidentiality**: Ensuring that information is accessible only to those authorised to have access. This principle protects against unauthorised disclosure of information.
2. **Integrity**: Safeguarding the accuracy and completeness of information and processing methods. This principle protects against unauthorised alteration or destruction of information.
3. **Availability**: Ensuring that authorised users have access to information and associated assets when required. This principle protects against disruptions to business operations.
4. **Accountability**: Ensuring that actions can be traced back to the responsible entity. This principle ensures that users are held responsible for their actions and helps in tracking activities.
5. **Non-repudiation**: Ensuring that a party cannot deny the authenticity of their signature on a document or a sent message. This principle helps in establishing trust and accountability.

6. **Authenticity**: Ensuring that information is genuine and from a verified source. This principle helps in preventing fraud and ensures trustworthiness.
7. **Reliability**: Ensuring that the information and services are dependable. This principle ensures consistent and dependable performance of information systems.

Planning/Risk Assessment

Kleene AI has established and maintains a program for managing Information Security across the company. Within this program, management sets the framework, approves the ISMS and policies, procedures, standards, guidelines, and processes derived from this system, assigns roles for implementing the program, and ensures that Kleene AI keeps its ISMS current and in compliance with relevant laws, regulations, and standard industry practices.

Information Security Policy Framework

The framework used to develop the Information Security Policy (“Policy”) describes the hierarchical structure of the Policy on Information Security as illustrated below. This framework is based on ISO regulatory and compliance requirements.

Information Technology Risk Management Framework and Security Program

Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.

Kleene AI has established a comprehensive Risk Management framework providing the organization with a central platform spanning the risk criteria across the organization. This framework, continuously reviewed and updated, shall allow Kleene AI to identify and categorize risks associated with the information system as well as risks across the organization, categorize these risks using an established risk rating system developed interdepartmentally, and mitigate the risks to the organization using existing controls mapped to risks or creating tasks to mitigate risks discovered in the assessment phase. This framework is detailed in the Kleene AI Compliance and Risk Management Policy and is authorized by management.

The COO and Information Security Team drives the Information Security Program. IT Risk Management shall align with the direction provided by the Risk Committee and manage risk in accordance with the Kleene AI Compliance and Risk Management Policy. See the Roles & Responsibilities matrix for more.

The primary objectives of the Risk Committee are to:

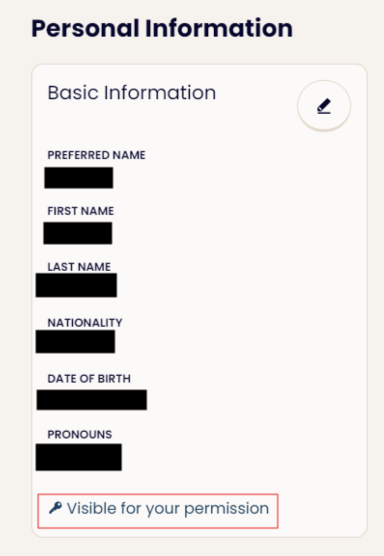
- Identify, assess, respond, report and monitor on IT risk across Kleene AI;
- Assess existing policies and procedures that address specific risk areas;
- Safeguard the continuity of the business;
- Conduct an annual risk assessment; and
- Promote effective communication of IT risk.

Metrics:

1. Keep number of employees trained for Security Awareness at 100%
2. Treat all Critical Risks within 30 days of identification
3. Treat all Major Risks within 60 days of identification
4. Treat all Significant Risks within 90 days of identification
5. Treat all Minor risks within 120 days of identification
6. Obtain and maintain ISO 27001 certificate

Data Masking

Kleene uses a HR software system to administer and process employee PII related to their employment. This system provides out of the box data masking on PII and other important employee data, restricting automatically based on user permissions which are linked to roles and responsibilities through a role based access control system. Masking is applied where information is not permitted see image for example:



Personal Information

Basic Information

PREFERRED NAME

[redacted]

FIRST NAME

[redacted]

LAST NAME

[redacted]

NATIONALITY

[redacted]

DATE OF BIRTH

[redacted]

PRONOUNS

[redacted]

Visible for your permission

Human Resources

Management is responsible for planning staffing and structures to ensure that the human resource plans are consistent with the organization’s goals which aim to:

1. Attract and appoint candidates who will understand and meet the requirements of both the organization and customers;
2. Adhere to relevant regulations; and
3. Promote and maintain a reputation as a responsible employer.

Competence of Personnel

The organization determines the level of competency of individuals required for ensuring the success of the ISMS. This includes ensuring that there are job descriptions for each role within the ISMS and assigning the roles to the appropriate individuals already within the organization. Additionally, the organization also incorporates competency screening during the hiring process for potential candidates. For more details, please refer to the Hiring Policy.

Training and Awareness

Kleene AI provides necessary training and development in system confidentiality and security concepts and issues including awareness training as detailed in the Information Security Policy (disseminated to authorized and relevant personnel). All employees within Kleene AI are to undergo annual security awareness training initiatives to ensure they stay abreast of significant security issues that pose a credible threat to the organization as a whole. Statement verbiage, should transform into a policy statement such as: All users with access to the Company's system are provided threat training for the system components they access to respond to a threat in an appropriate way.

As such, the security awareness training program provides both general, enterprise-wide training measures along with subject matter specifically related to system components. Security awareness is provided to all employees on a routine basis, rather than just a once-per-year calendar activity. It must be stressed that security awareness training is dynamic, changing as needed to meet the growing threats facing Kleene AI. As such, the training and awareness program is reviewed on at least an annual basis to ensure that it is effective for the organization's current and future state.

Training will be provided by management and conducted via a presentation ensuring the employee both understood and retained the information presented.

Communications

Please refer to communications plan.

Documented Information

The organization's documentation relating to the ISMS is controlled in accordance with the following requirements:

- Producing, reviewing, changing and distributing the document
- Maintaining good quality corporate records; and
- Releasing policy and process documents into the business, including the requirement for user training where appropriate.

The version history provides an overview of the ISMS documentation, providing information on the most current version number and a description of the last change made.

Internal Audit

Internal audits of the ISMS are conducted in accordance with the company’s Continual Improvement Review Procedure and Internal Audit Plan. Reviews are carried out to:

1. Assess the effectiveness of the ISMS and identify opportunities for improving company business processes
2. To ensure compliance with business policies and processes, and
3. To assist in identifying improvement action plans and how performance against plans will be measured.

Refer to the Continual Improvement Review Procedure and Internal Audit plan for further details.

Management Review

Kleene AI applies a principle of continuous improvement and monitoring by conducting regular quarterly management reviews of ISMS suitability, adequacy and effectiveness. This includes reviews of the risks identified and documented, as well as their associated mitigation strategies.

Furthermore, Kleene AI is committed to conducting internal audits on an annual basis, as defined by the internal audit procedures. This involves testing the validity of Kleene AI's security controls, procedures, and policies. These audits may also be conducted more frequently where a significant organisational or technological change event or incident takes place.

Review of the organization’s ISMS is conducted by the management team, which reviews progress and performance against plans and objectives. The review includes the following:

- Follow-up actions from previous reviews;

- Review of ISMS and any changes
- Results of internal audits and reviews
- Feedback from interested parties
- Review of performance against security objectives and overall effectiveness of the ISMS
- Status of risk assessment and treatment plan
- Review of Incidents
- Status of preventive and corrective actions
- Personnel matters
- Business Continuity status and testing
- Changes and recommendations for improvement

ISO 27002 (Annex A) Controls Mapping

Annex A-5: Information Security Policies

A number of policies and processes are in place to ensure Bottomline Technologies safeguards the confidentiality, integrity and availability of the respective information assets. Refer to the table below which lists each of the policies supporting the ISMS.

Annex A-6: Organization of Information Security

The organization is responsible for ensuring that information security responsibilities are defined and allocated which are defined within this ISMS as well as the Information Security Policy and Configuration and Change Management Policy.

Annex A-7: Human Resource Security

The organization must ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. This includes proper screening of candidates, establishing terms and conditions of employment, managing responsibilities, and providing information security awareness through education and training. Additionally, the organization establishes a disciplinary process for employees who have committed an information security breach which may lead to possible termination of employment responsibilities. Refer to the Information Security Policy, Hiring Policy, and the Employee Handbook.

Annex A-8: Asset Management

The organization must identify assets and feed in appropriate protection and responsibilities. Asset management includes maintaining an inventory of assets with ownership assigned to each asset. Additionally, there must be rules established for the acceptable use of assets and procedures for returning assets upon termination of employment.

The organization has established an information classification schema to ensure that the appropriate level of protection has been applied based on the nature of the information for proper handling. The organization is required to label all information within the scope of the ISMS according to the information classification schema.

Media must be handled with proper protections to prevent unauthorized disclosure, modification, removal or destruction of information.   This includes the management of removable media, disposal of media, and procedures for transferring physical media. Refer to Information Security Policy and the Data Protection and Handling Policy.

Annex A-9: Access Control

Limiting access to information and information processing facilities is an important objective within the organization's ISMS. There is an Access Control policy established which includes specific information security requirements applicable to all personnel and contractors within the scope of the ISMS. Additionally, the user registration/provisioning and de-registration/deprovisioning process has been properly documented to ensure authorized access to the organization's logical and physical assets.

Included within access control is the management of privileged access rights (i.e. elevated access or administrative access) to the in-scope systems within the ISMS. The organization has established policies including secret authentication management, review of user access rights, secure log-on procedures and password management. Refer to the Information Security Policy.

Annex A-10: Cryptography

The organization must ensure that proper and effective use of cryptography controls are in place to protect the confidentiality, authenticity and integrity of information within the scope of the organization. There is a policy detailing the use of cryptographic controls and key management below:-

Purpose

This document provides kleene employees and partners with the information required to effectively and efficiently plan, prepare and deploy encryption solutions in order to secure Confidential Information.

Scope

This policy applies to all users of Kleene information assets including but not limited to Kleene employees, contractors and partners. This policy applies whether electronic mail is accessed from Kleene networks or via any remote location.

Policy

When properly implemented, encryption provides an enhanced level of assurance that the data, while encrypted, cannot be viewed or otherwise discovered by unauthorized parties in the event of theft, loss or interception.

All users are required to employ company-approved encryption solutions to preserve the confidentiality and integrity of, and control access to, Confidential Information where this data is processed, stored or transmitted.

Encryption Approaches

A defence in depth approach is recommended when evaluating and deploying encryption products. In an ideal situation, full disk and/or boot disk encryption would be combined with file/ folder encryption in order to provide two 'layers' of encryption to protect data in the event the first layer is compromised. As a minimum, all sensitive data should be stored in an encrypted folder.

We recommend the use of FileVault for MacOS and Bitlocker for Windows to ensure that all data on boot disks are encrypted.

Removable Media

Given the risk associated with loss/theft of external disks, USB sticks, and memory cards, all removable media that contains sensitive data must be encrypted.

Encryption Keys

All generated encryption keys should be at least 2048 bit keys for RSA. It is essential that these keys are stored in 1Password and if they need to be sent to anyone, this is also done via 1Password to ensure that they are encrypted in transit.

Keys should never be stored in plain text files on any device, especially the device which holds the encrypted data.

For AWS services we rely on AWS managed encryption so that the keys are not stored outside of the cloud environment and are rotated automatically by AWS. This also enables access controls to be applied via IAM permissions.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Kleene reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Kleene does not consider conduct in violation of this policy to be within an employee’s or partner’s course and scope of employment, or the direct consequence of the discharge of the employee’s or partner’s duties. Accordingly, to the extent permitted by law, Kleene reserves the right not to defend or pay any damages awarded against employees or partners that result from a violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon as possible.

Definitions

Confidential Information (Sensitive Information) - Any Kleene information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form.

Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts.

Confidential Information also includes any confidential information received by Kleene from a third party under a non-disclosure agreement.

Encryption key - A secret password or bit string used to control the algorithm governing an encryption process.

Encryption - A process involving data coding to achieve confidentiality, anonymity, time stamping, and other security objectives.

Partner - Any non-employee of Kleene who is contractually bound to provide some form of service to Kleene.

Removable Media - Any device that can be connected to a computer and used to store data.

User - Any Kleene employee or partner who has been authorized to access any Kleene electronic information resource.

Annex A-11: Physical and Environmental Controls

The organization has an access-controlled office, in which visitor access is granted through sign in at reception.

Furthermore, there are no on-site servers or storage facilities, therefore, access is simply focused on the office space. The organization do not depend on the office for continuity of the product.

Annex A-12: Operations Security

The organization has established documented operational procedures to ensure proper controls over the information processing facilities, including change management, capacity management, and separation of operation environments (i.e. development, test and production).

Virus controls are applied to protect the integrity of company software and information. Virus controls include:

- Assessment of Virus Threats.
- Establishing Virus Countermeasures.
- Virus Outbreak handling

Backup procedures, including backup locations, responsibilities, environmental protection, and testing are implemented.

Monitoring of the organization’s environment is the responsibility of the Head of cloud and security. The logs generated from the monitoring activities are appropriately protected from tampering and unauthorized access. Time synchronization is enabled to ensure that there is a single reference time source.

Refer to the Information Security Policy, Configuration and Change Management Policy, and Business Continuity/Disaster Recovery Policy.

Annex A-13: Communications Security

The IT department monitors the network; any issues will be raised for investigation and resolution. There is constant monitoring over network activity.

All general client media within the company is treated as ‘Internal’ (unless specifically classified as ‘Confidential’) and requires management approval for it to be removed or copied outside of the company as described in the Information Classification section.

Email is used by the organization to communicate internally and with third parties, clients and suppliers. Protection for email applies to the company and includes measures to prevent Spamming, Relay and Abusive Content.

The company currently deals with virus and other threats by ensuring appropriate protection is on all machines. Measures to prevent destructive outbreaks include:

- Anti-virus software on Internal and Email servers.
- ProofPoint Email Security Gateway Solution
- Anti-Virus software on all desktops and laptops.

Annex A-14: System acquisition, development and maintenance

The Configuration and Change Management Policy describes and defines how to implement applicable security measures around asset/inventory management, audit and accountability ("auditable events"), access control, server/service/wireless baseline guidelines, application and operating system change management, quality testing requirements hardening systems, servers, middleware, applications, and cloud environment at rest.

Reasonable Industry-standard procedures, such as operating system, databases and device configuration hardening, patch management and structured control will be appropriately and consistently applied within the Configuration Management and Change Management Policy.

Annex A-15: Supplier Relationships

Information security controls are in place to protect the organization's assets that are accessible by suppliers. The Supplier Risk Management Policy defines our framework for managing supplier relationships. It describes our expectations for classifying our suppliers based on risk; establishes appropriate measures to mitigate risks; and outlines the processes and associated controls for selecting, risk ranking, contracting with, monitoring, and terminating relationships with our suppliers.

Annex A-16: Information Security Incident Management

The organization has established policies and procedures for the management of information security incidents, including communication on security events and weaknesses. The Incident Response Policy establishes responsibilities and procedures to ensure effective responses to information security incidents. Additionally, the policy provides the definition of a breach, staff roles and responsibilities, standards, and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms to help prevent the incidents from occurring again.

Annex A-17: Information Security Aspects of Business Continuity Management

Information security has been embedded within the organization’s business continuity management systems. The maintains this Business Continuity Plan (BCP) to document the standards and procedures for responding to and recovering from a significant business disruption. Disaster Recovery (DR) involves the policies, tools, and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a business disruption. The DR Plan is a subset of this BCP. This BCP considers the Company's software platform’s data architecture and deployment models; physical locations of operations; critical support and development systems; and reliance on third parties.

Annex A-18: Compliance

The organization has developed policies and controls to ensure that it avoids breaches of legal, statutory, regulatory and/or contractual obligations related to information security and of any information security requirements. Any relevant legislation and contractual requirements are explicitly identified and updated for each information system within the organization. Additionally, intellectual property rights and personal identifiable information are protected to ensure compliance with regulations and contractual obligations through the use of cryptographic controls.

Information security reviews are conducted on an annual basis to ensure that information security is implemented and operating in accordance with the organization’s policies and procedures. The review includes an independent audit of the ISMS and supporting technical controls. Refer to the Internal Audit procedure.

ISMS Controls and Policies

Aa Control Section #	Control Description	Associated Policy
A5	Information Security Policies	Kleene AI Information Security Policy
A6	Organization of Information Security	Kleene AI Information Security Policy/Configuration and Change Management Policy
A7	Human Resource Security	Kleene AI Information Security Policy/Kleene AI Hiring Policy/Kleene AI

Control Section #	Control Description	Associated Policy
		Employee Handbook
A8	Asset management	Kleene AI Information Security Policy/Kleene AI Data Protection and Handling Policy
A9	Access Control	Kleene AI Information Security Policy
A10	Cryptography	Kleene AI Information Security Policy
A11	Physical and Environmental Security	Kleene AI Information Security Policy
A12	Operations Security	Kleene AI Information Security Policy/Configuration and Change Management Policy
A13	Communications Security	Kleene AI Information Security Policy/Kleene AI Data Protection and Handling Policy
A14	System Acquisition, Development and Maintenance	Kleene AI Information Security Policy/Configuration and Change Management Policy
A15	Supplier Relationships	Kleene AI Supplier Risk Management Policy
A16	Information Security Incident Management	Kleene AI Incident Response Policy
A17	Information Security Aspects of business continuity management	Kleene AI Business Continuity and Disaster Recovery Policy
A18	Compliance	Internal Audit Policy