Third Party Supplier Security Policy

DOCUMENT CLASSIFICATION	Internal
VERISON	1.0
DATE	
DOCUMENT AUTHOR	Ayaz Sabir
DOCUMENT OWNER	

REVISION HISTORY

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES

DISTRIBUTION LIST

NAME	SUMMARY OF CHANGE

APPROVAL

NAME	POSITION	SIGN

Contents

1. Introduction

In today's interconnected business environment, organizations increasingly rely on third-party suppliers, vendors, and service providers to deliver products, services, and support critical business operations. While these relationships offer significant benefits, they also introduce inherent information security risks. Third-party access to organizational information, systems, and processes can create vulnerabilities that, if not properly managed, could lead to data breaches, service disruptions, reputational damage, and non-compliance with legal and regulatory requirements.

This Third-Party Supplier Security Policy establishes the framework for managing information security risks associated with all third-party relationships. It outlines the principles, requirements, and processes for ensuring that suppliers who access, process, store, or transmit the organization's information, or provide services that impact its information security, maintain an adequate level of security. By implementing this policy, the organization aims to protect its information assets, maintain operational resilience, and ensure compliance with relevant standards, including ISO/IEC 27001:2022, particularly Annex A controls related to supplier relationships (A.5.19, A.5.20, A.5.21, A.5.22, A.5.23).

2. Purpose

The primary purpose of this Third-Party Supplier Security Policy is to establish a robust framework for managing information security risks introduced by third-party relationships. This policy aims to:

- **Protect Information Assets:** Safeguard the confidentiality, integrity, and availability of the organization's information assets when they are accessed, processed, stored, or transmitted by third-party suppliers.
- **Minimize Risk:** Reduce the likelihood and impact of information security incidents, including data breaches, system compromises, and service

disruptions, arising from inadequate security practices of third-party suppliers.

- **Ensure Compliance:** Facilitate compliance with relevant legal, regulatory, and contractual obligations (e.g., data privacy laws, industry standards) and internal organizational policies related to third-party risk management.
- **Establish Clear Expectations:** Define clear information, security requirements and expectations for all third-party suppliers, ensuring they understand their responsibilities.
- **Promote Secure Practices:** Encourage and enforce the adoption of appropriate information security controls and practices by third-party suppliers throughout the entire supplier lifecycle.
- **Maintain Operational Resilience:** Ensure that the security posture of third-party services supports the organization's operational resilience and business continuity objectives.
- **Align with ISO 27001:2022:** Meet the specific requirements of ISO/IEC 27001:2022, particularly Annex A Controls 5.19 (Information security in supplier relationships), 5.20 (Addressing information security within supplier agreements), 5.21 (Managing information security in the ICT supply chain), 5.22 (Monitoring, reviewing and change management of supplier services), and 5.23 (Information security for the use of cloud services).

3. Scope

This Third-Party Supplier Security Policy applies to all organizational units, employees, contractors, and third-party personnel involved in the acquisition, management, or oversight of products and services provided by external suppliers that may impact on the organization's information security. This includes, but is not limited to:

- **All Third-Party Suppliers:** Any external entity that provides products, services, or support to the organization, and whose activities involve accessing, processing, storing, or transmitting the organization's information, or providing services that affect the organization's information systems or security posture. This includes vendors, service providers, consultants, partners, and cloud

service providers.

- **All Information Assets:** All forms of information (e.g., electronic, paper, verbal), data, databases, applications, and intellectual property that are shared with, processed by, or managed by third-party suppliers.
- **All Information Systems and Services:** Any information systems, networks, applications, or services provided by or managed by third-party suppliers that are used by or integrated with the organization's operations.
- **All Stages of the Supplier Lifecycle:** This policy applies throughout the entire lifecycle of a supplier relationship, including:
    - **Selection and Due Diligence:** Prior to engaging a new supplier.
    - **Contracting and Onboarding:** During the establishment of agreements and integration into operations.
    - **Ongoing Management:** Throughout the duration of the supplier relationship.
    - **Termination:** Upon the conclusion or termination of the supplier relationship.

This policy establishes the minimum information security requirements for engaging with third-party suppliers. Specifically detailed procedures and controls related to supplier security will be documented separately and referenced herein.

4. Policy Statements

This section outlines the mandatory principles and practices for managing information security risks associated with third-party suppliers, aligning with ISO/IEC 27001:2022 requirements. These statements provide clear management direction and support for all activities related to securing supplier relationships.

4.1 General Principles for Third-Party Supplier Security

All engagements with third-party suppliers must adhere to the following general principles. These principles ensure that information security considerations are integrated throughout the supplier lifecycle, minimizing risks and maintaining the organization's security posture:

- **Risk-Based Approach:** The level of security due diligence, contractual requirements, and ongoing monitoring applied to a third-party supplier must be proportionate to the information security risks associated with the products or services they provide and the sensitivity of the information they will access, process, or store.
- **Due Diligence:** Comprehensive information security due diligence must be conducted on all prospective third-party suppliers before engagement. This includes assessing their security posture, controls, and compliance with relevant standards and regulations.
- **Contractual Requirements:** All agreements with third-party suppliers must include clear and enforceable information security clauses that specify the security requirements, responsibilities, and liabilities of both parties. These clauses must align with the organization's information security policies and applicable legal and regulatory obligations.
- **Monitoring and Review:** The information security performance of third-party suppliers must be continuously monitored and regularly reviewed throughout the duration of the relationship. This includes verifying compliance with contractual obligations and assessing the effectiveness of their security controls.
- **Incident Management:** Third-party suppliers must have robust incident management processes in place and be required to promptly report any information security incidents that may impact on the organization's information assets or services.
- **Right to Audit:** The organization reserves the right to audit or request independent assurance reports (e.g., SOC 2, ISO 27001 certification) from third- party suppliers to verify their adherence to agreed-upon security requirements.
- **Termination Planning:** Information security considerations must be integrated into the termination planning for supplier relationships,

ensuring the secure return or destruction of organizational information and assets.

- **Communication and Collaboration:** Effective communication and collaboration with third-party suppliers are essential to ensure a shared understanding of information security requirements and to address any security concerns promptly.
- **Legal and Regulatory Compliance:** All third-party engagements must comply with relevant legal, regulatory, and industry-specific requirements concerning data protection, privacy, and information security.

4.2 Information Security in Supplier Relationships (ISO 27001:2022 Annex A 5.19)

As per ISO 27001:2022 Annex A 5.19, information security in supplier relationships shall be maintained. This control emphasizes the importance of managing the information security risks associated with the use of products or services provided by third parties. The organization shall implement the following to ensure information security in all supplier relationships:

- **Supplier Risk Assessment:** Before engaging with any new supplier, and periodically throughout the relationship, a comprehensive information security risk assessment shall be conducted. This assessment will evaluate the supplier's security posture, the criticality of the services or products provided, and the sensitivity of the information that will be accessed, processed, or stored by the supplier. The risk assessment shall inform the level of due diligence and the specific security controls required by the supplier.

- **Due Diligence Process:** A formal due diligence process shall be followed by all prospective suppliers. This process may include, but is not limited to:

    - **Security Questionnaires:** Requiring suppliers to complete detailed security questionnaires (e.g., SIG, CAIQ) to assess their information security management system, policies, and controls.
    - **Certifications and Attestations:** Requesting evidence of relevant security certifications (e.g., ISO 27001, SOC 2 Type 2 reports, CSA

STAR) or independent audit reports.

- **On-site Audits:** Conducting on-site security audits or assessments for high- risk suppliers or those handling highly sensitive information.
- **Reference Checks:** Contacting other clients of the supplier to inquire about their security practices and performance.

- **Defined Security Requirements:** Based on risk assessment and due diligence, clear and specific information security requirements shall be defined for each supplier. These requirements shall be communicated to the supplier and form a critical part of the contractual agreement. Requirements may include, but are not limited to:
  - Data protection and privacy controls.
  - Access control mechanisms.
  - Incident management and reporting procedures.
  - Business continuity and disaster recovery capabilities.
  - Security awareness training for supplier personnel.
  - Compliance with specific industry regulations or standards.
- **Contractual Agreements:** All supplier agreements shall include legally binding clauses that address information security requirements. These clauses shall cover:
  - The scope of information and systems accessible by the supplier.
  - The security controls and measures the supplier must implement.
  - Data ownership, privacy, and protection responsibilities.
  - Incident reporting obligations and timelines.
  - Audit rights and responsibilities.
  - Indemnification clauses related to security breaches.

- Termination clauses related to security non-compliance.

- **Ongoing Monitoring:** The organization shall establish a process for ongoing monitoring of supplier information security performance. This may involve:
  - Regular security reviews and performance evaluations.
  - Review of supplier-provided security reports or audit results.
  - Monitoring security incidents related to the supplier.
  - Periodic re-assessment of supplier risks.

- **Communication and Coordination:** Effective communication channels shall be established with suppliers to facilitate the exchange of information security- related matters, including changes to services, security incidents, and policy updates. The organization shall ensure that suppliers are aware of their information security responsibilities and any changes to these requirements.

4.3 Addressing Information Security Within Supplier Agreements (ISO 27001:2022 Annex A 5.20)

ISO 27001:2022 Annex A 5.20 requires that all relevant information security requirements shall be addressed in agreements with suppliers. This ensures that the security controls implemented by suppliers are consistent with the organization's information security policies and objectives. The organization shall ensure that supplier agreements include, but are not limited to, the following information security clauses:

- **Definition of Services and Information:** Clear definition of the services or products provided, the types of information to be accessed, processed, or stored, and the scope of the supplier's access to the organization's systems and data.

- **Information Security Controls:** Specific information security controls that the supplier must implement and maintain. These controls should be based on the risk assessment conducted during the due diligence phase and should cover:
  - **Access Control:** Requirements for managing user access,

including provisioning, de-provisioning, and periodic review of access rights.

- **Data Protection:** Measures for protecting the confidentiality, integrity, and availability of the organization's data, including encryption, data segregation, and data backup and recovery procedures.
- **Network Security:** Requirements for securing network connections, including firewalls, intrusion detection/prevention systems, and secure configurations.
- **Physical Security:** Controls for securing physical access to facilities where the organization's information or systems are processed or stored.
- **System Hardening:** Requirements for securing operating systems, applications, and databases against known vulnerabilities.
- **Vulnerability Management:** Procedures for identifying, assessing, and remediating security vulnerabilities in the supplier's systems and services.
- **Security Monitoring and Logging:** Requirements for logging security- relevant events and monitoring for suspicious activities.

- **Incident Management and Reporting:** Clear procedures for the supplier to report information security incidents, including:
  - **Notification Requirements:** Timelines and methods for notifying the organization of any security incidents, breaches, or suspected compromises.
  - **Incident Response Support:** The supplier's responsibilities in assisting the organization with incident investigation, containment, eradication, recovery, and post-incident analysis.
  - **Communication Protocols:** Agreed-upon communication channels and points of contact during an incident.
- **Business Continuity and Disaster Recovery:** Requirements for the supplier to maintain appropriate business continuity and disaster recovery plans to ensure the continued availability of critical services and the protection of

information during disruptions.

- **Audit and Assurance Rights:** The organization's right to conduct or commission audits, assessments, or reviews of the supplier's information security controls and practices. This may include:
    - **On-site Audits:** The right to conduct physical audits of the supplier's facilities.
    - **Remote Assessments:** The right to conduct remote assessments of the supplier's systems and processes.
    - **Third-Party Reports:** The requirement for the supplier to provide independent audit reports (e.g., SOC 2, ISO 27001 certification) or attestations.
- **Compliance with Laws and Regulations:** A clause requiring the supplier to comply with all applicable laws, regulations, and industry standards related to information security and data privacy (e.g., GDPR, CCPA, HIPAA).
- **Subcontracting:** Requirements for the supplier to obtain prior written approval from the organization before subcontracting any services that involve accessing, processing, or storing the organization's information. The supplier must also ensure that any subcontractors adhere to the same information security requirements as the primary supplier.
- **Data Ownership and Return/Destruction:** Clear provisions regarding the ownership of data, and requirements for the secure return or destruction of all organizational information upon termination or expiration of the agreement.
- **Liability and Indemnification:** Clauses defining the liabilities of both parties in the event of a security breach or non-compliance with information security requirements, including indemnification for damages caused by the supplier's negligence or breach of security obligations.
- **Termination Clauses:** Provisions for the immediate termination of the agreement in the event of a significant security breach or persistent non-compliance with information security requirements.

4.4 Managing Information Security in the ICT Supply Chain (ISO 27001:2022 Annex A 5.21)

ISO 27001:2022 Annex A 5.21 requires that information security risks associated with the organization's ICT supply chain shall be managed. This control addresses the increasing complexity and interconnectedness of modern supply chains, where vulnerabilities in one link can have cascading effects across the entire chain. The organization shall implement measures to manage information security risks throughout the ICT supply chain, including:

- **Supply Chain Risk Assessment:** Conducting a comprehensive risk assessment of the entire ICT supply chain to identify potential information security risks at each stage, from hardware and software development to procurement, delivery, and maintenance. This includes assessing the security practices of all entities involved in the supply chain, not just direct suppliers.
- **Security Requirements for Supply Chain:** Establishing and communicating clear information security requirements for all components and services within the ICT supply chain. This includes:
    - **Secure Development Practices:** Requiring suppliers to follow secure development lifecycle (SDLC) practices, including secure coding, security testing, and vulnerability management for software and hardware components.
    - **Tamper Protection:** Ensuring that hardware and software components are protected against tampering during manufacturing, transit, and storage.
    - **Authenticity and Integrity:** Verifying the authenticity and integrity of products and services received from suppliers, including using cryptographic controls (e.g., digital signatures, hashes) where appropriate.
    - **Vulnerability Disclosure:** Requiring suppliers to have a robust vulnerability disclosure program and to promptly inform the organization of any identified vulnerabilities in their products or services.

- **Supplier Due Diligence (Extended):** Extending the due diligence process to assess the information security practices of sub-suppliers and other entities within the ICT supply chain, especially for critical components or services. This may involve:
    - **Supplier's Supply Chain Management:** Evaluating how the direct supplier manages its own supply chain and the security controls they impose on their sub-suppliers.
    - **Transparency:** Requiring transparency from suppliers regarding their supply chain, including the origin of components and services.
- **Monitoring and Auditing (Extended):** Implementing mechanisms for monitoring and auditing the information security performance of entities throughout the ICT supply chain. This may include:
    - **Supply Chain Audits:** Conducting or commissioning audits of key suppliers and their sub-suppliers to verify compliance with security requirements.
    - **Threat Intelligence Sharing:** Participating in threat intelligence sharing programs to stay informed about emerging threats and vulnerabilities affecting the ICT supply chain.
- **Incident Response Planning:** Developing and testing incident response plans that specifically address supply chain security incidents, including procedures for isolating compromised components, communicating with affected parties, and restoring services.
- **Contractual Clauses (Extended):** Including specific contractual clauses in agreements with suppliers that address ICT supply chain security, including requirements for secure development, vulnerability management, and the right to audit sub-suppliers.
- **Secure Procurement:** Integrating information security requirements into the procurement process for all ICT products and services, ensuring that security is a key criterion in supplier selection and contract negotiation.

4.5 Monitoring, Reviewing and Change Management of Supplier Services (ISO 27001:2022 Annex A 5.22)

ISO 27001:2022 Annex A 5.22 requires that the organization shall regularly monitor, review and manage changes to supplier services to ensure that agreed levels of information security and service delivery are maintained. This control emphasizes the need for continuous oversight of supplier performance and security management of any modifications to their services. The organization shall implement the following:

- **Regular Performance Monitoring:** Establishing a continuous monitoring program to assess the supplier's adherence to information security requirements and service level agreements (SLAs). This includes:
    - **Security Metrics and KPIs:** Defining and tracking relevant security metrics and Key Performance Indicators (KPIs) for supplier services (e.g., incident response times, vulnerability remediation rates, uptime).
    - **Security Reports:** Requiring suppliers to provide regular security reports, including audit findings, penetration test results, and incident summaries.
    - **Vulnerability Scans and Penetration Tests:** Conducting or requiring suppliers to conduct regular vulnerability scans and penetration tests on systems and services provided by them, especially those that interact with the organization's critical assets.
    - **Compliance Checks:** Periodically verifying the supplier's compliance with contractual security clauses and relevant regulatory requirements.
- **Periodic Reviews:** Conducting formal periodic reviews of supplier relationships to assess their overall security posture and performance. These reviews shall involve:
    - **Review Meetings:** Regular meetings with suppliers to discuss security performance, review incident history, address any

concerns, and plan for future changes.

- **Security Assessments:** Re-assessing the supplier's information security controls and practices at defined intervals, especially for high-risk suppliers.
- **Contractual Compliance Review:** Verifying that the supplier continues to meet all information security obligations outlined in the contract.
- **Risk Re-Assessment:** Re-evaluating the information security risks associated with the supplier based on their performance, changes in their services, or changes in the threat landscape.

- **Change Management for Supplier Services:** Implementing a formal change management process for any modifications to supplier services that could impact on the organization's information security. This process shall align with the organization's internal Change Management Policy and include:
  - **Notification of Changes:** Requiring suppliers to notify the organization in advance of any planned changes to their services, systems, or security controls that could affect the organization's information security.
  - **Impact Assessment:** Conducting an impact assessment of proposed supplier changes on the organization's information security, operational continuity, and compliance.
  - **Risk Assessment:** Performing a risk assessment of the proposed changes to identify potential new vulnerabilities or risks.
  - **Approval Process:** Ensuring that all significant changes to supplier services are formally reviewed and approved by the relevant organizational stakeholders (e.g., Information Security, IT, Legal, Business Owners) before implementation.
  - **Testing and Verification:** Requiring suppliers to adequately test changes in a non-production environment and providing evidence of testing. The organization may also conduct its own testing or verification of critical changes.

Documentation Updates: Ensuring that all relevant documentation, including service descriptions, security policies, and incident response plans, are updated to reflect changes in supplier services.

Rollback Planning: Requiring suppliers to have a clear rollback plan for any changes and ensure the organization understands its implications.

Escalation Procedures: Establishing clear escalation procedures for addressing non-compliance, security incidents, or significant performance issues with suppliers. This includes defining roles and responsibilities for escalation and resolution.

4.6 Information Security for the Use of Cloud Services (ISO 27001:2022 Annex A 5.23)

ISO 27001:2022 Annex A 5.23 requires that information security for the use of cloud services shall be managed in accordance with the organization's information security management system. This control specifically addresses the unique security considerations and shared responsibility model inherent in cloud computing environments. The organization shall implement the following measures when utilizing cloud services:

- **Cloud Service Risk Assessment:** A thorough risk assessment shall be conducted for all cloud services, considering the type of service (IaaS, PaaS, SaaS), the sensitivity of the data to be processed or stored, the criticality of the service, and the cloud service provider's (CSP) security posture. This assessment shall inform the selection of appropriate cloud services and the implementation of necessary security controls.

- **Cloud Service Provider (CSP) Due Diligence:** Comprehensive due diligence shall be performed on prospective CSPs, similar to other third-party suppliers, but with a specific focus on cloud-specific security aspects. This includes:

    - **Security Certifications and Audits:** Reviewing CSP's security certifications (e.g., ISO 27001, SOC 2, FedRAMP) and independent audit reports to verify their adherence to industry's best practices

and regulatory requirements.

- **Shared Responsibility Model:** Understanding and documenting the shared responsibility model for each cloud service, clearly delineating the security responsibilities of the organization and the CSP.
- **Data Location and Sovereignty:** Verifying the geographical location of data centers and ensuring compliance with data residency and sovereignty requirements.
- **Exit Strategy**: Assessing the CSP's capabilities and processes for data portability, secure data deletion, and service termination.

- **Cloud Service Agreements:** Agreements with CSPs shall include specific information security clauses that address cloud-specific risks and responsibilities. These clauses shall cover:
  - **Security Controls:** Explicitly stating the security controls implemented by the CSP and the organization's responsibilities within the shared responsibility model.
  - **Data Protection and Privacy:** Provisions for data encryption (in transit and at rest), data segregation, data backup and recovery, and compliance with data privacy regulations.
  - **Incident Management:** Clear procedures for the CSP to report security incidents, breaches, and service disruptions, including timelines and communication protocols.
  - **Audit Rights:** The organization right to audit CSP's security controls or to receive independent audit reports.
  - **Service Level Agreements (SLAs):** Defining security-related SLAs, including availability, performance, and incident response times.

- **Secure Configuration and Management:** The organization shall be responsible for securely configuring and managing its cloud environments in accordance with the shared responsibility model. This includes:
  - **Identity and Access Management (IAM):** Implementing robust IAM controls for cloud access, including multi-factor authentication

(MFA), the least privilege principles, and regular access reviews.

- **Network Security:** Configuring virtual networks, firewalls, and security groups to restrict unauthorized access to cloud resources.
- **Vulnerability Management:** Regularly scanning and patching vulnerabilities in applications and operating systems deployed in the cloud environment.
- **Security Monitoring and Logging:** Implementing comprehensive logging and monitoring solutions to detect and respond to security events in the cloud.

- **Data Classification and Handling in the Cloud:** Information classified as sensitive or critical shall be handled in cloud environments only if the CSP provides adequate security controls and the contractual agreements address the specific handling requirements.
- **Cloud Security Awareness and Training:** Personnel involved in managing or using cloud services shall receive appropriate security awareness training specific to cloud environments, including understanding the shared responsibility model and secure configuration practices.
- **Continuous Monitoring and Review:** The security posture of cloud services shall be continuously monitored and regularly reviewed to ensure ongoing compliance with security requirements and to adapt to evolving threats and changes in the cloud environment.

5. Roles and Responsibilities

Effective management of third-party supplier security requires clear definition and assignment of roles and responsibilities across the organization. All individuals and departments involved in the lifecycle of third-party relationships must understand their duties to ensure the consistent application of this policy and the

protection of organizational assets.

- Senior Management / Executive Leadership:
    - Provides overall strategic direction and commitment to third-party supplier security.
    - Approves the Third-Party Supplier Security Policy and allocates necessary resources.
    - Ensures that third-party risk management is integrated into the organization's overall risk management framework.
- Information Security Officer (ISO) / CISO:
    - Develops, implements, and maintains the Third-Party Supplier Security Policy and associated procedures.
    - Oversee the information security risk assessment and due diligence processes for third-party suppliers.
    - Provides expert guidance on information security requirements for supplier agreements.
    - Monitors the information security performance of critical suppliers and advises on remediation efforts.
    - Acts as the primary point of contact for third-party security incidents.
- Procurement / Sourcing Department:
    - Initiates the supplier engagement process and ensures that information security requirements are included in procurement activities.
    - Facilitates the due diligence process by coordinating with the Information Security team and suppliers.
    - Ensure that contractual agreements with suppliers include all necessary information security clauses as defined by this policy.
- Legal Department:
    - Reviews and approvals all contractual agreements with third-party suppliers to ensure legal enforceability of information security

clauses and compliance with relevant laws and regulations.

- Provides legal advice on data protection, privacy, and liability matters related to third-party relationships.

- **Business Owners / Department Heads:**
  - Identify the need for third-party services and are responsible for the business relationship with the supplier.
  - Participate in the risk assessment process, providing insights into the criticality of the service and the sensitivity of the data involved.
  - Ensure that their teams adhere to this policy when interacting with third- party suppliers.
  - Monitor the operational performance of supplier services and report any security concerns.
- **IT Department / Technical Teams:**
  - Implement and manage technical controls for integrating with and accessing third-party services.
  - Provide technical expertise during supplier due diligence and ongoing monitoring.
  - Assist in the investigation and resolution of security incidents involving third-party suppliers.
  - Ensure secure configuration and management of cloud services in accordance with the shared responsibility model.

- **Audit and Compliance Teams:**
  - Conduct independent audits and reviews of the third-party supplier security program to ensure compliance with this policy and regulatory requirements.
  - Assess the effectiveness of controls implemented for managing third-party risks.

- All Employees:
    - Adhere to the guidelines and procedures outlined in this policy when interacting with third-party suppliers or using third-party services.
    - Report any suspected security incidents or policy violations related to third- party suppliers immediately.

6. Compliance and Enforcement

Adherence to this Third-Party Supplier Security Policy is mandatory for all individuals and entities within its scope. Compliance will be regularly monitored, and any non- compliance will be addressed through appropriate enforcement mechanisms. The following outlines our approach to ensuring compliance:

- **Monitoring and Auditing:** Regular monitoring and auditing activities will be conducted to assess adherence to this policy and the effectiveness of the third- party supplier security program. This includes:
    - **Review of Supplier Contracts:** Periodic review of supplier agreements to ensure that information security clauses are current and adequately address identified risks.
    - **Performance Reviews:** Regular assessment of supplier security performance against agreed-upon metrics and contractual obligations.
    - **Internal Audits:** Scheduled internal audits to verify compliance with policy requirements and identify areas for improvement in third-party risk management.
    - **External Audits/Certifications:** Review of external audit reports (e.g., SOC 2, ISO 27001 certifications) provided by suppliers to validate their security posture.

- Reporting and Investigation:

- All identified or suspected deviations from this policy, or any security incidents related to third-party suppliers, must be reported immediately to the Information Security Officer or designated contact.
- All reports will be investigated promptly and thoroughly to determine the root cause of non-compliance or incidents and implement corrective actions.

- **Training and Awareness:** Mandatory training will be provided for all personnel involved in managing third-party relationships, covering the principles, procedures, and their specific roles and responsibilities outlined in this policy. Awareness campaigns will reinforce the importance of third-party security.
- Non-Compliance by Internal Personnel:
  - Any instances of non-compliance with this policy by internal personnel will be investigated and addressed in accordance with the organization's disciplinary procedures.
  - Depending on the severity and frequency of non-compliance, disciplinary actions may range from mandatory re-training and formal warnings to suspension or termination of employment, in accordance with the organization's human resources policies and applicable labor laws.

- Non-Compliance with Third-Party Suppliers:
  - Instances of non-compliance by third-party suppliers with contractual information security obligations will be addressed promptly.
  - Actions may include, but are not limited to, requiring corrective action plans, imposing penalties as per contractual terms, withholding payments, or, in severe or persistent cases, termination of the supplier agreement.

    - The organization reserves the right to pursue legal remedies for damages resulting from a supplier's failure to adhere to agreed-upon security requirements.

- **Continuous Improvement:** The effectiveness of this policy and the overall third- party supplier security program will be continuously evaluated. Feedback from monitoring activities, incident investigations, and audits will be used to refine and improve the policy, associated procedures, and training programs. This commitment to continuous improvement ensures that our third-party risk management practices remain robust and adaptable to evolving threats and the changing supplier landscape.

7. Policy Review

This Third-Party Supplier Security Policy will be reviewed at least annually, or more frequently if significant changes occur in the organization's business operations, the third-party landscape, technological advancements, legal or regulatory requirements, or in response to major security incidents involving suppliers. The review process will involve:

- **Assessment of Effectiveness:** Evaluating the policy's effectiveness in managing third-party information security risks and achieving its stated objectives.
- **Feedback Integration:** Incorporating feedback from all relevant stakeholders, including employees, management, procurement, legal, IT, and information security personnel.
- **Alignment with Standards:** Ensuring continued alignment with ISO/IEC 27001:2022 (specifically Annex A Controls 5.19, 5.20, 5.21, 5.22, 5.23) and other relevant security standards and best practices.
- **Updates and Revisions:** Making necessary updates and revisions to the policy document to reflect changes in third-party risk management practices, emerging threats, organizational structure, and operational processes. All revisions will be formally approved and communicated to all

relevant personnel.

- **Lessons Learned:** Integrating lessons learned from actual incidents, near misses, and audits related to third-party security to continuously improve the policy and associated guidelines.

8. Definitions

- **Third-Party Supplier:** Any external entity that provides products, services, or support to the organization, and whose activities involve accessing, processing, storing, or transmitting the organization's information, or providing services that affect the organization's information systems or security posture. This includes vendors, service providers, consultants, partners, and cloud service providers.
- **Information Asset:** Any information or information system that has value to the organization. This includes data, software, hardware, services, and intellectual property.
- **Confidentiality:** The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity:** The property of safeguarding the accuracy and completeness of assets.
- **Availability:** The property of being accessible and usable upon demand by an authorized entity.
- **Information Security Management System (ISMS):** A set of policies and procedures for systematically managing an organization's sensitive data. The goal of an ISMS is to minimize risk and ensure business continuity by proactively limiting the impact of a security breach.
- **Cloud Service Provider (CSP):** A third-party company that offers cloud-based computing services to other businesses or individuals.
- **ICT Supply Chain:** The interconnected network of organizations, people, activities, information, and resources involved in the provision of information and communication technology (ICT) products and services.

9. References

- Information Security Policy
- Vendor Risk Management Policy
- Data Protection Policy
- Incident Response Policy
- Business Continuity & Disaster Recovery Policy
- Acceptable Use Policy (AUP)