Information Security Policy

Document Version 2.0

NOTE: Meant for employees within the organization and external staff associated with business operations.

Document Information	
Document Identification No.	NYK-ISMS-POL-001
Document Name	NYK-ISMS-POL-001-Information Security Policy
Document Classification	Internal
Document Version	V 2.0
Document Author	Vikalp (GRC Team)
Document Reviewer	Seema Aggarwal (GRC Head)
Document Approver	Praveen Kumar (CISO)
Date of Release/Approval	18-03-2025
Next Review Due	17-03-2026

Version	Change Description	Author	Reviewer	Approver	Approval Date
1.0	Initial Release	Vikalp (GRC Team)	Vaishali Narendra (Director - InfoSec)	Vikas Yadav (CISO)	22-12-2020
1.2	1. '*VisionStatement*' & '*Objectives*' added. 2. Other available InfoSec policies added as reference.	Vikalp (GRC Team)	Vaishali Narendra (Director - InfoSec)	Vikas Yadav (CISO)	16-06-2022
1.3	1. Policy updated basis input from other security policies	Vikalp (GRC Team)	Vaishali Narendra (Director - InfoSec)	Vikas Yadav (CISO)	18-05-2023
1.4	1. Highlighted that 'GenAI' tools should not be used for illegal activities (like creating deep fakes etc.) and/or sharing any company confidential information. 2. Added reference of MDM tool for using company's data (via email, drive, chat etc.) on personal devices.	Vikalp (GRC Team)	Vaishali Narendra (Director - InfoSec)	Praveen Kumar (CISO)	09-08-2024
2.0	Document revised to align with ISO 27001:2022 control requirements	Vikalp (GRC Team)	Seema Aggarwal (GRC Head)	Praveen Kumar (CISO)	18-03-2025

Contents

1. Introduction

Nykaa E Retail Limited (hereafter referred to as "Nykaa") a leading Indian retail company, offers a comprehensive range of beauty, wellness, and fashion products through its e-commerce platform, mobile application, and physical stores. As a key player in the e-commerce sector, Nykaa recognizes the paramount importance of protecting its information assets to ensure seamless business operations and maintain customer trust. The company is committed to establishing and maintaining a comprehensive Information Security Governance framework, which serves as the foundation for securing critical business information across all its operations.

The protection of information is a fundamental aspect of Nykaa's day-to-day activities, as the organization relies heavily on its information systems for effective service delivery. In this context, information security involves safeguarding data throughout its entire lifecycle—whether in creation, usage, transmission, storage, or disposal. By implementing a robust Information Security Management System (ISMS), Nykaa aims to address the growing complexity and risks associated with managing and securing sensitive information, while aligning with global best practices and compliance requirements.

This Information Security Policy (ISP) outlines Nykaa's commitment to ensuring the confidentiality, integrity, and availability of information, as well as the management of associated risks. It underscores the company's dedication to protecting not only internal data but also the personal and financial information of its customers, employees, and business partners. The policy also reflects Nykaa's proactive approach to securing its information systems and ensuring business continuity in an increasingly dynamic digital landscape. Through this policy, Nykaa strives to create a secure environment that supports its business objectives and fosters trust among all stakeholders

1.1 Definitions

- **Governance:** The set of responsibilities and practices exercised by the organization's leadership to ensure information security objectives are achieved. Governance involves, but not limited to, setting policies, defining roles, and overseeing the implementation of security measures.
- **Framework**: A structured set of guidelines, best practices, and standards that provide a systematic approach to managing information security. Frameworks like ISO/IEC 27001 offer a comprehensive structure for establishing, implementing, and maintaining an Information Security Management System (ISMS).
- **Asset**: Any item, data, or resource that has value to the organization. Assets can include information, software, hardware, personnel, intellectual property, and physical facilities. Protecting assets is a fundamental aspect of information security.
- **Information Security:** Refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.
- **Physical Security:** Measures taken to protect physical assets, such as buildings, equipment, and personnel, from physical threats like theft, vandalism, and natural disasters. Physical security controls include access restrictions, surveillance, and environmental protections.
- **Information Security Management System (ISMS):** The ISMS framework is a set of policies, procedures, guidelines, resources, and associated activities handled by an organization to protect its information. This framework is a systematic approach that aims at defining, implementing, monitoring, maintaining, and enhancing an organization's information security, to achieve its business and security goals.
- **Business Continuity Management (BCM)**: Processes and procedures that ensure critical business functions can continue during and after a disruptive event. BCM involves planning, risk assessment, and recovery strategies to maintain operations and minimize impact.
- **Disaster Recovery Plan (DRP):** A documented strategy and set of procedures to recover and restore IT systems and data after a catastrophic event. DRP focuses on minimizing downtime and ensuring the availability of critical systems.

- **Supplier Relationship Management (SRM):** The management of interactions and relationships with external suppliers and vendors to ensure that they comply with the organization's security requirements. SRM includes assessing supplier security practices and monitoring their performance.
- **Data Protection:** A set of strategies and measures designed to safeguard personal, financial, and other sensitive data from unauthorized access, loss, corruption, or theft, and to ensure compliance with applicable laws and regulations.
- **Confidentiality:** Confidentiality is the need to ensure that information is disclosed only to those who are authorized to view it.
- **Integrity:** Integrity is the need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.
- **Availability:** Availability is the need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it, on demand.
- **Risk Assessment:** A systematic process of evaluating the potential risks that may be involved in projected activity or undertaking. A Risk Assessment is the process by which risks are identified and the impact of those risks determined.
- **Risk Treatment:** The process of selecting and implementing measures to modify risk, including accepting, avoiding, transferring, or mitigating it. Risk treatment aims to reduce risk to acceptable levels based on the organization's risk appetite.
- **Incident:** An event that compromises the confidentiality, integrity, or availability of information assets. Incidents can range from security breaches and data leaks to system failures and unauthorized access.
- **Likelihood:** The probability that a specific threat will exploit a vulnerability, leading to a security incident. Assessing likelihood is a critical component of risk assessment and management.
- **Segregation of Duties:** It is the principle of splitting privileges among multiple individuals or systems. Segregation of Duties is an internal control designed to prevent error and fraud by ensuring that at least two individuals are responsible for the separate parts of any task.

1.2 Information Security Policy Statement

Nykaa aims to safeguard sensitive information such as Customer PII, financial statements, manage risks, ensure the confidentiality, integrity, and availability of information, and drive industry growth, while prioritizing security, trust, and sustainability to set global standards of information security in the ecommerce sector. Nykaa aims to achieve this by implementing and maintaining an Information Security Management System (ISMS) in accordance with ISO 27001:2022. Nykaa will identify and manage information security risks, comply with legal and regulatory requirements, and allocate the necessary resources for the effective operation of the ISMS. All employees, contractors, and third-party partners shall adhere to this policy and support information security objectives. Leadership will ensure regular reviews and continual improvement of the ISMS to address emerging risks and business needs.

2. Purpose

The purpose of Nykaa's Information Security Policy (ISP) is to ensure the protection of all information assets, both digital and physical, to maintain business continuity, safeguard sensitive data, and uphold customer trust. This policy aims to establish a robust framework for managing risks related to information security, ensuring compliance with applicable laws and regulations, and creating a secure environment for Nykaa's operations. By implementing and maintaining an Information Security Management System (ISMS) in accordance with ISO 27001:2022, Nykaa strives to safeguard the confidentiality, integrity, and availability of critical information. The policy outlines a comprehensive approach to prevent unauthorized access, use, disclosure, disruption, or destruction of information, while promoting a culture of security awareness across all levels of the organization. Ultimately, the ISP supports Nykaa's business objectives by enhancing the security posture, ensuring trustworthiness, and mitigating potential risks associated with data and information management.

3. Scope

The Information Security Policy (ISP) applies to all information, information systems (including digital, softcopy,

hardware, software and hardcopy) and technology assets controlled and managed by Nykaa. The ISP also applies to all clients, partners, consultants, contractors, vendors, suppliers, interns, and authorized individuals accessing Nykaa IT systems, servers, applications, networks, mobile devices, and telecommunications.

Specifically, in details, this policy covers the following:

Information Assets
The ISP applies to all information, irrespective of format or medium. This includes structured and unstructured data, digital records, physical documents, communications, and metadata managed, processed, or stored by Nykaa. The scope extends to information at rest, in transit, and in use, regardless of its location, whether within organizational premises, cloud environments, or partner systems.

Technology Systems and Infrastructure
All technology systems under Nykaa's control or management are covered, including:

- Core infrastructure such as enterprise servers, databases, storage systems, and network devices such as routers, switches, firewalls, and wireless access points.
- Endpoint devices such as desktops, laptops, mobile devices, tablets, and other peripherals, including personal devices used under authorized Bring Your Own Device (BYOD) policies.
- Applications and platforms such as e-commerce systems, internal applications, APIs, cloud-hosted services (SaaS, IaaS, and PaaS), and business-critical software solutions.
- Backup, disaster recovery, and business continuity systems.
- Communication technologies such as email systems, VoIP platforms, conferencing tools, and collaboration software.

Authorized Users
The policy is applicable to all individuals granted access to Nykaa's information and systems, including:

- Employees which includes all full-time, part-time, Interns, trainees, and temporary staff.
- Contractors, consultants, and vendors engaged by Nykaa.
- Clients, partners, and external stakeholders authorized to interact with Nykaa's IT systems.
- Any third party accessing organizational resources under contractual or other approved arrangements.

Access Methods and Channels
The ISP encompasses all methods and channels through which Nykaa's information and systems are accessed, including:

- Internal corporate networks (LAN, WAN, intranet).
- Remote access mechanisms, such as Virtual Private Networks (VPNs) and secure remote desktop connections.
- Cloud environments and externally hosted systems managed by Nykaa or its service providers.
- Mobile and wireless access, including telecommunications and IoT devices approved for use.

Physical and Logical Security
The policy extends to the physical and logical security of all Nykaa's IT assets, including data centers, office environments, and endpoint devices. Logical controls, such as access management, data protection, and encryption, are integral to the policy's scope.

Compliance and Regulatory Alignment
The ISP ensures adherence to applicable industry standards and regulatory requirements, such as ISO 27001, and local laws. It governs all security practices to safeguard data confidentiality, integrity, and availability across Nykaa's operations.

4. Leadership Commitment

Nykaa's management through the IS Steering Committee needs to provide sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS. In addition, it needs to effectively demonstrate its commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the ISMS by providing guidance and direction on following:

- Establishing an Information Security policy.
- Ensuring that ISMS objectives and plans are established and are compatible with the strategic direction of the organization.
- Ensuring the integration of the information security management system requirements into the organization's processes.
- Assigning and communicating responsibilities and authorities for roles relevant to information security.
- Communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement.
- Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS.
- Deciding the criteria for accepting the risk and acceptable levels of risk.
- Ensuring that internal ISMS audits are being conducted.
- Conducting management reviews of the ISMS.
- Providing decisions on the risk acceptance, budgetary approvals and/ or any other request put forward by the Information Security Lead for the maintenance and enhancement of the ISMS.

5. Roles and Responsibilities

Role	Responsibilities
Chief Information Security Officer (CISO)	• Govern overall Information Security initiatives. • Establish and oversee the organization's information security strategy and ISMS implementation. • Establish, review & approve ISMS policy, standards, procedures and define Risk Appetite • Advise senior management on Information security and risk management. • Facilitate creation of an information security and risk management structure covering the entire organization, with clearly defined roles and responsibilities. • Direct risk assessments and control implementation activities. • Provide necessary resources for implementation and execution, which includes budget, skilled personnel etc. • Monitor evolving security threats and ensure organizational preparedness, or delegate the activities to specialized personnel/ team. • Lead incident response and mitigation efforts, or delegate the activities to specialized personnel. • Drive organization-wide security awareness initiatives, and communicate importance of effective information security management system • Assume accountability of ensuring alignment of security objectives with business goals. • Establish Information Security related goals and determine how success will be measured. • Assure regular reviews and updates of ISMS are conducted, to maintain its relevance and effectiveness.

GRC Team	• Maintain a record of all Information Security Initiatives. • Execute ISMS operations, including risk assessments and control monitoring. • Maintain ISMS documentation to reflect current practices. • Evaluate Information Security exception requests based on valid business justifications. • Investigate and respond to security incidents, and conduct Root Cause Analysis. • Implement and monitor information security controls. • Act as Nykaa's representative when dealing with Law Enforcement agencies for all Information Security related incidents. • If required, conduct security assessments and support audits in coordination with Nykaa's GRC Team. • Deliver security awareness programs. • Ensure compliance with regulatory and organizational security requirements. • Collaborate with stakeholders to support secure business processes.
Department Head/ Business Heads	• Ensure implementation of ISMS policies and controls within their domains. • Promote adherence to ISMS requirements within their teams. • Monitor and mitigate security risks within business operations in coordination with Information Security and GRC Teams. • Collaborate with the Information Security Team on risk assessments and control enhancements. • Support compliance and audit activities alongside the GRC Team. • Report security incidents and vulnerabilities promptly to the Information Security team.
Nykaa Information Security Steering Committee (ISSC)	• Establish, review & approve ISMS policy, standards, procedures and define Risk Appetite • Facilitate creation of an information security and risk management structure covering the entire organization, with clearly defined roles and responsibilities. • Govern overall Information Security initiatives. • Set and drive the strategic direction of ISMS implementation. • Establish goals and scope as well as determine how success will be measured. • Provide necessary resources for implementation and execution, which includes budget, skilled personnel etc. • Communicate importance of effective information security management system • Assess and approve or reject implementation/sustenance plans and changes to implementation/sustenance plans. • Prioritize and reprioritize deliverables. • Annually attend the Management Review Meeting to evaluate the ISMS status, and provide recommendations.Monitoring of Information Security Management System and ensure Continual Improvement • Assure allocation of resources for ISMS operations and improvements.
Information Security	• Implementation of the ISMS framework • Improvement of the effectiveness of the ISMS. • Maintaining a record of all the Information Security initiatives.

Working Group (ISWG)	• Modification of procedures and controls that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS, including changes to:
	  ○ Business requirements.
	  ○ Security requirements.
	  ○ Business processes affecting the existing business requirements.
	  ○ Regulatory or legal requirements.
	  ○ Contractual obligations; and
	  ○ Levels of risk and/or criteria for accepting risks.
	• Facilitate implementation of Information Security Policies, standards, and procedures in coordination with the GRC Team, to ensure that all identified risks are managed within the organization's risk appetite.
	• Improvement to how the effectiveness of controls is being measured.
	• Ensure business continuity and disaster recovery integration within ISMS.
	• Review and approve relevant ISMS documentations.
	• Perform risk assessments and security control implementations.
	• Monitor the adopted risk treatment plans.
	• Evaluating information security exception requests based on valid business justification.
	• Update of the risk assessment and risk treatment plan
	• Ensure compliance to ISO 27001 requirements within their business functions.
	• Ensure completion of activities as per the ISMS program calendar.
	• Promote ISMS practices through training and awareness programs, and ensure that all employees are attending these sessions.
	• Monitor the effectiveness of Information Security initiatives across the organization with predefined Key performance indicators.
	• Participate and support Information Security audits.
	• Remediate any Information Security non-compliance applicable to the team.
	• Monitor deliverables quality and adjust accordingly.
	• Ensure that incidents impacting information security are promptly detected, assessed, and effectively responded to

Internal Audit Team	• Conduct independent assessments of ISMS effectiveness and compliance with ISO 27001 and regulatory requirements. • Report audit findings to the ISSC. • Verify implementation of remediation measures. • Provide assurance on ISMS performance and effectiveness.
All Employees/ Contractors, Vendors	• Adhere to Nykaa's Information Security policies and procedures. • Report Information security incidents promptly. • Participate in mandatory security awareness training. • Cooperate during the information security audits and checks. • Safeguard the confidentiality, integrity, and availability of sensitive information. • Only use authorized devices and systems for handling company data. • Ensuring compliance with contracts, data protection clauses, non-disclosure agreements and all applicable regulatory requirements.

Refer: NYK-ISMS-DOC-002-Information Security Governance Structure for further information.

6. Information Security Objectives

The objective of this policy and the ISMS program is to document the high-level information security strategy to ensure that the information and information assets of Nykaa are appropriately protected. Below are the objectives which the ISMS program at Nykaa is trying to achieve:

- Develop, implement, and sustain a robust information security policy framework that aligns with organizational goals and fulfills legal, regulatory, and contractual obligations.
- Establish a governance structure to clearly define roles, responsibilities, and accountabilities, Including those of all personnel, ensuring effective oversight and management of information security.
- Conduct regular risk assessments to identify, evaluate, and mitigate risks to information assets, aligning mitigation strategies with the organization's risk appetite.
- Implement and maintain strict access controls to ensure that access to systems and data is limited to authorized personnel, based on business needs and regularly reviewed.
- Ensure all information assets are identified, classified, and protected with appropriate controls throughout their lifecycle, from creation to disposal.
- Deliver ongoing security awareness initiatives and tailored training programs to personnel at all levels, fostering a proactive security culture within the organization.
- Deploy comprehensive physical security measures to protect critical facilities and sensitive assets from unauthorized access, theft, or environmental threats.
- Maintain secure and resilient IT operations by establishing stringent controls for system monitoring, change management, and regular backup processes.
- Apply advanced cryptographic techniques to ensure the confidentiality, integrity, and availability of sensitive data, whether at rest, in transit, or during processing.
- Safeguard the exchange of information internally and externally by implementing secure communication channels and protocols to prevent unauthorized interception or tampering.
- Embed security controls and best practices into the entire lifecycle of system and application development, from initial design to decommissioning.
- Define and enforce robust security requirements for third-party providers and suppliers, continuously monitoring their compliance with organizational standards.
- Implement an incident response process that enables timely identification, escalation, and resolution of information security incidents, minimizing operational disruptions.
- Establish, test, and continuously refine business continuity and disaster recovery plans to ensure seamless operations during and after a disruption or crisis.
- Continuously evaluate and improve the effectiveness of the Information Security Management System through the use of key performance indicators, regular audits, and strategic management reviews.

6.1 Planning to achieve these Objectives

When planning to achieve its information security objectives, Nykaa shall identify and addresses the following elements:

- An action plan shall be developed to achieve the desired ISMS outcomes and should address:
  - Items listed in the Risk Register
  - Risk Treatment Plans
  - The Information Security Management System Program Calendar
  - Corrective or preventive actions identified during internal audits
  - Non-conformities from external audits
  - Information security incidents
  - Results from security effectiveness measurement activities
- The action plan shall specify an action owner accountable for completing each task.
- Each actionable item shall include a defined target date for closure.
- The action plan's success shall be assessed based on inputs from security effectiveness measurements, internal audit findings, and reported information security incidents.

7. Planning (Risk Management)

7.1 Actions to address Risks and Opportunities

Nykaa shall conduct regular risk and opportunity assessments for all relevant parties to ensure the ISMS achieves its intended outcomes. Identified risks and opportunities shall be addressed through action plans integrated into ISMS processes, monitored via the Nonconformity and Corrective Actions (NCCA) process, and reviewed annually to adapt to changing circumstances.

Refer: NYK-ISMS-PRO-014-InfoSec Risk Management Procedure for further information.

7.2 Security Risk Assessments

The Information Security team shall conduct structured risk assessments to identify, analyze, and evaluate threats and vulnerabilities inline to the Nykaa's defined risk assessment process for all critical processes and information assets annually and prior to introducing any significant change to the environment. These assessments shall guide the selection of prevention and mitigation strategies to bring risks to acceptable levels, ensuring business processes remain secure and informed by the risk treatment process.

Refer: NYK-ISMS-PRO-014-InfoSec Risk Management Procedure for further information.

7.3 Security Risk Treatment

Identified risks shall be prioritized and business function/ department head(s) shall be responsible for developing a mitigation plan and treating the risks in consultation with the Information Security team.

Refer: NYK-ISMS-PRO-014-InfoSec Risk Management Procedure for further information.

7.4 Monitoring and Review

It shall be ensured that the Information Security team, in coordination with the Information technology team, tracks all the information security risks identified in the information risk assessment report. Risk register shall be maintained and reviewed annually and additionally as needed following significant organizational or technological changes.

Refer: NYK-ISMS-PRO-014-InfoSec Risk Management Procedure for further information.

8. Performance Evaluation and Continuous Improvement

8.1 Performance Evaluation

8.1.1 Monitoring, Measurement, Analysis, and Evaluation

Nykaa shall identify and define the aspects of the ISMS that require monitoring and measurement, including processes and controls. Methods for monitoring, measurement, analysis, and evaluation shall be established to ensure results are valid, reproducible, and aligned with organizational objectives. Designated individuals shall perform analysis and evaluation at defined intervals, with documented records maintained as evidence. The performance of the ISMS and its controls shall be periodically assessed to ensure their effectiveness and alignment with intended outcomes.

8.1.2 Internal Audit

Nykaa shall conduct internal ISMS audits annually to evaluate the effectiveness and adequacy of implemented controls, processes, and procedures. These audits shall verify that the ISMS:

- Conforms to applicable standards, legislation, and security requirements.
- Aligns with identified information security needs and objectives.
- Is effectively implemented, maintained, and operates as intended.

Audit findings, including non-conformities and observations, shall be addressed promptly, with corrective actions documented and monitored to completion.

8.1.3 Management Review

Nykaa's management shall conduct an annual review of the ISMS or upon significant changes, ensuring its continued suitability, adequacy, and effectiveness. Reviews shall evaluate improvement opportunities, necessary updates to policies and objectives, and the overall performance of the ISMS. Outcomes of these reviews, including any required actions, shall be documented, and records maintained in accordance with ISMS requirements.

8.2 Continuous Improvement

8.2.1 Non-Conformities and Corrective Actions

Nykaa shall address non-conformities identified through audits, security incident reports, or feedback by implementing corrective actions to resolve root causes and prevent recurrence. Preventive actions shall also be taken to mitigate potential non-conformities arising from changes in the environment or operations. Corrective action plans shall be developed and executed by process owners, with oversight from the Head of Security to ensure timely and effective resolution.

8.2.3 Initiation and Recording

All non-conformities and corrective actions shall be documented, categorized, and monitored. Observations from third-party and internal audits shall be addressed promptly, with corrective actions tracked until successful resolution. Major and minor non-conformities shall be classified and resolved in consultation with relevant departments, ensuring risks are mitigated and lessons learned are incorporated.

8.2.4 Continual Improvement

Nykaa shall strive for continual improvement of the ISMS through the analysis of monitoring data, audit results, corrective actions, and management reviews. Opportunities for improvement shall be identified and acted upon to ensure the ISMS remains effective, resilient, and aligned with evolving organizational needs and security objectives.

9. Policy

The following policies are in place for maintaining an adequate level of protection and control for Information systems and assets throughout Nykaa:

9.1 Acceptable Usage Policy

- Roles and responsibilities shall be defined for using Nykaa's IT resources by all employees, contractors, business partners, and vendors, ensuring confidentiality, integrity, and availability of information assets.
- Unauthorized access, sharing of credentials, and installation of unapproved software shall be prohibited.
- Information Security controls such as strong authentication controls, data encryption as per the data classifications, and
- Guidelines for secure handling of Nykaa's assets shall be defined, and adhered by all.
- Guidelines for internet, email, social media, and remote work usage shall be clearly outlined to prevent security breaches and misuse of company resources.
- Strict prohibitions on prohibited activities, including use of pirated software, unauthorized data transfers, and access to restricted content, shall be defined and enforced.
- IT security measures such as anti-malware controls, role-based access management, endpoint protection, and regular audits shall be implemented.
- Continuous monitoring of employee actions shall be conducted,
- Employee security awareness training shall be provided to all employees which will also include the disciplinary action which will be taken against them for non-compliance.

Refer: NYK-ISMS-POL-007-Acceptable Usage Policy for further details.

9.2 Artificial Intelligence Security Policy

- A secure, ethical, and compliant framework shall be established for deploying and managing AI systems.
- All AI operations shall uphold fairness, accountability, and transparency.
- Compliance with all applicable regulations when deploying and managing AI systems shall be maintained.
- Clear roles and responsibilities shall be defined for individuals involved in AI operations and management.
- The AI lifecycle shall be covered by the policy and will include development, deployment, monitoring, and decommissioning phases.
- Employees shall undergo regular training to ensure they are informed of AI policy guidelines, ethical standards, and regulatory requirements.

9.3 Asset Management Policy

- A comprehensive framework shall be established to manage and protect information assets throughout their lifecycle.
- All information assets, including physical and digital resources, shall be identified, classified, and assigned ownership.
- Clear accountability for the security, integrity, and availability of information assets shall be established.
- A systematic process for asset identification, registration, and periodic audits shall be established.
- Assets shall be categorized based on their value and sensitivity to Nykaa's operations.
- All media, whether physical (e.g., hard drives of laptops) or digital (e.g., cloud storage), shall be securely managed through proper labeling, storage, and disposal procedures.
- Sensitive data on media shall be encrypted to prevent unauthorized access.
- Media shall be securely transferred in accordance with established security protocols.
- Strict guidelines for media sanitization shall be implemented to protect against data leakage.
- Media containing sensitive or confidential data shall be securely disposed of or destroyed when no longer required, in compliance with industry best practices for data destruction.
- All employees, contractors, and third parties shall be trained on the proper handling, protection, and disposal of assets, particularly media.
- Asset management and media handling practices shall be updated in response to emerging threats and technologies.

Refer: NYK-ISMS-POL-018-Asset Management Policy for further details.

9.4 Authentication Policy

- A comprehensive guidelines shall be established to ensure the security and confidentiality of authentication information within the organization.
- Authentication information, including passwords, shall be non-guessable, unique, and transmitted securely.
- Users shall be required to change initial passwords upon first use.
- Users shall create strong, complex passwords and are prohibited from sharing, writing down, or revealing their passwords.
- Password management best practices shall be implemented, including the use of multi-factor authentication (MFA).
- Passwords shall be encrypted via strong encryption algorithms such as AES to ensure their security.
- Password reuse and the use of sequential patterns shall be restricted.
- Periodic password changes shall be enforced.
- Mandatory lockouts shall be implemented after multiple incorrect login attempts.

- Any compromised passwords shall be immediately reported to the appropriate authorities such as InfoSec team.
- IT and Information Security teams shall be responsible for implementing, enforcing and reviewing the implementation of these password controls.
- Periodic audits and security checks shall be conducted to ensure compliance with the policy.
- All individuals, including employees, contractors, and partners, shall adhere to these password protocols to prevent unauthorized access and data breaches.

Refer: NYK-ISMS-POL-017-Authentication Policy for further details.

9.5 Business Continuity Management Policy

- A Business Continuity Management (BCM) Policy shall be defined to ensure the resilience, availability, and security of its critical business operations, IT systems, and infrastructure.
- The policy shall outline a structured approach to identifying, assessing, mitigating, and recovering from business disruptions.
- Nykaa shall ensure operational continuity, data integrity, and compliance with regulatory requirements through the BCM policy.
- A business impact analysis (BIA) shall be conducted as part of the BCM process.
- A risk assessment shall be performed to identify potential threats to business operations.
- Crisis management and disaster recovery planning shall be mandatory to minimize disruption to critical services.
- Nykaa shall implement and maintain business continuity strategies, including redundancy, backup solutions, IT disaster recovery (DR), and emergency response protocols.
- Regular testing, audits, and employee training shall be conducted to ensure the effectiveness of business continuity strategies.
- Governance and accountability for BCM shall lie with senior leadership to ensure alignment with organizational objectives.
- Continuous monitoring, testing, and improvement of business continuity plans (BCP) and disaster recovery plans (DRP) shall be enforced.
- Crisis communication frameworks shall be integrated into the BCM policy.
- All personnel, including employees, vendors, and third parties, shall adhere to the BCM policy to uphold service continuity, safeguard assets, and maintain customer trust.

9.6 Change Management Policy

The aim of the Nykaa's Change Management Policy is to establish a structured and controlled approach to managing modifications within Nykaa's IT and business environments to ensure operational continuity, security, and compliance. It mandates a systematic process for requesting, evaluating, approving, implementing, and documenting changes across IT assets, infrastructure, software, cybersecurity, and business operations.

The objectives of the Change Management policy is the following:

- All changes shall be controlled and reviewed. For consequences arising out of unintended changes, actions shall be taken to mitigate any adverse effects, as necessary.
- The InfoSec team shall ensure that all information system security aspects are considered as part of the change management process.
- Responsibilities for initiating, approving, and executing changes or access rights shall be assigned to different individuals.
- Change managers shall ensure that the management and the individuals are aware of the impending changes and its effects on the business process as per any change.
- A documented Change Management Procedure shall be defined by Nykaa to ensure that all changes are documented and deliberated on the scope, effects in the context of the Nykaa business.

- The change manager shall evaluate and assess all the change requests for the impact of the change on the business process, its technical viability, and its impact on the security posture of the Nykaa.
- The change manager shall collaborate with representatives from Product, Development, Infosec, DevOps, QA Teams, or any other representatives considered required.

Refer: NYK-ISMS-PRO-001-Change Management Procedure for detailed Change Management process.

9.7 Clear Desk and Clear Screen Policy

To reduce the risk of unauthorized access or loss of Information, Nykaa shall enforce a clear desk and clear screen policy as follows:

- Personal or confidential business information shall be protected using security features provided. For example: Authentication control on printers. Due care shall be taken to not leave confidential material on printers or photocopiers.
- Computers shall be logged off/ locked or protected with a screen locking mechanism controlled by a password when left unattended.
- All business-related printed matter shall be disposed of using confidential waste bins or shredders.
- Desktop/ laptop screens shall be kept clear of sensitive data such as passwords.
- Whiteboards containing restricted and/ or sensitive information shall be erased after meeting or discussion.
- Sensitive or critical business information shall be securely stored in firesafe cabinets with physical logs.
- User endpoint devices shall be protected by physical locks or other appropriate security measures when not in use or left unattended.
- All computers and systems shall be configured with timeout or automatic logout features to enhance security when devices are left unattended.
- All documents and removable storage media containing sensitive information shall be securely stored and, when no longer required, disposed of using secure disposal mechanisms.

9.8 Cloud Security Policy

- A structured approach to securing Nykaa's cloud-based assets shall be defined to ensure the confidentiality, integrity, and availability of information stored and processed in cloud environments.
- Risk-based selection and evaluation of cloud service providers shall be conducted.
- Nykaa shall enforce strict security controls, compliance requirements, and contractual obligations under the shared responsibility model.
- Robust identity and access management (IAM) protocols while keeping the Role Based Access Controls (RBAC), Principle of least privilege and Segregation of Duties shall be established.
- To prevent unauthorized access into the cloud environment, multi-factor authentication (MFA) shall be enabled as default for all users.
- Cloud data security measures, such as encryption, data loss prevention (DLP), backup management, and secure data destruction, shall be enforced to protect sensitive information, including personally identifiable information (PII).
- Continuous monitoring, vulnerability assessments, and incident response mechanisms shall be implemented to ensure proactive threat detection and mitigation.
- Nykaa shall enforce service-level agreements (SLAs) with cloud providers to define security roles, compliance expectations, and exit strategies for the secure decommissioning of cloud services..

Refer: NYK-ISMS-POL-006-Cloud Security Policy for further details.

9.9 Communication Policy

- A structured framework for effective internal and external communication shall be established to ensure transparency, engagement, and alignment with organizational objectives.
- Nykaa shall ensure that communication enhances awareness, maintains corporate identity, and promotes Nykaa's reputation.
- Clear communication principles such as openness, accessibility, confidentiality, and compliance with legal regulations shall be followed.
- Internally, Nykaa shall prioritize staff engagement, team briefings, policy awareness, and two-way communication channels to foster collaboration and professional development.
- Externally, Nykaa shall aim to build stakeholder relationships, maintain public confidence, and promote Nykaa's services through media relations, digital platforms, events, and marketing initiatives.
- Roles and responsibilities for communication shall be clearly defined, with senior management accountable for policy implementation.
- Employees shall be expected to uphold professionalism and corporate integrity in all communication efforts.
- Operational guidelines for media handling, event management, advertising, and digital content strategies shall be defined and communicated to all relevant stakeholders to ensure consistency across all communication efforts.
- A proactive and reactive communication strategy, shall be considers which shall include steps for issue identification, message development, audience targeting, and evaluation.
- Nykaa shall ensure that the communication addresses business developments, crisis situations, or promotional campaigns effectively.

Refer: NYK-ISMS-POL-021-Communication Policy for detailed requirements.

9.10 Compliance Policy/ Monitoring and Compliance Policy

- A Monitoring and Compliance Policy shall be established to ensure alignment with ISO 27001:2022 standards, focusing on adherence to national and international legal, regulatory, and contractual requirements.
- A list of all applicable rules, regulations and laws shall be maintained.
- Compliance with all relevant information Security laws and regulations shall be ensured by GRC team, to safeguard Nykaa from potential legal and financial risks.
- Roles and responsibilities of the Legal and Information Security teams in relation to compliance shall be clearly defined.
- The processes for identifying, managing, and adhering to compliance obligations shall be defined and documented.
- Robust controls shall be implemented to protect sensitive data, prevent misuse of information systems, and ensure proper software licensing and intellectual property rights protection.
- Continuous monitoring and proactively management of compliance requirements shall be conducted to ensure operations remain aligned with evolving regulatory requirements..

Refer: NYK-ISMS-POL-026-Monitoring and Compliance Policy for further details.

9.11 Configuration Management Policy

- A Configuration Management policy shall be established to enforce secure configurations across its hardware, software, services, and networks.
- This policy shall apply to both newly deployed and operational systems, ensuring consistent configuration management throughout their lifecycle.
- The organization shall assign clear roles and responsibilities to ensure that all configuration changes are appropriately controlled.
- Standard templates for secure configurations shall be created, based on publicly available guidelines and vendor recommendations.

- These templates shall be designed to meet required security standards and align with Nykaa's information security policies.
- The templates shall be reviewed and updated periodically to address emerging threats, vulnerabilities, and updates to hardware and software.
- To comply with the policy, Nykaa shall minimize privileged access, disable unnecessary or insecure identities, and restrict access to critical utility programs.
- Default vendor authentication settings shall be updated immediately upon installation, and license compliance shall be verified.
- Additionally, devices shall be configured with time-out features to automatically log off after a specified period of inactivity.
- Nykaa shall record and securely store all configuration settings, maintaining logs of configuration changes through databases or templates.
- Configuration changes shall follow the established change management process, with records including ownership details, modification dates, and version history.
- Monitoring tools shall be employed to regularly assess configuration settings, password strength, and system activities.
- Any deviations from the defined configurations shall be addressed promptly, either through automated enforcement or manual intervention.
- Configuration management shall be integrated with asset management processes, ensuring the protection of configuration information from unauthorized access.

Refer: NYK-ISMS-POL-018-Asset Management Policy for further details as it contains a separate section for configuration management.

9.12 Cryptography and Encryption Policy

- A Cryptography and Encryption Policy shall be established to ensure the confidentiality, integrity, and availability of its data.
- The policy shall outline the processes for managing cryptographic keys, including generation, storage, and disposal, to secure sensitive information and maintain secure data transfers.
- The policy shall apply to all employees, contractors, vendors, and IT resources across Nykaa's platforms.
- The policy shall mandate the use of robust encryption methods like AES-256 for sensitive data and require hashing of passwords using industry-standard algorithms like bcrypt.
- Data in transit and at rest shall be encrypted using secure protocols like HTTPS and TLS.
- Removable media containing sensitive information shall be encrypted and approved by the IT department.
- Cryptographic keys shall be securely managed through a centralized system with strict guidelines for their protection, rotation, and revocation.
- Key custodians shall be responsible for managing keys, and all key management actions shall be logged.
- Keys shall be securely stored and destroyed when no longer needed.
- The policy shall ensure that all key management activities are documented and retained for auditing purposes, ensuring compliance and operational continuity.

Refer: NYK-ISMS-POL-014-Cryptography and Encryption Policy for further details.

9.13 Customer Data Management Policy

- Protection and secure handling of customer data shall be implemented across Nykaa's e-commerce platform, mobile app, and physical stores.
- Customer data shall only be stored in production systems within India and shall be secured according to Nykaa's cloud security guidelines in Cloud security policy.
- Access to production systems shall be strictly controlled, requiring approval from Nykaa's Security and Senior Management teams.

- Detailed logging and monitoring shall be implemented to ensure compliance with data protection requirements.
- Customer data shall be encrypted at all times.
- Data retention and disposal shall be managed according to customer agreements or Nykaa's internal policies.
- Data access shall be limited to authorized personnel on a need-to-know basis.
- Strong restrictions shall be applied to transferring data to non-production environments.

Refer: NYK-ISMS-POL-024-Customer Data Management policy for further details.

9.14 Data Backup and Disaster Recovery Policy

- A Data Backup policy shall be defined to address its data retention and information security requirements.
- Mechanisms shall be established to ensure that all essential information and software can be recovered in the event of an incident or failure.
- A well-defined backup plan shall be in place, which includes accurate records, documented restoration procedures, and considerations of both business and security needs.
- The backup plan shall define the frequency and type of backups, with secure off-site storage and physical and environmental protection for backup data.
- Regular testing of backup media and restoration procedures shall be conducted to ensure reliable recovery.
- Backups shall be encrypted as needed to safeguard sensitive information.
- Operational procedures shall be in place to monitor backup execution and address any failures to maintain completeness.
- Backup measures for critical systems and services shall be tested regularly to support incident response and business continuity objectives.
- Nykaa shall verify that its cloud providers' backup services meet the company's backup requirements.
- The retention periods for essential business information shall be determined in compliance with legal and regulatory obligations.
- Expired backup data shall be securely deleted to maintain regulatory compliance.

Refer: NYK-ISMS-POL-002-Data Back-up and Disaster Recovery Policy for further details.

9.15 Data Privacy Policy

- A comprehensive framework shall be established for collecting, processing, storing, and securing personal data, ensuring compliance with applicable data protection laws.
- The policy shall apply to current, former, and prospective employees and define key roles such as Personal Data, Sensitive Personal Data, Data Fiduciaries, Data Processors, and Data Privacy Officers (DPOs) to govern data handling.
- Nykaa shall collect various employee-related personal data, including identification, payroll, biometric, employment history, performance records, and emergency contact details, with strict transparency and notification procedures in place.
- The collected data shall be used for payroll processing, benefits administration, performance evaluation, legal compliance, security, and fraud prevention.
- Nykaa shall only share personal data with authorized third-party service providers, such as insurance companies, payroll processors, and legal entities, ensuring they adhere to strict data protection requirements.
- In specific legal or compliance scenarios, personal data shall be shared without explicit consent, as required by law.

- Nykaa shall employ robust security measures to protect personal data, including encryption, controlled access, and compliance with industry best practices.
- Employees shall have the right to access, modify, delete, or request data portability of their personal data, and Nykaa shall address data subject requests within stipulated legal timelines.
- Incident response mechanisms shall be implemented to ensure timely notification of data breaches to both regulatory authorities and affected individuals.
- Personal data shall be retained only for as long as necessary for employment, legal, and business purposes, with strict deletion procedures in place.
- Nykaa shall periodically review and update its privacy policies and ensure employees are informed of any changes.
- Employees shall be able to contact the Data Privacy Officer (DPO) for inquiries or complaints, with the option to escalate concerns to the relevant data protection authorities.

Refer: Nykaa Data Privacy Policy for further information.

9.16 Data Protection Policy

- Nykaa shall draft a Data Protection Policy to ensure the integrity, confidentiality, and availability of its data.
- The policy shall govern the entire data lifecycle, focusing on security, regulatory compliance, and resource
- The policy shall outline the secure retention, classification, and disposal of data to protect sensitive information, reduce data-related risks, and promote operational efficiency.
- Violations of the policy shall be considered breaches, with corrective or disciplinary actions taken as necessary.
- Nykaa shall store data securely in systems like SharePoint and databases, minimizing physical storage.
- Data shall be classified by sensitivity and retained based on business needs or legal requirements, with specific retention periods for assets like contracts, payroll, and financial records.
- Retention periods for data shall be set by department heads and cannot be altered without proper justification.
- Data at the end of its retention period shall be securely deleted or destroyed using methods like shredding, degaussing, or data wiping, with encryption required before disposal.
- Only authorized personnel shall handle data deletion, and records of disposal shall be maintained for audit purposes.
- Extensions for data retention shall require justification and approval.
- Data media, such as hard drives and tapes, shall be securely disposed of using appropriate methods based on data sensitivity.
- Backup shall be ensured before disposal of data media.
- Third-party vendors shall meet the appropriate disposal standards for data media.

Refer: NYK-ISMS-POL-025-Data Protection Policy for further details.

9.17 DLP Policy

- Nykaa shall establish a comprehensive Data Leakage Prevention (DLP) process to protect sensitive and confidential data from unauthorized access, disclosure, or loss, ensuring compliance with legal and regulatory requirements.
- The policy shall apply to all employees, contractors, and stakeholders, fostering a culture of data security and accountability across Nykaa.
- Non-compliance with the DLP policy shall result in disciplinary or corrective action.
- Nykaa shall define clear roles and responsibilities for DLP governance, including the Chief Information Security Officer (CISO) for overall enforcement, the Data Protection Officer (DPO) for compliance

oversight, the Information Security Team for monitoring technical aspects, and End Users for adhering to data handling practices.

- The Incident Response Team shall investigate DLP violations, assess risks, and mitigate threats.
- Nykaa shall deploy DLP tools across all endpoints, email gateways, and network channels to monitor, detect, and prevent data breaches while ensuring business continuity.
- DLP controls shall include blocking unauthorized actions or transmissions involving sensitive information, such as copying database entries, uploading data to non-Nykaa cloud services, or AI platforms like ChatGPT.
- Sensitive data shall be encrypted during storage, transmission, and at rest.
- High-risk channels, including email, internet access, file transfers, mobile devices, and portable storage media, shall be monitored.
- Data transmissions shall be quarantined and restricted when unauthorized sharing is detected.
- Strict access controls shall be enforced on data exports and transfers, ensuring that data owners approve sensitive data exports.
- Unauthorized screenshots or photographs shall be prevented through policies, employee training, and auditing.
- Nykaa's DLP Tool shall proactively log, warn, and block unauthorized data transfers across email, print, network uploads, USB devices, and external storage.
- The Information Security Team shall conduct regular audits to assess the effectiveness of DLP measures, fine-tune policies, and adapt to emerging threats.
- Any changes to the DLP policy or configuration shall follow formal risk assessment and change management procedures.
- Nykaa shall consider advanced DLP tactics, such as decoy information (honeypots), to mislead potential attackers and prevent espionage.
- Real-time alerts shall be provided to users when risky behavior is detected, fostering immediate awareness and corrective action.

9.18 HR Security Policy

- Nykaa shall implement a Human Resource Security Policy to protect personnel-related information and organizational assets by enforcing robust security measures across the company.
- The policy shall establish clear protocols for screening, onboarding, and conducting periodic background checks for all employees, contractors, and third parties, emphasizing confidentiality and data protection.
- Employees shall be required to sign confidentiality agreements and assume specific security responsibilities, with defined consequences for non-compliance.
- The policy shall address the management of employee terminations, role changes, and access control to ensure the secure handling of sensitive information throughout employment.
- Regular security awareness training shall be mandatory for all employees.
- The policy shall be reviewed annually to ensure alignment with industry standards, such as ISO 27001:2022.
- Nykaa shall reinforce its commitment to maintaining a secure and trusted environment for all stakeholders by ensuring adherence to this policy.

Refer: NYK-ISMS-POL-011-HR Security Policy for more details

9.19 Identity & Access Management Policy

- Nykaa shall outline principles and practices for securely managing digital identities and controlling access to its information systems through the Identity and Access Management (IAM) Policy and shall maintain Segregation of Duties (SOD) for all allocated roles and responsibilities.
- The policy shall cover user identity creation, access management, account termination, and user off-boarding to safeguard Nykaa's data and systems.
- Key controls shall include role-based access, privileged account monitoring, regular user access reviews, and two-factor authentication for sensitive access.

- The policy shall emphasize the need for clear authorization processes, password management, and strict oversight of shared, emergency, and privileged accounts.
- Network and cloud access controls, along with session management, shall be enforced to ensure secure connections and compliance with security standards.
- The policy shall be subject to annual review and audits to maintain regulatory compliance and operational integrity.

Refer: NYK-ISMS-POL-020-Identity and Access Management Policy for further details.

9.20 Information Classification and Labelling Policy

- Nykaa shall implement an Information Classification and Labelling Procedure to ensure the proper classification, labelling, and handling of information and information systems.
- The procedure shall support Nykaa's commitment to protecting critical business information and maintaining the confidentiality, integrity, and availability of data across its operations.
- The procedure shall provide clear instructions to Nykaa employees, vendors, and contractors on how to classify and handle various types of information, both electronic and physical.
- Nykaa shall define four levels of information classification—Public, Internal, Confidential, and Sensitive—each with defined risks and impacts associated with unauthorized disclosure or destruction.
- Information shall be stored, transmitted, and handled with appropriate security measures based on its classification.
- Information shall be labelled according to its classification level, with specific handling controls for each type of data, including storage, transmission, and disposal protocols.
- The procedure shall apply to all personnel and all types of information that Nykaa processes, stores, or destroys.
- Specific guidelines shall be followed for the secure storage of information, including encryption and password protection.
- The procedure shall detail controls for the handling of printed and electronic documents and email communications.
- Sensitive data shall be masked when shared, used for testing, or analyzed.
- Nykaa shall implement strict access controls, multi-factor authentication, and monitoring of information to ensure compliance with security standards.
- Proper disposal techniques for both digital and physical media shall be followed to prevent unauthorized access or data leaks.
- The procedure shall be reviewed annually and updated as needed based on audits, regulatory changes, or modifications to Nykaa's security practices.
- Violations of the policy shall be treated as breaches and may result in disciplinary actions.

Refer: NYK-ISMS-PRO-013-Information Classification and Labelling Procedure for further details.

9.21 Logging and Monitoring Policy

- Nykaa shall implement a Logging and Monitoring Policy to safeguard its digital assets and ensure the confidentiality, integrity, and availability of its information systems.
- The policy shall apply to all employees, contractors, consultants, and partners interacting with Nykaa's IT infrastructure.
- Nykaa shall establish structured guidelines for the collection, analysis, and retention of log data to identify and mitigate security risks.
- The policy shall define clear roles and responsibilities for key stakeholders, including the Head of Information Security, IT, DevOps, and application owners, to ensure adherence to security protocols and effective log management.
- Log data shall be secured from unauthorized access to protect sensitive information such as Personally Identifiable Information (PII).
- Logs shall be retained for a minimum of one year to meet compliance and audit requirements.

- Continuous monitoring shall be implemented, with automated analysis and the use of advanced tools to detect anomalies.
- Nykaa shall ensure that its infrastructure is fortified against evolving security threats through effective logging and monitoring practices.

Refer: NYK-ISMS-POL-007-Logging and Monitoring Policy for further details.

9.22 Malware Protection Policy

- Nykaa shall implement a Malware Protection Policy to safeguard its digital infrastructure, IT systems, and sensitive information against evolving malware threats, including viruses, worms, Trojans, spyware, and ransomware.
- The policy shall mandate the deployment, configuration, and continuous monitoring of advanced anti-malware solutions across all endpoints, servers, networks, and cloud environments.
- Nykaa shall enforce real-time protection, scheduled scans, intrusion detection, and automated updates to mitigate security risks associated with malware.
- Strict access controls shall be implemented, with threat intelligence integration and incident response mechanisms to ensure rapid detection, containment, and remediation of malware incidents.
- The policy shall apply to all employees, contractors, third parties, and IT assets.
- Clear roles and responsibilities shall be assigned across Information Security, IT, and DevOps teams to ensure accountability for malware protection.
- Unauthorized software, malicious websites, and unapproved system changes shall be strictly prohibited, with exceptions managed through a formal approval process.
- Compliance with the policy shall be mandatory, with regular audits, logging, and post-incident reviews conducted to continuously enhance Nykaa's cyber resilience.

Refer: NYK-ISMS-POL-003-Malware Protection Policy for further details.

9.23 Network Security Policy

- Nykaa shall implement a Network Security Policy to protect its network infrastructure, data transmission, and access controls from unauthorized access, cyber threats, and security breaches.
- The policy shall ensure the confidentiality, integrity, and availability of network resources through robust access control mechanisms, segmentation, firewalls, intrusion prevention, monitoring, and incident response protocols.
- Nykaa shall mandate the use of multi-factor authentication (MFA), VPN enforcement, secure wireless configurations, encryption protocols, and role-based access control (RBAC) to safeguard network access.
- Comprehensive logging, real-time network monitoring, web filtering, and endpoint security enforcement shall be implemented to detect and mitigate security threats.
- Formal change management, periodic audits, vulnerability assessments, and third-party interconnection security reviews shall be conducted to ensure ongoing compliance with industry best practices and regulatory requirements.
- Cloud network security controls, time synchronization mechanisms, and data protection measures shall be enforced to secure hybrid and virtualized environments.

Refer: NYK-ISMS-POL-003-Malware Protection Policy for further details.

9.24 Physical and Environmental Security Policy

- Nykaa shall implement a comprehensive Physical and Environmental Security Policy to safeguard its assets, personnel, and facilities from internal and external threats.
- The policy shall ensure the protection of buildings, equipment, and data centers from threats such as fire, natural disasters, theft, and terrorism, while promoting operational continuity and employee safety.

- Nykaa shall apply this policy to all employees, contractors, and authorized personnel with access to Nykaa's physical and environmental assets, including office buildings, data centers, and storage facilities.
- Strict access controls shall be implemented, including security checks for visitors, baggage inspections, and the use of identification badges.
- All sensitive areas shall be classified into four security levels, with restricted access based on the level of sensitivity.
- Physical security measures shall include secure perimeters, alarm systems, CCTV, and continuous monitoring to prevent unauthorized access.
- Specific guidelines shall be implemented for protecting against environmental threats like fire, flooding, and earthquakes, with required safety equipment and regular testing of fire detection and suppression systems.
- Secure areas shall be strictly controlled to prevent unauthorized activity, with provisions for the secure handling of prohibited or restricted items.
- Nykaa shall ensure the secure siting of equipment and utilities, ensuring proper environmental controls for sensitive systems.
- Procedures shall be implemented for material movement, including thorough security checks for incoming and outgoing materials, with all movements documented and authorized.
- The policy shall provide a comprehensive approach to managing physical and environmental risks, ensuring a secure and resilient operating environment.

Refer: NYK-ISMS-POL-012-Physical and Environmental Security Policy for further details.

9.25 Remote Working Policy

- Nykaa shall outline comprehensive guidelines for remote work, addressing physical security, equipment management, network and data security, system integrity, working schedules, and performance.
- Remote working sites shall address physical security and environmental risks, while employees shall be responsible for securing company-provided equipment and ensuring a safe and suitable workspace.
- All remote workers shall connect to Nykaa's network via an approved VPN with two-factor authentication, adhering to strict data security practices, including proper handling and disposal of sensitive information.
- Regular software updates and antivirus scans shall be mandatory for device security.
- Employees shall maintain the same level of productivity, communication, and performance as in-office work, with regular evaluations to ensure ongoing compliance.
- Timely system patching and updates shall be mandated to maintain system integrity.
- Upon cessation of remote work, access to company networks and assets shall be revoked, and all temporary equipment shall be returned within five business days.
- For employees utilizing personal devices (BYOD), the policy shall emphasize the need for compliance with Nykaa's security protocols, including encryption, VPN usage, and secure storage practices.
- Employees shall create an environment conducive to productivity while maintaining a secure, compliant setup, including using company-approved communication tools, participating in virtual meetings, and ensuring reliable internet connectivity.
- BYOD users shall meet Nykaa's security standards to ensure safe remote access to company systems and information.

Refer: Draft_NYK-ISMS-POL-013-Remote Working Policy for further details.

9.26 SDLC Policy

- The SDLC Policy shall establish a structured approach towards the entire Software Development Lifecycle process.
- The document shall provide guidance towards the software development principles such as General Principles for Secure Development Life Cycle, Application Security Principles, Test Data Security, Code Repository Security Principles, Secure Branching Principles, Secure Code Pull Request (PR) and Merging

Process, Secure Third Party Integration Principles, Securing Sensitive Integration Keys, and Securing Mobile Applications.

- The document shall describe the requirements of drafting Secure coding practices for Development teams.
- Training shall be provided to developers on secure coding practices.
- Role-based access control (RBAC) or attribute-based access control (ABAC) shall be enforced while adhering to the principle of least privilege.
- Controls for Input and output validations shall be implemented within the application/ service during the development process.
- Implementation of data protection mechanisms shall be implemented at all stages of data processing, transmission, and storage.
- Regular security assessments, including web application penetration tests, source code reviews, vulnerability assessments, and transactional security testing shall be conducted.
- Security of test data shall be maintained throughout the development lifecycle.
- Management of source code repositories shall be done in accordance with security best practices.
- Multi-Factor Authentication (MFA) for all user access shall be enforced.
- Quarterly access reviews shall be conducted to ensure only the required stakeholders have the access.
- Management protocols for branches and naming conventions in source code shall be established.
- Peer reviews shall be mandatory for every pull request.
- CI/CD pipeline security shall be secured as per the industry best practices.
- Security requirements shall be considered at each stage of the development lifecycle, including Sprint Planning and Grooming (Planning and Requirement Gathering), Development, Testing, Deployment, and Securing the Deployment.
- Secure Artifact repository and Dependency management practices shall be defined and followed during the deployment phase.
- Applications and services, once they are no longer in use, shall be securely Disposed or Retired.

Refer: NYK-ISMS-POL-008-SDLC Policy for detailed SDLC requirements.

9.27 System Acquisition, Development, and Maintenance Policy

- The System Acquisition, Development & Maintenance Policy shall be defined to ensure the secure, efficient, and compliant management of IT systems throughout their lifecycle.
- The policy shall cover acquiring, developing, and maintaining IT systems, with a focus on risk minimization and value maximization.
- The policy shall apply to all Nykaa personnel, vendors, suppliers, and authorized individuals handling sensitive information or managing IT systems that store, process, or transmit such data.
- Strict adherence to software licensing and installation protocols shall be enforced, ensuring that only authorized and licensed software is used within Nykaa.
- All software installations, whether on desktops, laptops, or servers, shall require prior approval from relevant teams to comply with licensing and security standards.
- The IT team, in coordination with other teams such as DevOps, shall manage and monitor the software inventory to prevent unauthorized use and ensure license compliance.
- Process for acquiring new software or technology shall be clearly defined, incorporating security requirements into the selection and evaluation process to maintain confidentiality, integrity, and availability of business-critical assets.

Refer: NYK-ISMS-POL-026-System Acquisition, Development, and Maintenance Policy for further details.

9.28 Third-party Risk Management Policy

- A structured approach shall be established for assessing, monitoring, and mitigating risks associated with Nykaa's vendors, contractors, suppliers, and third-party service providers.

- The policy shall ensure governance, compliance, and risk control in outsourced services to safeguard Nykaa from business continuity disruptions, data breaches, financial losses, and regulatory non-compliance.
- Rigorous due diligence shall be conducted, with vendor classification based on risk exposure.
- Contractual security clauses shall be included in vendor agreements.
- Regular audits, and periodic assessments shall be conducted.
- Roles and responsibilities shall be clearly defined across business stakeholders, procurement, legal, and information security teams to ensure accountability in vendor onboarding, data protection, access control, and security compliance.
- Third-party vendors shall be classified into Highly Critical, Critical, Significant, and Non-Essential categories, with security controls, audit frequency, and risk scoring tailored to their classification.
- Formal agreements, service level agreements (SLAs), security audits, continuous monitoring, and contractual obligations shall be enforced, ensuring that only compliant third parties gain access to Nykaa's systems and data.

Refer: NYK-ISMS-POL-009-Third-Party Risk Management Policy for further information.

9.29 Threat Intelligence Policy

- A comprehensive threat intelligence program shall be established to ensure appropriate responses and recovery measures are in place for all levels of threat intelligence: strategic, tactical, and operational.
- Nykaa shall collect, analyze, and continuously monitor information on existing and emerging threats from a variety of reliable sources, both internal and external.
- This collection and analysis shall facilitate proactive and informed decision-making to prevent harm to Nykaa's operations, assets, and stakeholders, while minimizing the impact of potential threats.
- Nykaa shall address three critical layers of threat intelligence as part of its approach:
    - Strategic Threat Intelligence: Focused on high-level information about the evolving threat landscape, such as understanding attacker motivations, attack methods, and broader industry trends. This intelligence informs long-term planning and policy development.
    - Tactical Threat Intelligence: Emphasizing details on attacker methodologies, tools, and technologies, enabling Nykaa to enhance its detection and prevention capabilities.
    - Operational Threat Intelligence: Providing specific and actionable details about known attacks, such as indicators of compromise (IoCs), tactics, techniques, and procedures (TTPs), and targeted vulnerabilities.
- Nykaa shall ensure the quality of threat intelligence by adhering to the following principles:
    - Insightful: Threat intelligence shall provide a detailed and accurate understanding of the threat landscape to enable informed decision-making.
    - Contextual: Threat intelligence shall include situational awareness to add context and relevance to the information, making it meaningful to Nykaa's environment and operations.
    - Actionable: Threat intelligence shall enable timely and effective actions, allowing Nykaa to mitigate risks quickly and efficiently.
- Nykaa shall integrate threat intelligence into its risk management processes, ensuring that insights from intelligence sources enhance risk assessments, technical controls, and security testing.
- Nykaa shall foster collaboration and information sharing, exchanging threat intelligence with other organizations, industry groups, and regulatory bodies on a mutual basis to strengthen collective defense capabilities and improve overall situational awareness.
- Nykaa shall utilize threat intelligence for multiple purposes, including:
    - Preventing, detecting, and responding to threats.
    - Producing its own threat intelligence using internal resources and expertise.
    - Relying on threat intelligence produced by trusted external sources to complement internal efforts.

- Nykaa shall establish mechanisms to operationalize threat intelligence, ensuring that intelligence insights are effectively translated into actionable controls, security measures, and decision-making processes.
- Nykaa may use automated tools and platforms to collect, analyze, and disseminate threat intelligence efficiently, leveraging technology to improve accuracy and scalability.
- Nykaa shall periodically review and update its threat intelligence processes, ensuring alignment with evolving threats, technologies, and best practices in threat intelligence management.

9.30 Information Security Training and Awareness Policy

- Nykaa's Internal Information Security Training and Awareness Policy shall aim to equip all personnel with the knowledge and skills needed to identify and mitigate cybersecurity risks, fostering a culture of security compliance.
- The policy shall apply to all employees, contractors, partners, and authorized users across Nykaa's operations.
- The program shall include mandatory annual security training, onboarding security induction for new employees, quarterly phishing simulation campaigns, and role-specific security training.
- The training program shall cover key topics such as Nykaa's security policies, legal responsibilities, and individual accountability for safeguarding information.
- The effectiveness of the training program shall be evaluated through quizzes and feedback, with escalation procedures in place for incomplete training.
- The policy shall be reviewed annually to ensure compliance with regulatory requirements.
- Management shall receive biannual reports on the program's effectiveness.

Refer: NYK-ISMS-POL-015-Information Security Training and Awareness Policy for further details.

9.31 Vulnerability and Patch Management Policy

- A comprehensive and accurate inventory of IT assets to effectively manage vulnerabilities and ensure timely patching. This will include various asset types such as servers, endpoints, cloud resources, and applications, with regular vulnerability assessments and penetration tests.
- Responsibilities for managing vulnerabilities shall be clearly defined across teams, including IT, DevOps, and engineering.
- Nykaa shall employ automated tools like Qualys for vulnerability scanning and ensure asset accountability through designated owners.
- The patch management process shall ensure that patches are tested and deployed in a controlled environment, with critical vulnerabilities addressed immediately.
- The process shall include risk-based patching, prioritizing patches based on asset criticality, vulnerability severity, and exploitability.
- Regular scans, penetration tests, and continuous monitoring shall be employed to assess patch effectiveness and address any system disruptions post-deployment.
- Nykaa shall ensure that suppliers follow vulnerability reporting protocols and consider using bug bounty programs for external vulnerability identification.

Refer: NYK-ISMS-PRO-011-Vulnerability And Patch Management Procedure for further details.

9.32 Incident Management policy

Nykaa shall establish and maintain an information security incident management process to ensure timely detection, response, and resolution of security incidents.

- Clearly defined roles and responsibilities shall be assigned for reporting, managing, and responding to security incidents. Competent personnel shall handle incidents, with training and professional development provided as needed.
- A structured process shall be implemented for detecting, classifying, analyzing, and responding to incidents, including containment, evidence collection, escalation, and coordination with internal and external stakeholders.

- Standardized reporting procedures shall be in place, ensuring prompt reporting, tracking, and communication of incidents while maintaining compliance with legal and regulatory requirements.
- Post-incident analysis, root cause identification, and corrective measures shall be conducted to improve incident response and prevent recurrence. Lessons learned shall be used to enhance security controls, risk assessments, and awareness programs.
- Procedures shall be established to ensure the proper collection, preservation, and documentation of digital evidence, meeting legal and regulatory requirements across relevant jurisdictions.

Refer: NYK-ISMS-PRO-008-Incident Management Procedure for further details.

9.33 InfoSec Internal Audit policy

Nykaa shall establish and maintain a process for conducting independent reviews of its information security framework to ensure effectiveness, compliance, and continuous improvement.

- Periodic independent reviews shall be planned and initiated by management to assess the adequacy of information security policies, controls, and implementation. These reviews shall identify opportunities for improvement and necessary changes.
- Reviews shall be conducted by individuals who are independent of the area under review, such as internal auditors, independent managers, or external specialists, ensuring unbiased assessments. Reviewers shall possess the required competence and shall not be in the line of authority of the reviewed function.
- Findings from independent reviews shall be reported to the initiating management and, where necessary, to senior leadership. Management shall ensure that corrective actions are taken if the reviews indicate non-compliance or inadequacies in security measures.
- Independent reviews shall also be conducted in response to significant changes, such as regulatory updates, major security incidents, business expansion, or modifications to security controls.
- Records of all independent reviews shall be maintained to support accountability, tracking of improvements, and future assessments.

9.34 Information Security in the Project Management

Information security shall be integrated into project management to ensure risks are identified, assessed, and addressed throughout the project lifecycle, regardless of the project's size, complexity, or application area. Key requirements shall include:

- Security risks shall be assessed early and periodically reviewed, with effective treatment measures implemented and evaluated.
- Projects shall incorporate security requirements from policies, regulations, and threat assessments, ensuring compliance with legal and contractual obligations.
- Security responsibilities shall be clearly allocated within the project team, with governance oversight at key project stages.
- Internal and external communication security, access controls, transaction logging, and monitoring mechanisms shall be considered.
- Security expectations for vendors and external parties shall align with organizational policies and be enforced through contracts.

10. Policy Compliance and Governance

Strict adherence to this policy is essential to maintaining Nykaa's ISMS Standard and operational integrity. Any deviation shall be considered a breach of company policies and may result in disciplinary or corrective action. To ensure ongoing compliance with Nykaa's Governance Framework, ISO 27001:2022, and all relevant regulatory requirements, this document shall undergo a formal review at least annually to maintain its accuracy and relevance. Additionally, any significant findings from internal or external audits, regulatory changes, or substantial modifications to Nykaa's information security practices, IT infrastructure, or broader operational framework shall trigger an immediate review and update. All revisions shall be systematically documented and formally approved to uphold the policy's effectiveness and alignment with evolving compliance standards.

11. Annexures and References

Annexure I - Glossary

Terms	Description
ISP	Information Security Policy
ISC	Information Security Committee
IST	Information Security team
IT	Information Technology
SLA	Service Level Agreement
HOD	Head of Department
IPR	Intellectual Property Rights
ISMS	Information Security Management System
VPN	Virtual Private Network
NDA	Non-Disclosure Agreement
LAN	Local Area Network
DC	Data Center
OS	Operating System
HR	Human Resources
ICT	Information and communication technology
Data/ Asset owner	A person to whom an information or information asset is assigned
Data/ Asset custodian	A person who is responsible for day-to-day operations and maintenance of an information or information asset
Data/ Asset User	A person who uses information or information assets in course of their job responsibilities
Administrator	A person who has administrative access/ privileges to system components including hardware, software, and services.
Third Party	An external party on a short- or long-term engagement with Nykaa. Third parties include vendors, contractors, suppliers, consultants, business partners and auditors. Third party excludes customers.

Annexure II - Reference

S. No.	Circular Reference	Description
1.	ISO/IEC 27001:2022	ISO/IEC 27001:2022 recommends information security controls addressing information security control objectives arising from risk to the confidentiality, integrity, and availability of information.