

Information Security Policy

A public statement of Nykaa's information security principles, commitments and protection practices.

Document Control

Field	Value	Field	Value
Document title	Information Security Policy	**Classification**	Public
Document owner	Information Security Team	**Version**	2.1
Effective date	18/03/2026	**Review**	Annual / as required
Applies to	Refer Scope section 3 of Document	**Status**	Approved for public disclosure

Public Disclosure Note

This document is deliberately written at a principle and commitment level. Detailed security standards, procedures, technical architecture, control configurations, internal risk criteria, security tooling, operational thresholds and other sensitive information are maintained separately and are not part of this public policy.

Table of Contents

1. Introduction 4
2. Purpose 4
3. Scope 4
4. Information Security Principles 4
5. Information Security Governance 4
6. Risk Management 5
7. Information and Asset Management 5
8. Information Classification and Data Protection 5
9. Privacy and Personal Data Protection 5
10. Identity and Access Management 6
11. Authentication and Credential Security 6
12. Cloud and Technology Security 6
13. Application and Secure Development 6
14. Vulnerability and Patch Management 7
15. Malware and Endpoint Security 7
16. Network and Communications Security 7
17. Logging, Monitoring and Security Detection 7
18. Data Loss Prevention 8
19. Cryptography and Encryption 8
20. Business Continuity and Disaster Recovery 8
21. Incident Management 8
22. Threat Intelligence 9
23. Third-Party and Supplier Security 9
24. Human Resources and Security Awareness 9
25. Acceptable Use and Responsible Technology Use 9
26. Artificial Intelligence Security 10
27. Physical and Environmental Security 10
28. Remote and Mobile Working 10
29. Change and Configuration Management 10
30. Information Security in Projects 10
31. Compliance and Legal Requirements 11
32. Security Assurance, Audit and Review 11
33. Continuous Improvement 11
34. Roles and Responsibilities 11
35. Reporting Security Concerns 12
36. Policy Governance 12
37. Public Disclosure Statement 12
38. Reference Frameworks 12

1. Introduction

Nykaa recognizes that information is a critical business asset and that protecting information is fundamental to maintaining the trust of our customers, employees, business partners and other stakeholders.

- Protect information and technology assets against unauthorized access, use, disclosure, alteration, loss, disruption or destruction.
- Maintain the confidentiality, integrity and availability of information.
- Manage information security risks in a structured and risk-based manner.
- Support secure and resilient business operations.
- Meet applicable legal, regulatory and contractual obligations.
- Promote information security awareness and accountability.
- Continually improve information security practices.

These commitments apply across relevant digital, physical, cloud and technology environments.

2. Purpose

This policy establishes Nykaa's public commitment to protecting information and managing information security risks. It provides an external overview of the principles and security domains through which information security is managed.

3. Scope

This policy applies broadly to information and technology resources used to support Nykaa's business operations, including information processed, stored or transmitted through digital, physical, cloud-based and other technology environments.

- Employees and other personnel.
- Contractors and consultants.
- Suppliers, service providers and business partners, where applicable.
- Information systems, applications and technology assets used in support of Nykaa's operations.

Specific security requirements may vary according to the nature, sensitivity, risk and regulatory requirements associated with an information asset or business activity.

4. Information Security Principles

Nykaa's information security approach is based on the following principles:

- Confidentiality — protecting information against unauthorized access, disclosure or use.
- Integrity — protecting information against unauthorized or inappropriate modification.
- Availability — supporting reliable and resilient access to information and services.
- Risk-based security — identifying, assessing and addressing risks according to potential impact and likelihood.
- Security by design — considering security throughout relevant business, technology, product, application and project lifecycles.
- Continuous improvement — strengthening security practices as business needs, technology, threats and requirements evolve.

5. Information Security Governance

Nykaa maintains an information security governance framework designed to provide appropriate oversight, accountability and direction.

- Establishing information security objectives and policies.
- Identifying and managing information security risks.

- Monitoring security performance.
- Reviewing significant security matters.
- Supporting compliance with applicable requirements.
- Promoting continual improvement.

Detailed internal governance structures, committees, reporting mechanisms and approval authorities are maintained as internal information.

6. Risk Management

Nykaa follows a structured, risk-based approach to identifying and managing information security risks.

- Identification and assessment of information security risks.
- Evaluation of potential business impact and likelihood.
- Identification and evaluation of appropriate security measures.
- Risk treatment and mitigation.
- Monitoring and periodic reassessment.
- Management of residual risk where appropriate.

Risks may be reassessed when there are significant changes to business operations, technology, systems, regulatory requirements or the threat environment.

7. Information and Asset Management

Nykaa identifies and appropriately protects information and technology assets throughout their lifecycle.

- Asset identification and ownership.
- Appropriate classification of information.
- Secure handling and storage.
- Protection against unauthorized access or use.
- Secure transfer where appropriate.
- Appropriate retention and disposal.
- Protection of physical and digital media.

8. Information Classification and Data Protection

Information is protected according to its sensitivity and business importance.

- Appropriate classification and handling.
- Access based on legitimate business requirements.
- Protection of sensitive and personal information.
- Secure storage and transmission.
- Appropriate retention and secure disposal.
- Measures to reduce unauthorized disclosure or loss.

Requirements may differ based on applicable legal, regulatory, contractual and business requirements.

9. Privacy and Personal Data Protection

Nykaa is committed to protecting personal information entrusted to it by customers, employees, business partners and other stakeholders.

- Lawful and responsible processing of personal information.
- Appropriate security safeguards.
- Access and use based on legitimate requirements.
- Appropriate retention and disposal.
- Management of data protection risks.

- Handling of applicable privacy-related requests.
- Response to personal data incidents in accordance with applicable requirements.

Further information about personal information processing may be provided through Nykaa's applicable privacy notices and policies.

10. Identity and Access Management

Nykaa applies access management principles intended to ensure that information and systems are accessible only to appropriately authorized individuals.

- Appropriate authorization before access is granted.
- Access based on business need and role.
- Least-privilege principles where appropriate.
- Protection of privileged access.
- Appropriate authentication mechanisms.
- Periodic review of access.
- Timely modification or removal of access when circumstances change.

Detailed access configurations and security mechanisms are maintained internally.

11. Authentication and Credential Security

Nykaa takes measures to protect authentication information and reduce the risk of unauthorized access.

- Protect authentication credentials.
- Do not share passwords or authentication information.
- Use strong authentication practices.
- Follow applicable multi-factor authentication requirements.
- Report suspected credential compromise through appropriate channels.

Technical authentication configurations and security parameters are maintained as internal information.

12. Cloud and Technology Security

Nykaa recognizes the security considerations associated with cloud computing and technology services.

- Security assessment of relevant technology services.
- Appropriate access controls.
- Data protection measures.
- Encryption where appropriate.
- Security monitoring.
- Vulnerability management.
- Resilience and recovery measures.
- Appropriate contractual and security requirements for service providers.

Specific technology platforms, configurations, architectures and security tooling are not disclosed in this public policy.

13. Application and Secure Development

Security is considered throughout relevant application and technology lifecycles.

- Identification of security requirements.
- Secure design and development practices.
- Appropriate access controls.
- Protection of application data.
- Security testing and assessment.

- Management of third-party integrations.
- Protection of development and testing environments.
- Secure deployment and maintenance.
- Secure retirement of applications and technology assets.
- Detailed development standards and technical security requirements are maintained internally.

14. Vulnerability and Patch Management

Nykaa maintains processes to identify and manage technology vulnerabilities and security weaknesses.

- Identification of vulnerabilities.
- Risk-based prioritization.
- Security testing and assessment.
- Timely remediation of significant vulnerabilities.
- Security patch management.
- Monitoring of remediation activities.
- Evaluation of emerging security threats.

Specific vulnerability-management tools, configurations, scan schedules and technical thresholds are not disclosed publicly.

15. Malware and Endpoint Security

Nykaa applies appropriate security measures to protect endpoints and technology environments against malicious software and other threats.

- Endpoint protection.
- Malware detection and prevention.
- Security updates.
- Device configuration controls.
- Security monitoring and alerts.
- Protection of removable media where appropriate.
- Security awareness and user guidance.

16. Network and Communications Security

Nykaa maintains appropriate measures to protect communications and networked environments.

- Network access controls.
- Secure communications.
- Protection against unauthorized access.
- Monitoring of relevant security events.
- Segmentation or other appropriate security measures.
- Protection of information transmitted across networks.

Detailed network architecture, configurations and security controls are maintained as confidential internal information.

17. Logging, Monitoring and Security Detection

Nykaa uses appropriate monitoring and security practices to support the detection and investigation of security events.

- Collection and protection of relevant security information.
- Identification of unusual or potentially malicious activity.
- Security event analysis.
- Investigation and escalation of significant events.
- Retention of relevant records in accordance with applicable requirements.

Specific monitoring technologies, detection rules, alert thresholds and retention configurations are not disclosed in this public policy.

18. Data Loss Prevention

Nykaa implements appropriate measures to reduce the risk of unauthorized disclosure, transfer or loss of sensitive information.

- Data handling requirements.
- Access controls.
- Monitoring of relevant information transfer channels.
- Protection of sensitive information.
- Appropriate restrictions on unauthorized data sharing.
- Security awareness and user education.

Detailed DLP technologies, rules and configurations are maintained internally.

19. Cryptography and Encryption

Nykaa uses appropriate cryptographic and encryption measures to protect information where required by risk, sensitivity, technology and applicable requirements.

- Encryption may be applied to information during storage, transmission or other relevant stages of its lifecycle.

Specific cryptographic configurations, algorithms, keys and implementation details are maintained as internal security information.

20. Business Continuity and Disaster Recovery

Nykaa recognizes the importance of maintaining resilient business operations and recovering from disruptive events.

- Business impact and risk assessments.
- Continuity planning.
- Disaster recovery planning.
- Data backup and recovery measures.
- Resilience measures for critical services.
- Testing and validation of recovery capabilities.
- Crisis management and communications.
- Continual improvement based on lessons learned.

Specific recovery architecture, recovery parameters and operational procedures are maintained internally.

21. Incident Management

Nykaa maintains an information security incident management capability to support timely identification, assessment, response and resolution.

- Identification and reporting.
- Assessment and classification.
- Containment and response.
- Investigation and evidence preservation.
- Communication and escalation.
- Recovery and resolution.
- Root-cause analysis and lessons learned.
- Corrective and preventive actions.

Security incidents are managed in accordance with applicable legal, regulatory and contractual requirements.

22. Threat Intelligence

Nykaa monitors relevant information regarding emerging and evolving cybersecurity threats to improve its ability to identify, prevent and respond to security risks.

- Understanding emerging threats.
- Supporting risk assessments.
- Strengthening preventive and detective controls.
- Informing security testing.
- Improving incident preparedness and response.
- Supporting security decision-making.

Specific intelligence sources, indicators, detection logic and operational intelligence are maintained internally.

23. Third-Party and Supplier Security

Nykaa recognizes that third-party relationships may introduce information security risks.

- Security due diligence.
- Risk assessment.
- Appropriate contractual requirements.
- Data protection requirements.
- Access controls.
- Security assessments where appropriate.
- Ongoing monitoring based on risk.
- Secure termination of relationships and access.

Third-party security requirements may vary according to the nature and risk of the service provided.

24. Human Resources and Security Awareness

Nykaa promotes security awareness and responsible security practices among personnel.

- Security expectations during onboarding.
- Security awareness and training.
- Confidentiality obligations.
- Appropriate access management.
- Security considerations during role changes and offboarding.

Security awareness activities are designed to help personnel recognize and appropriately respond to common information security risks.

25. Acceptable Use and Responsible Technology Use

Nykaa expects authorized users to use information, systems and technology responsibly and securely.

- Use authorized systems and services.
- Protect company and customer information.
- Protect authentication credentials.
- Avoid unauthorized access or disclosure.
- Follow applicable information handling requirements.
- Exercise caution when using email, internet, collaboration and communication services.
- Report suspected security incidents or suspicious activity.

Unauthorized activities, misuse of information assets and violations of applicable security requirements may be subject to appropriate corrective action.

26. Artificial Intelligence Security

Nykaa recognizes the opportunities and security risks associated with artificial intelligence and emerging technologies.

- Protection of confidential and sensitive information.
- Privacy and data protection.
- Appropriate authorization and access.
- Security risks associated with AI systems.
- Applicable legal and regulatory requirements.
- Responsible and ethical use.
- Appropriate oversight throughout the AI lifecycle.

Specific internal restrictions, approved tools and implementation requirements are maintained separately as internal information.

27. Physical and Environmental Security

Nykaa applies appropriate physical security measures to protect information, facilities, equipment and other assets.

- Controlled physical access.
- Protection of equipment and information.
- Secure handling of physical documents.
- Environmental safeguards.
- Protection against theft, damage and unauthorized access.
- Secure disposal of physical media and information.

Detailed facility security arrangements are not disclosed publicly.

28. Remote and Mobile Working

Where remote or mobile working is permitted, appropriate security measures are applied to protect information and technology resources.

- Protect devices from unauthorized access.
- Use approved access mechanisms.
- Protect confidential information from unauthorized viewing or disclosure.
- Maintain appropriate device security.
- Follow applicable information security requirements when working remotely or using mobile devices.

29. Change and Configuration Management

Changes to relevant technology and information environments are managed in a controlled manner to reduce security and operational risks.

- Appropriate assessment before significant changes.
- Authorization of changes.
- Consideration of security impact.
- Controlled implementation.
- Appropriate testing where required.
- Documentation and traceability.
- Review of significant changes.

Configuration management practices support the secure and consistent operation of relevant technology environments.

30. Information Security in Projects

Information security considerations are incorporated into relevant projects and initiatives.

- Project planning.
- Requirements definition.
- Solution design.
- Technology selection.
- Development and implementation.
- Testing.
- Deployment.
- Operational transition.
- Retirement or decommissioning.

The level of security assessment is determined based on the nature and risk of the project.

31. Compliance and Legal Requirements

Nykaa is committed to complying with applicable information security, privacy, data protection and other relevant legal, regulatory and contractual requirements.

- Periodic evaluation of applicable obligations.
- Incorporation of relevant requirements into security practices.
- Consideration of recognized industry standards and frameworks, including ISO/IEC 27001:2022, where applicable.

32. Security Assurance, Audit and Review

Nykaa periodically evaluates the effectiveness of its information security practices through appropriate assurance activities.

- Internal reviews.
- Security assessments.
- Audits.
- Compliance assessments.
- Risk reviews.
- Control effectiveness evaluations.
- Management oversight.
- Corrective and improvement actions.

The information security framework is reviewed and improved based on changes in the business, technology, threat landscape and applicable requirements.

33. Continuous Improvement

Nykaa is committed to continually improving its information security capabilities.

- Security incidents and lessons learned.
- Risk assessments.
- Audit and assessment findings.
- Changes in technology.
- Emerging threats.
- Regulatory developments.
- Business requirements.
- Industry good practices.

34. Roles and Responsibilities

Information security is a shared responsibility.

- Management — provides appropriate direction, oversight and support for information security.
- Information Security Function — provides security governance, risk management, security guidance, monitoring, assurance and response capabilities as appropriate.
- Business and Technology Functions — implement and maintain appropriate security practices within their respective areas and support management of information security risks.
- Employees and Authorized Users — protect information, follow applicable security requirements and promptly report suspected incidents or concerns.
- Third Parties — meet applicable contractual and security requirements when accessing Nykaa information or systems.

35. Reporting Security Concerns

Employees, customers, partners and other relevant stakeholders should report suspected security incidents, vulnerabilities or information security concerns through the appropriate channels made available by Nykaa.

Reports should contain sufficient information to support appropriate assessment and response while avoiding unnecessary disclosure of sensitive information.

36. Policy Governance

This Public Information Security Policy represents Nykaa's high-level information security commitments.

- Detailed policies, standards and procedures are maintained separately.
- Technical controls and configurations are not disclosed through this public policy.
- Internal risk criteria and security architecture are maintained separately.
- The policy may be reviewed and updated periodically to reflect business requirements, technology, security risks, applicable laws, regulations and recognized good practices.

37. Public Disclosure Statement

This document is intended for public disclosure and provides a high-level overview of Nykaa's information security commitments.

- It does not provide detailed information that could compromise the security of Nykaa's systems, information assets, personnel or operations.
- Nothing in this document should be interpreted as providing access to Nykaa systems or information.
- Nothing in this document should be interpreted as disclosing confidential security arrangements.

38. Reference Frameworks

Nykaa's information security practices take into consideration recognized industry standards, frameworks and applicable legal or regulatory requirements, including:

- ISO/IEC 27001:2022.
- Applicable privacy and data protection requirements.
- Applicable cybersecurity and information technology regulations.
- Relevant contractual and industry requirements.
- Recognized information security good practices.