Information Security Policy

Document Owner: CISO, Information Security
Version 1.2

DOCUMENT DETAILS

Organization Name	One97 Communication Ltd (Paytm)
Document Name & Number	ISMS / POL-20 / Information Security Policy
Document Classification	Internal
Document Author	GRC (InfoSec)
Current Version	1.2

REVISION HISTORY

Sl. No.	Version	Reviewed /Approved By	Approval Date
1	1.0	CISO	July 2023
2	1.0	Board	Aug 2023
3	1.1	CISO	Aug 2024
4	1.2	CISO	Aug 2025

Table of Contents

1. Objective

The objective of this policy is to ensure that management will establish an information security management process to address information security risk requirements. It may include information security objectives, which shall be reviewed and updated on a regular basis, to be made available as documented information for all colleagues within the organization, and communicated in a timely manner, in line with business related security risks, relevant compliance, legal and regulatory requirements.

2. Scope

One97 Communications Limited and its subsidiaries, affiliates and any other investments for the purpose of this policy are collectively referred to as "One97" or "the Company" or "Paytm". One97 is committed to maintain the highest level of professional and ethical standards in the conduct of the business in India and around the world.

This Policy is applicable to One97 including all full-time or part-time employees, interns, trainees, vendors, customers, third parties including contractors, sub-contractors to third parties or anyone who has access to, handles, use or process Paytm's information assets. All business units, processes, information systems, applications, and all forms of information, including digital, printed, and visual data. All users must understand and adopt use of this policy and are responsible for ensuring the safety and security of the Organization's systems and the information that they use or manipulate.

3. Compliance with Code of Conduct

Policy end users remain responsible to ensure the confidentiality, integrity and availability of Paytm's information assets. Any employee to have violated this policy may be subjected to disciplinary action, up to and including termination of employment as per the disciplinary procedures at Paytm as outlined in the Consequence Management policy. Any violation of this policy by the supplier shall be reported to his/ her organization in order to take appropriate action. The supplier organization may be subjected to penalties and/ or Legal Action as per the contractual agreement between both parties. Non-compliance to this policy may lead to civil litigation and/or criminal prosecution under applicable national and federal statutes.

4. Policy Owner/Custodian

This document is owned by the Chief Information Security Officer (CISO) and he is responsible for maintaining versions, ensuring dissemination and issuing clarifications whenever required.

5. Confidentiality

This document is internal and hence would be made available to employees through Paytm's Intranet Portal and other similar channels/websites.

6. Policy Linkage

This document is primarily based on ISO 27001:2022 guidelines and has linkages & references from industry standard security framework and relevant regulatory publications.

7. Policy Statement

The primary goal is to safeguard Paytm's information and systems from damage, destruction, unauthorized disclosure, or modification, whether accidental or intentional, by implementing a risk-based information security framework. Additionally, Paytm's information systems must adhere to relevant laws, regulations, and contractual obligations. Paytm is dedicated to maintaining and continually enhancing its information security measures.

7.1 What is Information?

Information is the result of processing data in a way that adds to the knowledge of the receiver. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation.

7.2 What is Information Asset?

An asset is anything that has value to an organization. Any information, like other important business assets, which has value to business, is Information Asset. Information Systems which help in processing, storing and disseminating information are also Information Assets.

7.3 What is Information Security?

Information Security is protection of Information and Information Assets, from a wide range of threats to ensure business continuity and to minimize business risk thereby enhancing the return on investments. This is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and technology. These controls need to be established, implemented, monitored, reviewed and improved to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

7.4 Principles of Information Security

Information Security Program is based on the following principles:

a. **Confidentiality:** Protection of information by ensuring that information is accessible only to those authorized.
b. **Integrity:** Assuring the accuracy and completeness of information and its associated information processing methods and ensuring controls for preventing unauthorized modification.
c. **Availability:** Ensuring that information and associated assets or systems are available to authorized users when required.

7.5 What is Information Security Risk Management?

An Information Security Risk is the probability that an Information Asset will be subjected to loss, destruction, unauthorized modification and/or disclosure.

Information Security Risk Management pertains to protecting critical information & reducing Information Security Risk for Paytm, including associated corporate assets and services by:

a. Identification of security requirements and associated controls, based on a pre-defined assessment of Information Security Risks.
b. Effective implementation of controls to minimize Information Security breach.
c. Continuous monitoring & review of controls to determine their effectiveness.

7.6 Information Security Objectives

- Protect Information and Systems: Ensure that Paytm's information and systems are safeguarded against damage, destruction, unauthorized access, and changes, whether they occur accidentally or deliberately.
- Compliance: Ensure that Paytm's information systems comply with all applicable laws, regulations, and contractual obligations.
- Continuous Improvement: Maintain and continually improve Paytm's information security practices to adapt to evolving threats and standards.
- Provide training and awareness to all employees and stakeholders.
- Establish measurable ISMS objectives and track performance.

7.7 Cloud Security Principles

- The organization's Information Security Management System (ISMS) and all security controls shall extend to cover the use of cloud services and their associated data.
- Paytm shall operate under a shared responsibility model, clearly defining security responsibilities between the company and its Cloud Service Providers (CSPs).
- Data and information ownership remains with Paytm, regardless of whether it is processed or stored in a cloud environment.

8. Ownership and Management

- To avoid conflict of interest, formulation of policy and implementation / compliance to the policy should remain segregated.
- The Chief Information Security Officer (CISO) is responsible for articulating the IS Policy that Paytm uses to protect the information assets apart from coordinating the security related Issues within the organization as well as relevant external agencies.
- All the employees and external parties as defined in policy are responsible for ensuring the confidentiality, integrity, and availability of Paytm's information assets.
- The information security policy shall be approved by the Board if there are any changes or amendments in the policy.

9. Information Security Governance

- Executive management acknowledges the importance of ensuring information security and is committed to supporting the information security goals and principles.
- Paytm should establish an Information security governance program, based on international standards and globally accepted best practices like ISO 27001.
- CISO is accountable for Paytm's information security governance program and enforcement of this policy.
- The information security team is responsible for monitoring and reviewing Information Systems for compliance with information security policies and producing regular management reports on the status of information security. Team is also responsible for ensuring information security policies are regularly reviewed and updated as necessary to ensure that they remain appropriate in the case of any relevant changes to the law, organizational policies, or contractual changes.
- Paytm shall carry out comprehensive security risk assessment of their people, IT, business process environment, etc., to identify risk exposures with remedial measures and residual risks.
- Reports on risk assessment, security compliance posture, security audit reports and security incidents shall be presented to the management.
- Paytm shall carry out and submit to the management annually, internal and annual external audit reports; annual Vulnerability Assessment / Penetration Test (VAPT) reports.

10. Information Security Requirement

- Paytm should follow a risk-driven methodology to minimize the security risk level for its processes and information assets, including (but not limited to) data, facilities, technology, application systems and people.
- Paytm should develop and follow a detailed set of enforceable policies and procedures commensurate with the criticality and sensitivity of information and processing facilities
- Paytm should apply all reasonable, appropriate, practical, and effective security measures to adequately protect its critical information and information processing facilities.
- Paytm should apply the necessary security controls required to meet its contractual, legislative, regulatory, privacy and ethical responsibilities.
- Paytm management must ensure that information security requirements are assessed and identified during the initiation of every information system or service project.
- Any information system or service hosted or managed by Paytm should follow and comply with Paytm's information security policies and procedures.
- A standard Information Security Confidentiality Clause (including a Non-Disclosure Agreement) and relevant compliance obligations should be included in all agreements, contracts, and purchase orders between Paytm, and any third party being granted access to confidential or sensitive data, information, and system.
- Paytm should ensure that it respects the intellectual property rights of any third party whose products are used for business purposes.
- Paytm should ensure continuity for critical business processes, in case of any disturbance, by implementing proper business continuity & disaster recovery plans and solutions.

- It is the responsibility of all users to report any security related or suspected incidents to the Information Security team. All breaches of information security should be reported to the Information Security team and investigated by the appropriate staff, depending upon the type of breach.
- Any violation, non-adherence to this policy should be considered seriously and should be liable for disciplinary action that may include termination.

11. Continual Improvement of Information Security Governance

- The Information Security Policy should be reviewed and approved by the Board whenever there is a change affecting the policy.
- The Information Security Team should facilitate the overall policy review process.
- Paytm should define and establish responsibility for implementing and maintaining all relevant compliance program across the environment.
- All employees should have an acceptable level of security education and knowledge and be aware of their responsibilities towards information security. Therefore, the Information Security Team should introduce various programs for security awareness. All employees should participate in the security awareness programs during induction and annual basis.
- The Information Security Team must deliver all approved and endorsed policies, standards, and procedures to all employees via its official channel, in addition to other efficient channels.

12. Information Security Management Framework

For ease of reference, this document is organized in accordance with the ISO/IEC 27001:2022 framework. It defines Paytm's overall approach to information security governance, risk management, and compliance.

1. Organizational Controls – Governance, roles, responsibilities, and policies.
2. People Controls – Security training, HR security, and awareness programs.
3. Physical Controls – Facility security, environmental protection, and access management.
4. Technological Controls – Identity management, secure coding, encryption, logging, monitoring, and threat intelligence.

13. Organizational Controls

13.1 Information Security Policy

The Information Security policy provides management direction and support to Information Security. It explains the policies, principles, legislative, regulatory, and contractual compliance requirements for Paytm.

13.2 Organization of Information Security

The Organization of Information Security policy provides a structured framework for managing Information Security at Paytm. Refer (Organization of Information Security Policy) for detailed policy.

14. People Controls

14.1 Human Resource Security

All employees / contractors at all levels shall understand their responsibilities towards Information Security and shall be suitable for the roles for which they are considered. This includes Information Security responsibilities in job definitions, user training and response to Information Security incidents. Paytm ensures that employees, contractors, and third-party resources undergo background verification in compliance with applicable local laws and regulations. The company also enforces confidentiality agreements and implements structured offboarding processes to promptly revoke access upon termination or contract completion.

Refer *(Human Resources Security Policy)* for detailed policy.

15. Physical Controls

15.1 Physical and Environmental Security

Operational facilities that contain proprietary or confidential information and information processing facilities shall be physically protected from unauthorized access, damage and interference. Information assets shall be sited in secure areas, protected by a defined security perimeter, with appropriate entry controls and security mechanisms.

Refer *(Physical and Environmental Security Policy*) for detailed policy.

16. Technological Controls

16.1 Asset Management

Assets associated with information / information systems and information-processing facilities shall be identified and documented to indicate the ownership, importance and shall be classified, used and protected in accordance with their importance to Paytm. Paytm ensures that information is safeguarded across all formats - digital, printed, verbal, and visual - and implements secure disposal practices to prevent unauthorized access or misuse.

Refer *(Asset Management Policy)* for detailed policy.

16.2 Identity & Access Management

Access to information / information systems (operating systems, applications, databases, network equipment and other technologies deployed at Paytm) and information processing facilities shall be controlled to prevent unauthorized access and at the same time ensure that the access is provided to authorize personnel.

Refer *(Identity & Access Management Policy)* for detailed policy.

16.3 Cryptography

Paytm applies industry-standard cryptographic techniques to safeguard the confidentiality, authenticity, and integrity of information by using approved algorithms and key lengths, maintaining robust cryptographic key management processes covering generation, storage, rotation, and destruction, and applying encryption to data at rest, in transit, and in backups.

Refer *(Cryptography Policy)* for detailed policy.

16.4 Operations Security

Secure operational processes for information processing facilities should be established to address the Confidentiality, Integrity and Availability of Information assets by implementing change management to authorize, track, and validate changes, monitoring systems for malware, vulnerabilities, and abnormal activities, ensuring logging, monitoring, and retention of critical events for forensic purposes, and applying secure backup and recovery processes to maintain data availability.

Refer (*Operations Security Policy*) for detailed policy.

16.5 Communications Security

The network infrastructure shall be secured to protect information from unauthorized access and enable effective usage of various networking, communications and computing facilities by securing internal and external networks through firewalls, IDS/IPS, and segmentation, ensuring secure transmission of sensitive information via encryption and VPNs, and implementing email security, DLP controls, and monitoring to prevent potential data leakage.

Refer *(Communications Security Policy)* for detailed policy.

16.6 System Acquisition, Development and Maintenance

Adequate controls shall be deployed in the software development process to address risks in meeting functional and security requirements by integrating security by design into all technology initiatives. Applying secure coding practices aligned with OWASP and industry guidelines, enforcing security testing such as static and dynamic application security testing (SAST/DAST), and ensuring security reviews and approvals for all system enhancements, integrations, and upgrades.

Refer *(System Acquisition, Development & Maintenance Policy)* for detailed policy.

16.7 Supplier Relationships

All the suppliers (outsourcing vendors, agents, third parties and other contract employees) who have access to internal information / information assets to maintain confidentiality and adopt security procedures. Supplier's access to internal information / information assets shall be restricted. Paytm manages third-party risks through robust vendor security governance by assessing suppliers before onboarding using risk-based

security assessments, ensuring the inclusion of information security clauses in supplier contracts, and monitoring supplier compliance through periodic reviews and audits.

Refer *(Supplier Relationship Management Policy)* for detailed policy.

16.8 Information Security Incident Management

Information security incidents and abnormal behaviour associated with information and/or information systems need to be reported and responded appropriately to minimize their damage.Paytm adopts a structured incident detection, reporting, and response framework by requiring immediate reporting of suspected or confirmed security incidents, maintaining an Incident Response Plan (IRP) aligned with CERT-In and regulatory guidelines, and conducting root cause analysis with documented lessons learned to enhance security controls. Refer (*Incident Management Policy*) for detailed policy.

16.9 Information Security aspects of Business Continuity Management

Controls shall be planned and implemented to mitigate the impact of disaster and timely resumption of business activities to minimize information security losses.Paytm ensures resilience and continuity of operations by maintaining a Business Continuity Management System (BCMS) aligned with ISO 22301, identifying critical business processes and defining Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), and testing business continuity and disaster recovery plans at least annually to ensure effectiveness.

Refer (*Business Continuity Management Policy*) for detailed policy.

16.10 Information Security Compliance

Paytm shall comply with relevant laws, regulations, industry standards and contractual agreements which impact its information security activities by ensuring adherence to CERT-In, RBI, PCI DSS, and other regulatory mandates.

Refer (Information Security *Compliance Policy*) for detailed policy.

17. Policy Compliance

17.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

17.2 Deviations and Exceptions

- Compliance to the requirements outlined in this document is mandatory and deviations, if any, shall be treated as exceptions. An Exception Management process shall be defined for handling

short term and long term / recurring deviations to this policy. All exceptions shall be validated by Paytm Information Security Team and shall be approved by Paytm Senior Management.

- All Exceptions shall be granted for a limited period post which the exception requirement shall be reconsidered.
- Any long term / recurring deviations due to technical / operational limitations, shall be communicated to the management team review and tracking. Validated by Paytm Information Security team and shall be approved by Paytm Senior Management; and Shall be reviewed annually.
- Shall be accompanied with a valid business justification and recorded. The record shall capture exception details, business justification, exception validity, supporting documents and associated approvals; and Shall be assessed for associated risks.

17.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment as per HR policies and disciplinary process.
Third parties found in violation would be subject to a fine/termination and/or possible legal action taken.

18. Policy Review

The Information Security Function is responsible for coordinating policy reviews and seeking Board approval if there are any changes. The change log must be kept up-to-date, with immediate updates made whenever modifications occur.