One97 Communications Limited
Information Security Policy
Version 1.3

DOCUMENT INFORMATION

Document Name & Number	ISMS / POL-20 / Information Security Policy
Document Author	GRC (InfoSec)

REVISION HISTORY

Sl. No.	Description	Version	Reviewed By	Approved By	Approval Date
1	Policy prepared	1.0	CISO	Board	15th Aug 2023
2	Annual Review (No changes done)	1.1	CISO	NA	12th Aug 2024
3	Annual Review (No changes done)	1.2	CISO	NA	27th Aug 2025
4	Annual Review (Revised to align with ISO 27001:2022)	1.3	CISO	Board	29th Jan 2026

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.

8. 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.

9. Organizational Controls

9.1 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.

9.2 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.

10. People Controls

10.1 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.

11. Physical Controls

11.1 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.

12. Technological Controls

12.1 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.

12.2 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.

12.3 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.

12.4 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.

12.5 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.

12.6 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.

12.7 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.

12.8 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.

12.9 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.

12.10 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.

13. Policy Compliance

13.1 Compliance Measurement

The information security 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.

13.2 Deviations and Exceptions

- Adherence to the requirements stated in this policy is compulsory. Any deviations will be managed under a formal Exception Management process, designed to address both temporary and recurring/long-term exceptions. Each exception must be reviewed and approved by the by the CISO and Business HOD.
- Exceptions will only be granted for a defined duration, after which the need for continuation must be re-evaluated.
- Every exception request must include a valid business justification and be properly documented. The documentation should include exception details, justification, and duration of validity, supporting evidence, and approvals. All exceptions must undergo risk assessment to identify and evaluate associated risks.

13.3 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.

14. 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.