Acceptable Usage Policy

Document Owner: CISO, Information Security
Version 1.0

DOCUMENT DETAILS

Organization Name	One97 Communication Ltd (Paytm)
Document Name & Number	ISMS / POL-01 / Acceptable Usage Policy
Document Classification	Internal
Document Author	GRC (InfoSec)
Current Version	1.0

REVISION HISTORY

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

TABLE OF CONTENTS

1.Objective

The purpose of this policy is to outline the acceptable use of IT assets and resources including but not limited to laptops, desktops, printers, internet etc. at Paytm. These protocols are in place to protect the employees, customer, corporate data and technology infrastructure at premises and on the cloud. An inappropriate use of any asset in any means exposes Paytm to risks including but not limited to virus attacks, compromise of network systems, services legal and reputational issues.

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 corporate information. 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 27001:2013 guidelines and has linkages & references from industry standard security framework and relevant regulatory publications.

7. Policy

7.1 General Use & Ownership

I. Any proprietary information stored on electronic and computing devices whether owned or leased by Paytm, employees or a third party, remains the sole property of Paytm. It needs to be ensured, through legal or technical controls, that proprietary information is protected.
II. All staff have a responsibility to promptly report any kind of information security incident, loss or unauthorized disclosure of organization's proprietary information to Information.Security@paytm.com.
III. All staff may access, use or share proprietary information only to the extent it is authorized and necessary to fulfil assigned job duties.
IV. All staff are responsible for exercising good judgment regarding the necessity of personal use. Individuals, department heads are responsible for ensuring that the policy is followed. In case of any uncertainty, staff should reach out to the Information Security team.
V. The organization reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

7.2 Security & Proprietary Information

I. All mobile and computing devices that connect to the internal network shall comply with the policy.
II. System level and user level passwords shall comply with the Password Management Standard. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
III. Staff shall use their computing devices for business purpose and personal use judiciously and shall not use the device to perform illegal acts.
IV. Paytm reserves the right to examine any data or software on any company issued devices to ensure compliance and system security.
V. All installed software shall be licensed and inventoried. If employees require any software for business purposes, they should reach out to the IT department to obtain licensed software.
VI. All computing devices shall be secured with the automatic activation feature set to 15 minutes or less. All employees shall lock the screen or log off when the device is unattended.

8. Due Care and Due Diligence

I. Under no circumstances, staff is authorized to engage in any activity that is illegal under local, state, or international law while utilizing company owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.
    a) Corporate emails should be preferably used for business communication
    b) The endpoints (Laptops, Desktops, mobile devices etc.) provided / issued to employees and the data stored on it is the property (Asset) of the company.
    c) These endpoints are loaded with protection software and tools which may be used to safeguard assets and data from malwares, unauthorized access, manage assets and update operating systems.
    d) Users are not allowed to uninstall any mandatory tools or applications which

protects the IT systems from malwares, virus and other business impacting intrusions. Users will be accountable for breach arising out of any violation.

e) Usage of unauthorized software which covers but not limited to pirated/cracked software, freeware, shareware, torrent, firewall bypassing tools & proxies, etc. is strictly prohibited.

II. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the company or the end user does not have an active license is strictly prohibited.

III. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

IV. Making fraudulent offers of products, items, or services originating from any company account. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

V. Circumventing user authentication or security of any host, network or account is illegal. Introducing honeypots, honey nets, or similar technology on the company network. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

VI. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet is forbidden.

VII. Disclosure of corporate classified information to parties outside Paytm.

9. Email and Communication Activities

The Company’s email system, network, and Internet/Intranet access are intended for business use only.

All information created, sent, or received via the Company's email system, network, Internet, or Intranet, including all email messages and electronic files, is the property of the Company. Use of the internet, email for personal use is allowed, however, the information security department has the right to monitor, analyse logs etc. for any security breach/vulnerability in any form, and all emails including personal emails are subject to acceptable use guidelines covered below.

I. Employees should review with managers/department heads before sending any confidential/restricted information through e-mail to intended recipients or outside the organization. Wherever feasible, employees shall mark a copy to their supervisors while mailing confidential information and the same should be restricted to “Do Not Forward” mail.

II. Use extreme caution to ensure that the correct email address is used for the intended recipient(s). Unauthorized use, or forging, of email header information is strictly prohibited.

III. Use of the company’s email system to solicit for any purpose, personal or otherwise, without the consent of the Company is strictly prohibited.

IV. Employees shall not access any mail from unknown sources, download or open suspicious

attachments or links. Employees or third party contractors are not permitted to “blanket forward” (the automatic forwarding of every email received) their corporate e-mail messages, or forward confidential messages to a personal account obtained through a third-party internet service provider for access when at home or travelling. Employees shall not misuse the e-mail access to create, send, receive or store any message which may be constructed as offensive, disruptive, or a threat to the business.

V. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

VI. Email messages shall contain professional and appropriate language always. Employees are prohibited from sending abusive, harassing, intimidating, threatening, and discriminatory or otherwise offensive messages via email. Sending abusive, harassing, intimidating, threatening, discriminatory, sexual, or otherwise offensive messages via email will result in disciplinary action up to and including termination.

VII. Email usage shall conform to the Company’s harassment and discrimination policies. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

VIII. Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam) is considered to be illicit.

IX. Employees should exercise sound judgment when distributing messages or posting content on third party sites like LinkedIn, Twitter, Facebook, Myspace, Flickr etc. Client-related messages should be carefully guarded and protected.

X. Employees are strictly prohibited from posting any business-related matters on public forums, responding to media queries, or engaging in informal conversations about business or strategy. Only authorized teams or individuals are permitted to share information about the Company on social media.

XI. Personal content that is not appropriate for colleagues, employers, customers or partners to view should not be made public to them.

XII. Misuse and/or abuse of electronic access, including but not limited to, personal use during working hours, copying or downloading copyrighted or confidential materials, visiting pornographic sites or sending abusive email messages will result in disciplinary action, up to and including termination.

10. Password Security

Employees are not permitted to authorize others to login using their account and shall not attempt to determine another user’s password. Employees shall keep their passwords secure and shall not share it with anyone.

Employees are responsible for the selection of passwords that are compliant with security baselines:

I. Configure multi factor authentication on all possible authentication wherever technically and operationally feasible.

II. Employees shall not enable auto log-on options on their systems by saving their passwords locally on their workstations

III. If the security of a password is compromised, it must be changed immediately

IV. Passwords must be unique from all other previous passwords.

11. Anti-Malware & DLP

Any file attached to an email from an unknown, suspicious or untrustworthy source shall not be opened and caution shall be exercised while downloading files from the internet. The source shall be ensured to be legitimate and reputable.

Overriding anti-malware and DLP related controls such as changing the configuration settings of the anti-virus client or interrupting anti-virus scan or disabling DLP agent shall not be done. Any virus incident should be intimated to the IT Service Desk or Information Security team at the earliest.

IT departments manage assets, critical patches, upgrades of OS, applications through remote management tools, these are mandatory for ensuring company assets are protected and maintained up to date on vulnerability, license and asset management process.

12. Unattended Equipment

Employees shall be responsible for the equipment assigned to them. The employees shall be made aware of the measures to be taken to protect the information assets of the organization.

These measures shall include:

I. Employees shall log off from applications, telecommunication and computing devices after the session is completed.
II. Employees should not leave the laptop/computers unattended, any such unattended laptops will be recovered by security and will be issued back upon approval of the employee's manager.

13. Blogging/ Social Media

This policy identifies standards regarding activities associated with internet use, including, but not limited to, blogging, posting information, pictures, or other material on Weblogs or the Internet, and creating or maintaining blogs, message boards, or profile pages on social or business networking sites as defined below. Even though the Internet is frequently used to express personal views, employees are not allowed to discuss anything related to business or proprietary information in public forms. It can directly or indirectly interfere with employees in the workplace, or harm the goodwill and reputation of Paytm among its customers or the community at large. Therefore, employees are reminded that being compliant with all company policies is required.

Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material that is confidential to the company while engaged in Blogging/Social Networking and may not also not attribute personal statements, opinions or beliefs when engaged in Blogging/Social Networking. Communications that are associated with or linked to the company, even directly that may exhibit disrespect for other individuals are not permitted.

Blogs often express the personal view of the individuals who post or communicate them and not the ideas, views, or opinions of the company. Employees should understand that individuals who view blogs may not recognize this fact. Accordingly, employees who mention the company or their employment with the company in any social media should include a prominent disclaimer that clearly and conspicuously states the following: “The views expressed here reflect only my personal views and are not the views of my employer”.

For more details, please go through the Social Media Policy

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.

15.Deviations and Exceptions

There shall be a business case presented to the responsible team (Information Security) for a formal approval on the deviations of policies and describing challenges. All exceptions shall undergo a formal risk assessment and wherever applicable there shall be a compensating and monitoring control exercised.