Wipro’s

Acceptable Usage Policy

**Document Control**

|  |  |
| --- | --- |
| Function | Group Chief Information Security Office (GCISO) |
| Sub-function | - |
| Policy Owner | Lakshminarayanan RS, Group Head - Information Security Policy & Framework |
| Policy Effective Date | July 27, 2023 |

**Purpose**

This policy governs the Acceptable Usage of information systems by user(s) of these systems.

**Audience**

Organization’s employees, including retainers, contractors, and service providers.

**Scope**

This policy is applicable to the information systems owned or managed by the Organization.

**Policy Details**

**AU.1 INFORMATION SYSTEM USAGE REQUIREMENTS:**

**AU.1.1** Information systems provided by the Organization are secured and used for business purposes only.

**AU.1.2** Clear desk and clear screen practices shall be followed as defined in the Clear Desk and Clear Screen Standard.

**AU.1.3** Information systems shall not be accessed by unauthorized personnel, including family members, friends, and visitors.

**AU.2 PASSWORD USAGE REQUIREMENTS:**

**AU.2.1** Default login passwords shall be changed after the first login.

**AU.2.2** Strong passwords shall be used and changed periodically as per the Password Management Standard.

**AU.2.3** Passwords shall be changed immediately upon suspected compromise or disclosure.

**AU.2.4** Passwords shall not be written and shared with others by any medium.

**AU.2.5** Accidental or intentional password breaches shall be reported immediately as defined in the Security Incident Management Policy.

**AU.3 INTERNET USAGE REQUIREMENTS:**

**AU.3.1** Users shall use the Organization’s internet for business purposes only.

**AU.3.2** Inappropriate or potentially malicious content shall not be accessed or downloaded.

**AU.3.3** The Organization's confidential information shall not be disclosed on the Internet.

**AU.3.4** Customer deliverables shall be classified and securely transmitted.

**AU.3.5** The Internet shall not be used to access, publish, distribute, or disseminate any inappropriate, profane, defamatory, infringing, obscene, indecent, or unlawful information.

**AU.3.6** Information posted on social media shall comply with the Code of Business Conduct (COBC).

**AU.4 EMAIL AND INSTANT MESSAGING (IM) USAGE REQUIREMENTS:**

**AU.4.1** The Organization’s email shall be used for business communications.

**AU.4.2** The Organization or its customer’s emails shall not be forwarded to personal email accounts.

**AU.4.3** Anonymous web links and attachments originating from unknown sources shall not be accessed or downloaded.

**AU.4.4** Emails shall be considered valid documentary evidence for electronic approvals.

**AU.4.5** The Organization emails shall be classified and labelled as per the Information Classification, Labelling, and Handling Standard.

**AU.4.6** Personally Identifiable Information (PII) shall not be transmitted without approval from designated personnel.

**AU.4.7** Emails that constitute offensive language, religious propaganda, vulgarities, obscenities, sexually explicit language or content, derogatory and defamatory remarks, discriminatory statements or contribute to a hostile work environment shall not be forwarded.

**AU.4.8** Group emails, announcements, and broadcast emails shall not contain photographs of employees, retainers, or contractors without the consent of the respective individuals.

**AU.4.9** The Organization emails shall not be used for external surveys, contests, spamming, or unsolicited messages.

**AU.4.10** Email and IM services shall not be used to defame, abuse, harass, stalk, or threaten colleagues.

**AU.4.11** Email and IM services shall not be used to publish, distribute, or disseminate any inappropriate, profane, defamatory, infringing, obscene, indecent, or unlawful material.

**AU.5 SOFTWARE USAGE REQUIREMENTS:**

**AU.5.1** Authorized software with appropriate licenses and permissions shall be used. Use of unauthorized software shall be prohibited.

**AU.5.2** Freeware or shareware software shall not be distributed, installed, or used without approval from the business or function head.

**AU.5.3** The customer-provided software shall be used as per the terms and conditions, and license agreements.

**AU.6 REMOVABLE STORAGE MEDIA REQUIREMENTS:**

**AU.6.1** Personal or unauthorized removable storage media shall not be used for business purposes.

**AU.6.2** Authorized removable storage media shall be scanned for malicious code before usage.

**AU.6.3** The Organization information shall not be transferred to removable storage media without business or function head’s approval.

**AU.6.4** Customer’s approval shall be obtained for the usage of removable storage media and organization provided collaborative tools including Teams, OneDrive, SharePoint within Offshore Development Centres (ODC).

**AU.6.5** Confidential information in removable storage media shall be encrypted.

**AU.7 GENERATIVE AI USAGE REQUIREMENTS**

**AU.7.1** Define responsible usage, deployment, and development of Generative AI across the Organization.

**AU.7.2** Govern the risk of usage of Generative AI tools for internal use and client engagement.

**AU.8** Unusual or anomalous behavior related to information systems, email, internet, instant messaging, removable storage media, and passwords shall be reported as per the ‘Security Incident Management Procedure’.

**AU.9** The Organization’s information systems shall be classified and handled as defined in the ‘Information Classification, Labelling and Handling Procedure’.

**AU.10** Confidential information shall be disclosed on a ‘need-to-know’ basis.

**AU.11** Information shall be protected against shoulder surfing.

**AU.12** Information and storage media shall be disposed securely as defined in the Asset Management Procedure.

**Definitions**

|  |  |
| --- | --- |
| **Definition** | **Description** |
| Encryption | The process of changing plain text into cipher text using a cryptographic algorithm and key. |
| Information Systems | Set of applications, services, information technology assets, or other information-handling components. |
| Instant Messaging | A facility for exchanging messages in real-time with people over the Internet and tracking the progress of a given conversation. |
| Malicious Code | A code designed to cause damage, security breaches, or other threats to the information systems security. |
| Organization | Wipro Limited, including subsidiaries, affiliates, and acquired entities, but excluding acquired entities governed by an independent set of security policies. |
| PII | Information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual. |
| Removable Storage Media | A system component that can communicate with and be added to or removed from a system or network and that is limited to data storage. |
| Social Media | Forms of electronic communications, including websites and applications, which enable users to create and share content or participate in social networking. |
| Spamming | The practice of sending unwanted email messages, frequently with commercial content in large quantities. |
| Shoulder Surfing | A type of social engineering technique used to obtain information such as personal identification numbers (PINs), passwords, or confidential information, by looking over the victim's shoulder. |
| Users | The term “User” includes employee of the Organization, retainers, contractors, trainees or interns, customers, partners, suppliers, and vendors. |

**Acronyms**

|  |  |
| --- | --- |
| **Acronym** | **Description** |
| COBC | Code of Business Conduct |
| GCISO | Group Chief Information Security Office |
| IT | Information Technology |
| ODC | Offshore Development Center |
| PII | Personally Identifiable Information |

**References**

* Data Protection and Privacy Policy (Personally Identifiable Information)
* Security Incident Management Policy
* Acceptable Usage Standard
* Clear Desk and Clear Screen Standard
* Password Management Standard
* Asset Management Procedure
* Information Classification, Labelling and Handling Procedure
* Security Incident Management Procedure
* [Responsible Use and Development of Generative AI](https://thedot.wipro.com/sites/legal-compliance-data-privacy/document/374528/Responsible-Use-and-Development-of-Generative-AI)

## Revision History

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Revision Date** | **Reason for Change** | **Drafted/ Reviewed By** | **Approved By** | **Date Approved** |
| 1.0 | 25th July 2023 | Merged “Acceptable Removable Media Usage Policy”, “Acceptable Software Usage Policy” & “Acceptable E-mail and Internet​​ Usage Policy” to form “Acceptable Usage Policy” as per the ISO 27001:2022 and best practices of NIST 800-53 Rev5. | Nagarajendra Neel Kuruvemula | Lakshminarayanan RS | 17th Jan 2024 |
| 1.1 | 27th June 2024 | Added section AU.7 for Generative AI Usage Requirements. | Thirunavukkarasu A M | Lakshminarayanan RS | 28th June 2024 |