Wipro’s

Bring Your Own Device (BYOD) 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 | December 7, 2015 |

**Purpose**

This policy governs the use of personal devices that employees utilize for business purposes, termed as Bring Your Own Device (BYOD) in this policy. This policy establishes the security requirements to protect the information systems from the risks arising through BYOD usage.

## Audience

Organization’s employees, retainers, contractors, and service providers who use BYOD.

**Scope**

This policy is applicable to devices owned by the users, including but not limited to, computers, laptops and mobile devices used for business purposes.

**Policy Details**

**BYOD.1 COMMON FOR MOBILE DEVICES, LAPTOPS, AND COMPUTERS**

**BYOD.1.1** **Acceptable BYOD Usage**

1.1.1 BYOD shall be used for business purposes only in compliance with Organization’s Information Security Management System (ISMS) policies and Code of Business Conduct (COBC).

1.1.2 Information on personal devices shall be accessed by authorized users.

1.1.3 User(s) shall be responsible and accountable for all the activities performed on their personal devices.

1.1.4 The applications and plugins installed on personal devices shall be from trusted and authorized sources.

1.1.5 Any shared, loaned, or rented devices shall not be used to enroll with Organization’s BYOD Solution.

1.1.6 User(s) shall access the Organization’s applications or information only through trusted networks.

1.1.7 Necessary precautions shall be taken while using devices in public and open office places.

1.1.8 Devices shall not be left unattended and shall be protected from loss or theft.

1.1.9 Lost or stolen devices shall be reported to the service desk.

1.1.10 Active Directory (AD) password shall be changed immediately upon loss or theft of a device.

1.1.11 Devices shall not be used to perform administrative activities on the Organization’s information systems.

1.1.12 This policy shall be subject to applicable laws and regulations.

1.1.13 The Organization reserves the right to de-register any inactive or rogue devices from time to time as defined in Bring Your Own Device (BYOD) Standard.

**BYOD.1.2 Organization’s Right to Monitor and Protect**

1.2.1 The Organization reserves the right to monitor it’s applications or information contained in BYOD as per applicable laws, regulations, and business requirements.

1.2.2 The Organization shall not monitor the user’s personal information in devices enrolled in BYOD.

1.2.3 The Organization reserves the right to impose a ‘legal hold’ on information contained in devices enrolled in BYOD to preserve and access information during various circumstances, including but not limited to security incident investigations, customer disputes, lawsuits, and corporate and legal investigations.

1.2.4 The Organization reserves the right to inspect devices enrolled in BYOD in line with country-specific laws. The user(s) shall be notified before such actions are initiated.

1.2.5 User(s) shall not intentionally prevent remote access required to support the e-discovery of the Organization’s information contained in the device.

**BYOD.1.3 Device Backup and Data Synchronization**

1.3.1 User(s) shall use approved applications or storage for backup of the Organization’s information.

1.3.2 User(s) shall not synchronize Organization’s information from devices enrolled in BYOD to any third-party device or storage.

1.3.3 Unauthorized devices (personal hard drive, memory sticks, or cards), personal internet cloud services, Instant Messaging (IM) services, and personal mail accounts shall not be used for synchronization, transmission, or backup.

1.3.4 The Organization shall not control, access, backup, or delete user’s personal data in devices enrolled in BYOD without prior consent of the user(s).

**BYOD.2 POLICY FOR MOBILE DEVICES**

**BYOD.2.1 Device Enrolment**

2.1.1 User(s) shall enroll mobile device to the Organization’s BYOD Solution. All required software shall be installed and configured to protect the Organization’s information stored on mobile devices.

2.1.2 Jail-broken and rooted devices shall not be used to enroll with the Organization BYOD Solution.

2.1.3 The Organization’s IT resources shall be accessed only after complying with BYOD pre-requisites and Bring Your Own Device (BYOD) Standard.

**BYOD.2.2 Organization’s Right to Wipe or Erase Information**

2.2.1 The Organization shall reserve the right to initiate the remote wiping of its data from devices enrolled under its BYOD Solution, excluding personal data. The Organization shall also stop the synchronization services during user separation, user’s unauthorized absence from work, device loss or theft, change or disposal of the device, and malware attacks. This shall be done after notifying the user(s).

**BYOD.2.3 Organization’s Right to Monitor and Protect**

2.3.1 The Organization reserves the right to deploy technical controls on devices enrolled in its BYOD Solution to protect its information.

**BYOD.3 POLICY FOR COMPUTERS**

**BYOD.3.1 Virtual Desktop Infrastructure (VDI) Based Access**

3.1.1 VDI solution shall be implemented on user-owned laptops and desktops to protect the Organization’s information.

3.1.2 VDI instances shall be restricted from performing system administrative activities.

3.1.3 “Anti-keylogging” and “Anti-screen-capturing” shall be enabled in BYOD VDI instances.

**BYOD.3.2 Personal Computer (Non-VDI) Based Access**

3.2.1 Enrolment of personal computers with Organization’s Device Management Solution shall be restricted.

3.2.2 User(s) shall be allowed to access internet applications via web browser from personal computers.

3.2.3 User(s) shall refrain from transferring the Organization’s information outside the Organization or to personal computers.

**BYOD.3.3 BYOD Users Working from Office**

3.3.1 User(s) connecting devices to Organization’s Wi-Fi or LAN network shall be redirected to an isolated network with restricted access. The isolated network shall be restricted, with access to only limited URL’s, Organization’s VDI, customer’s VPN, and customer’s VDI.

3.3.2 A separate Wi-Fi or LAN network shall be enabled with Multi-Factor-Authentication to connect devices enrolled under the BYOD Solution.

**BYOD.4** Security incidents related to BYOD devices shall be reported as defined in the Security Incident Management Procedure.

**BYOD.5** Logging and monitoring of devices enrolled under the BYOD Solution shall be enabled as per the Logging and Monitoring Standard.

**Definitions**

|  |  |
| --- | --- |
| **Definition** | **Description** |
| BYOD Solution | A software that allows IT administrators to automate, control, and secure administrative policies on laptops, desktops, smartphones, and tablets. |
| BYOD | Refers to the usage of personal devices for business purposes including laptops, desktops, mobile devices, and VDI platforms used by personal devices. |
| Computers | Laptops, desktops, and VDI platforms used as BYOD. |
| Jail Broken or Rooted Device | A device that has been modified to gain unrestricted access to the root of the operating system and applications. |
| Legal Hold | To prevent destruction of official information and preserve official records under circumstances such as security incident investigations, customer dispute, lawsuit, corporate and legal investigation. |
| Mobile Device | Portable computing devices such as smartphones, tablets, and e-readers. |
| Organization | Wipro Limited, including subsidiaries, affiliates, and acquired entities, but excluding acquired entities governed by an independent set of security policies. |
| Security Baseline Requirements | A recognized, standardized, and established benchmark that stipulates specific secure configuration settings for a given information technology platform. |
| User | The term “User” includes employee of the Organization, retainers, contractors, trainees or interns, customers, partners, suppliers, and vendors. |
| VDI | A technology that utilizes virtual machines to manage and provide virtual desktops. |

**Acronyms**

| **Acronym** | **Description** |
| --- | --- |
| AD | Active Directory |
| BYOD | Bring Your Own Device |
| COBC | Code of Business Conduct |
| GCISO | Group Chief Information Security Office |
| IM | Instant Messaging |
| IT | Information Technology |
| ISMS | Information Security Management System |
| VDI | Virtual Desktop Infrastructure |

**References**

* Bring Your Own Device (BYOD) Standard
* Logging and Monitoring Standard
* Security Incident Management Procedure

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Revision Date** | **Reason for Change** | **Drafted/ Reviewed By** | **Approved By** | **Date Approved** |
| 1.0 | 11th August 2023 | Reviewed and updated the policy as per the ISO 27001:2022 and best practices of NIST 800-53 Rev5.  Merged Acceptable Smart Phone Usage Policy as part this policy. | Prem Anand Rajan, Joji M and Sivakumar Veerabadran | Lakshminarayanan RS | 15th January 2024 |
| 1.1 | 27th May 2024 | Renamed BYOD.3.2 section.  Added 3.2.1 point.  Updated 3.2.2 and 3.2.3 points. | Prem Anand Rajan, Joji M and Sivakumar Veerabadran | Lakshminarayanan RS | 29th May 2024 |