Information Security Management System
Bring Your Own Device Policy

Document no. JMBGRP/ISMS/Pol-BY

Version no. v1.2

Document details

Classification	Internal	
Released date	28.08.2018	
Description	The policy document defines controls to protect organization's information while accessed and processed through personal devices.	
Custodian	Corporate IT dept.	
Approved by	Manish Jaiswal (Group CTO)	
Owner	Corporate IT dept.	

Distribution list

Name
To all locations of JMB group.

Version History

Version no.	**Version date**	**Approved by**	**Comments**	**Signature**
v1.0	28.08.2018	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	10.01.2019	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	08.02.2020	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	11.02.2021	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.1	25.03.2022	Manish Jaiswal (Group CTO)	Logo changes done in this policy	
v1.2	18.08.2023	Manish Jaiswal (Group CTO)	Document reviewed. Modification done to "Reference to ISO 27001:2022"	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Modifications done in Section: "Policy Statement, Procedure, Responsibilities"	

Contents

Purpose

JMBGRP understands that computing is increasingly getting heterogeneous with users making use of smart phones / tablet and tablets with phone capability excluding laptops. These would be personal devices or as provided by the company based upon eligibility as per designation and business need. The rationale is to provide speed of communication and facile access to facilitate agile decision making, provide visibility to data, statistics, and reports; while on the move through the personal devices or company provided devices. However, information security essentials need to be integrated with letter and spirit pertinent to users' BYOD (Bring your own device). This policy seeks to achieve the said purpose of Data Governance.

Scope

This policy applies to the following:

- All Locations of J.M Baxi Group
- All Employees of J.M Baxi Group

Policy Statement

- The provisioning of mobile computing devices such as smartphones , tablets with phone capability, tablets without phone capability but with Wi-Fi and data access capabilities shall be done based on demonstrated business need by an Employee and or HOD as the case may be. Currently the BYOD (Bring Your Own Device) policy has not been extended too personal laptops.
- There will be a formal process for provisioning and de- provisioning of mobile devices for use in the corporate environment.
- Adequate and sufficient levels of physical and logical security controls shall be deployed on these mobile devices.
- Appropriate technology platforms shall be promulgated to ensure management of mobile devices with diverse operating systems in a seamless manner with required security controls.
- Availability of JMBGRP Network delivered services are of critical importance to the users who use such computing devices, and the technical support shall be commensurate with the criticality.
- Acceptable usage norms shall be articulated to the user.
- JMBGRP shall prescribe permissible applications and services that can be mounted on such devices to access corporate data.

Procedure

1.1 This procedure shall address the deployment of the devices across, iOS, Windows and Android Devices.

1.2 This procedure shall address two categories of devices. The first categories of devices are those which have been provided by the company to the employee. The second category consists of individual employees who have procured mobile devices on their own and wish to connect to JMBGRP's network post clearance of the eligibility criteria as set forth by JMBGRP.

1.3 **Eligibility:**

1.3.1 The eligibility conditions to avail BYOD service by employees will be defined by L1 level officials in conjunction with the HOD and IT shall facilitate in the provisioning.

1.3.2 For any exceptions the concerned HOD shall raise request on Ticketing Tool.

1.3.3 IT shall ensure that only permitted devices are used by the employees.

1.4 Android and iOS devices are currently being used in JMBGRP.

1.5 The challenge today is to manage non-Black Berry devices which use iOS, Windows and Android Platforms. All these platforms do not have a management server and hence extreme care shall be taken while provisioning these devices.

1.6 It is hereby recommended that an appropriate Mobile Device Management Platform shall be deployed at JMBGRP which shall facilitate the deployment and use of mobile devices in a secure manner. The Mobile Device Management Platform shall integrate existing mobile devices into a common framework and shall enable application of policy settings in a methodical manner. The parameters which shall be addressed by the Mobile Device Management Platform shall comprise of as under:

1.6.1 Compliance to Law and Regulations

1.6.2 Support of Devices and Operating Systems

1.6.3 Compartmentalization of the device with the features as listed below:

1.6.3.1 Enforcement of Encryption (on basis of Business Requirement)

1.6.3.2 Distribute Settings Over the Air (OTA)

1.6.3.3 Requirement Passcodes

1.6.3.4 Restrict Device Features as Necessary

1.6.3.5 Application Use and Management

1.6.3.6 Device Tracking and Locking

1.6.3.7 Remote Data Wipe

1.6.3.8 Incident Management

1.6.3.9 Monitoring of the devices

1.7 **Meeting the Regulatory Requirements**

1.7.1 JMBGRP shall ensure that deployment of any MDM solution shall be in keeping with the TRAI (Telephone Regulatory Authority of India) Regulations and other allied agencies of Government of India to take cognizance of the legal ramifications on account of usage of mobile devices to discharge organizational duties. Employees shall be educated in the safe and correct usage of their mobile devices. JMBGRP shall not deploy the MDM platform on jail broken and rooted devices as this is a legal violation.

1.8 **Support of Devices and Operating Systems**

1.8.1 The deployed platform shall enable integration of Windows, Android and iOS devices.

1.9 **Compartmentalization**

1.9.1 The deployed platform shall enable compartmentalization of the mobile device. This shall separate the device into 2 containers. One container section shall be for Corporate Use and the second part of the container shall be for personal use. This way JMBGRP shall bifurcate personal and private zones. The following security measures shall be adopted on the corporate container.

1.9.1.1 The Corporate Container shall be encrypted. The encryption shall be either file level or block level. Devices which don't support encryption shall not be deployed with the MDM solution and allowed to connect to the corporate network.

1.9.1.2 **OTA (Over The Air)** policy and configuration allows enforcement of policy updates, passcode configuration settings, encryption controls, and application management

1.9.1.3 **Setting up of the Passwords** – These must be atleast 8 characters either numeric or shall contain alphanumeric and special characters. Password Complexity and History shall be enforced as per JMBGRPs' Logical Access Policy. The password shall be renewed after every 60 days.

1.9.1.4 Device shall be locked post limited login attempt.

1.9.1.5 If the device is idle then the device shall be locked after 5 minutes of idle time.

1.9.1.6 **Application Management:** The list of applications which can be installed shall be made available through the MDM Platform only. User shall be

allowed to download and install applications inside the corporate container as per permissions provided.

1.9.1.7 Employees are automatically prevented from downloading, installing and using any application that does not appear on the JMBGRP's list of approved apps from the company catalogue on the platform.

1.9.1.8 Access to applications shall be through a suitable virtual interface or through a secure browsing environment; with an authentication mechanism involving either physical or an OTP along with the application password.

1.9.1.9 Usage of NFC (Near Field Communication), Bluetooth and USB shall be disabled. The Wi-Fi shall be configured to connect only to the JMBGRP network and not to any other Wi-Fi hotspot.

1.9.1.10 While accessing mails – user activity shall be monitored. It is recommended that users shall not download the mails onto the mobile device, but do so when back to the desktop/laptop.

1.9.1.11 **Remote Wipe:** JMBGRP reserves right to remotely wiped if employees' 1) the device is lost, 2) the employee terminates his or her employment, and 3) IT detects a data or policy breach, a malware or similar threat to the security of the company's data and technology.

1.9.1.12 **Monitoring:** User activity shall be logged when using the MDM platform, for any inappropriate use, the platform shall display a warning message. The user activity monitoring shall comprise of :

1.9.1.12.1 Mobile Device Hardware Type, Battery Condition and Storage Space

1.9.1.12.2 To ensure that all devices have current updated and patched versions of the OS and there is security compliance with the set policies.

1.9.1.12.3 Network Information comprising Carrier, country, Wi-Fi access and last connection date.

1.9.1.12.4 Location Information consisting of where the device last connected along with complete historical record of where the device accessed the network.

1.9.1.12.5 Security & Compliance: View applied policies, compliance history, passcode settings, application settings and device features.

1.9.1.12.6 Installed Software: Permit view of all installed software and apps meet corporate mobile standards.

1.9.1.12.7 Provide a view into the type of documents accessed, videos viewed on the mobile device along with their listing. If the user. Content Management shall be deployed to prevent un-acceptable use of the Internet.

1.9.1.12.8 Mobile Data Usage: Get real-time stats on mobile device data usage.

1.9.1.13 Users shall not be allowed to synchronize data with their office laptops or desktops.

1.10 **Devices and Support:**

1.10.1 Devices must be presented to IT for job provisioning and configuration of standard apps, such as browsers SAP and security tools, before they can access the network in a secure manner.

1.10.2 For any technical support, call shall be logged with the IT Helpdesk.

1.10.3 Employee shall not undertake to resolve technical issues related to the hardware / operating system through an external vendor or the service provider.

1.10.4 IT shall issue a ticket for incidents reported by the user and these shall be resolved and message shall be sent to the employee upon closure of the reported incident

1.10.5 For a company provided mobile device, which has to undergo a refresh / upgrade process. IT Helpdesk shall do the necessary activities to ensure that no company data is present on the mobile device. Disposal shall happen through a documented process as framed by IT.

1.10.6 The servicing activity shall be done by the IT Person in the presence of the user. By deputing any other person, the user is knowingly permitting privacy violation and shall take complete responsibility for any data theft/leakage/loss and JMBGRP shall not be responsible for loss of any personal data.

1.11 **Access to Private Data:**

1.11.1 For a device procured by the employee which is to be connected to the JMBGRP Network and Information Systems, then automatically JMBGRP security policies shall be applicable on that device.

1.11.2 For any inappropriate use of the device which shall tarnish JMBGRP's image and or reputation, impact business, the user shall be held responsible and appropriate disciplinary action shall be initiated.

1.11.3 Even any use on the personal container of the device any inappropriate use leading to the compromise of the device which will hamper productivity and communication shall be considered as a breach and appropriate disciplinary action shall be taken against the employee.

1.11.4 By employees accepting the MDM Policies, they agree to give up their personal privacy in exchange for the convenience of choosing their own phone and conducting activities on a single device.

1.12 **Reimbursement :**

1.12.1 JMBGRP will reimburse the employee a percentage of the cost of the device in accordance with the existing policy.

1.12.2 JMBGRP will reimburse the other incidental expenses on performance of job function through the device like internet connectivity, subscription plan etc.

1.12.3 JMBGRP will not reimburse the following charges: roaming, plan overages.

1.13 **Liabilities :**

1.13.1 IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.

1.13.2 JMBGRP reserves the right to disconnect devices or disable services without notification.

1.13.3 Lost or stolen devices must be reported to the company within 24 hours after which the deactivation of services would be initiated from Mobile Devices.

1.13.4 The employee is expected to use his or her devices in an ethical manner at all times and adhere to the JMBGRP's acceptable use policy as outlined above.

1.13.5 Employees are personally liable for all costs associated with the self- owned device.

1.13.6 Employees assume full liability for risks including, but not limited to, the partial or complete loss of JMBGRP's and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

1.13.7 JMBGRP reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

1.13.8 JMBGRP reserves the right to audit the device, conduct forensic examination of the mobile device should circumstances warrant such an action.

1.13.9 JMBGRP reserves the right to submit the mobile device as evidence in the court of law, should circumstances warrant such an action.

Responsibilities

The responsibility for the planned initiative in this document lies with the following personnel:

- IT:
  - Configuration of devices according to requirement
  - Provisioning applications services and SAP access as the case may be.
  - Maintaining applications, SAP and services with updates and patches.
  - Managing security requirements stipulated by the Information Security Team.
  - Conduct IT audit on employee's devices.
  - Maintain the records of Audit and findings.
  - Monitor employee's devices and report incidents.
  - Remotely wipe off data of stolen devices or employees who have left the organization/ been transferred. This shall be done upon instruction from HOD>>>HR>>>IT.
- HOD:
  - To approve the employees' requirement and forwarding to IT for service enabling/provisioning.

Enforcement

- This policy and procedure is applicable for all the employees and contractors of the company who have access to and use the information assets and IT assets as listed in the Information Asset Classification sheet which have been created for all the departments. Any violation shall be dealt with in accordance with the disciplinary action process as laid down in the Code of Conduct.
- Violations by the vendors shall also come under the purview of the Information Security Framework and action shall be taken accordingly.
- Management's interpretation of the clauses in this procedure shall be final and binding. Management reserves the rights to alter or amend any clause in this document at any time as per its discretion.

Metrics

- Metrics shall be prepared by IT and reported to Head GIS and also to Security In-charge.
- The metrics shall be measured on a quarterly basis and reported. The points include as given below, but not restricted to.
  - Number of attempts to download non permissible applications.
  - Number of incidents of unacceptable usage of devices.
  - Number of failed attempts to log into provisioned services.
  - Consumption of bandwidth for official and personal use.
  - Audit trails of users to evaluate the reported incidents by IT.

Exceptions

- Exceptions shall not be universal but shall be agreed on a case-by-case basis, upon official request made by the information owner. These may arise, for example, because of local circumstances, conditions or legal reasons existing at any point of time.

- Exceptions to this Policy and Procedures shall have to be allowed at the time of implementation of this policy and procedures or at the time of making any updation to this document or after implementation on an ad-hoc basis as per business or a specific and a peculiar manifestation of circumstances which could be of temporary or permanent in nature.
- Any exceptions during implementation shall be submitted by the HODs responsible for the particular vendor. These shall be submitted through an Exception Form and sign-off on the same shall be maintained by the requester.
- The Security In-charge shall review all exceptions, as the case may be, every year for validity and continuity.

Disclaimer

- JMBGRP reserves all rights and is the exclusive owner of all intellectual property rights over this Acceptable usage Policy and Procedures document. This document shall not, either in part or in full, be reproduced, published, copied, displayed, distributed, transferred, stored into any media (such as hard disks, USB Drives, Pen Drives, Memory Cards, CDS, DVD's), and/or captured or transmitted through by any means (such as electronic, digital, mechanical, photocopying, recordings, video and film or photographs and otherwise) by any person without prior consent from the Apex Committee. The Acceptable usage policy and procedure document is meant to be published on the intranet of JMBGRP and/or any other forum as decided by the management of JMBGRP. Anything not specifically stated in this Acceptable usage policy and procedure document shall not be considered as implied in any manner.
- For any clarifications related to this Acceptable usage policy and procedure document with respect to its interpretation, applicability and implementation, please raise a request in Ticketing Tool.

References:

- Control Objectives: A 8.1