Choice
The Joy of Earning

CHOICE EQUITY BROKING PVT. LTD

MOBILE DEVICE POLICY

Version Control

Action	Date	Revision Details	Prepared / Amended By	Approved By
Created On	17-Oct-16	1.0	Mahesh Tamhankar	Amit Jaokar
Reviewed On	21-Feb-17	1.1	Mahesh Tamhankar	Amit Jaokar
Reviewed On	13-Feb-18	1.2	Mahesh Tamhankar	Amit Jaokar
Reviewed On	20-Feb-18	1.3	Mahesh Tamhankar	Utpal Parekh
Reviewed On	10-Aug-19	1.4	Mahesh Tamhankar	Yogesh Jadhav
Reviewed On	11-Jan-20	1.5	Mahesh Tamhankar	Yogesh Jadhav
Reviewed On	15-July-21	1.6	Sunil Utekar	Yogesh Jadhav
Reviewed On	08-Jan-22	1.7	Sunil Utekar	Yogesh Jadhav
Reviewed On	09-Apr-23	2.0	Ashutosh Bhardwaj	Yogesh Jadhav
Reviewed On	31-Jan-24	2.1	Anil Ashok & Associates	Ashutosh Bhardwaj

1.0 Purpose

Choice Equity Securities Pvt. Ltd. and its subsidiaries, associates, and entities in India and overseas (collectively referred to as 'Choice').

The policy aims at providing guidelines to authorized users on usage of Choice supported Mobile devices for permitted corporate services.

2.0 Scope

This policy applies to users authorized to use corporate or personally owned (BYOD) mobile devices. Mobile devices currently scoped as part of this policy are limited to the following:

- Apple iOS 11.0 and later
- Apple iPad OS 13.0 and later
- Mac OS X 10.14 and later
- Android 5.0 and later (including Samsung KNOX Standard 2.4 and higher

Corporate mobility services provisioned under corporate mobile devices policy are:

- Email services
- Outlook Contacts
- Outlook Calendar
- Business Applications
- Corporate Collaboration Tools

Note: Above services shall only be provisioned via MDM (Mobile Device Management)/ MAM (Mobile Application Management). MDM/ MAM is security software that helps administer mobile device and protects corporate services/data published over mobile device with below controls:

- Protection against Jailbroken/Rooted device – MDM/ MAM detect and restrict installation of corporate application on rooted or jailbroken devices.
- Protection against unauthorized access - In case where a user does not implement screen lock, MDM/ MAM can use a policy in order to prevent data theft or unauthorized application usage.
- The corporate data is not accessible outside the MDM/ MAM container. It protects the data stored in the devices by access control policies
- Current/Updated app on all endpoints – Reduces pain of IT & user on installing updated app .Ensure all the endpoints with current/updated app.
- Data wipe – For resigned/unwanted employees or stolen devices.

3.0 Definitions

Personal Device: Device purchased and owned by an employee which can be used to deploy corporate mobile services.

Corporate service device: A mobile devices on which the corporate services are deployed.

MDM: Mobile Device Management
MAM: Mobile Application Management
Authorized software: Software required for basic functioning of the device
Unauthorized software: Software not required for basic functioning of the device.

4.0 Policy for Corporate Devices

4.1 Eligibility

- For existing employees, user will be required to raise a Logit ticket for corporate mobile device
- For new joiners, corporate mobile device may be allocated based on Logit raised by HR

4.2 Device Provisioning

- Users seeking corporate mobility service can avail the services on their personal device with appropriate versions of mobile device (as defined in scope – 2.0).
- The user's device should meet the pre-requisites and should not be rooted or-jail broken.
- A user can only have one device configured under this policy.

4.3 Device Configuring

- Corporate Devices
    - Technology Mobility team shall be responsible for configuring of corporate devices to eligible users.
    - Procurement/ Purchase/ Asset team hands over the corporate device to Technology Mobility team
    - Technology Mobility team configures the device as per corporate policy and hands over the device to user.

- Personal Devices
    - Users are required to download the company portal application and register the device with O365
    - Users are expected to complete the configuration process by following on- screen instructions
    - User shall backup the data prior configuration. Technology Mobility team will not be responsible for any data loss that happens during the configuration of corporate mobile services.

4.4 Pre-requisites

- For personal device, please refer Section 2.0.
- Data services must be available on the device to allow Technology

Mobility team to provision the corporate services.

4.5 Responsibilities

- Technology Mobility team shall be responsible for providing support for authorized corporate service devices only
- Technology Mobility team shall not be responsible for the accessories, service fees or charges incurred due to personal use of company-provided equipment or services, and any other related billing costs
- User shall be responsible and accountable for storing any personal or company's sensitive,
  proprietary or confidential information on the device under this policy.
- User shall be responsible for physical safeguarding of the mobile device.

4.6 Appropriate usage policy for corporate service device

- The user shall not use this mobile device for business activities that mandate certain safeguard / protocol to be followed in accordance with prevailing laws including but not limited to, call recording, logging, monitoring etc.
- User shall refrain from malicious downloads and storage on this device
- Users shall not install any unauthorized software (i.e hacking,
  cracking etc.) on the devices under this policy
- Users shall not leave the devices unattended anytime
- Users shall not share the device passwords with anyone
- When travelling devices would be kept within close view and shall not be left unattended at any point in time to avoid theft.
- In the event, if the device (company provided or personal) is lost or stolen, users are required to report the incident to Technology Mobility team immediately. These actions shall ensure that appropriate steps are taken to remotely wipe information residing on the device.
- The user shall not be allowed to create backup of the data on an unauthorized device.
- In case of violation, corporate services will be discontinued by the Technology Mobility team without any prior notice to the user.

4.7 Support Service Levels

- For corporate service mobile devices, Technology Mobility team would be responsible for supporting corporate applications/services only.

4.8 Exit User

- In cases where the user exits through the resignation or termination process, Technology Mobility team would remotely remove/wipe the MDM container. This activity would not impact the user's personal data stored anywhere outside the MDM container.
- For all the Apple devices, it is mandatory for the users to support the Technology Mobility team to delete their Apple ID/Profile so that the devices can be used / accessible by the Technology Mobility team.

4.9 Violation

- Any Violation of the policy, or any of its tenets, could result in disciplinary action which may even lead to and include termination of employment and civil and/or criminal prosecution under local, state and federal laws.

5.0 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 reason existing at any point of time.

- All exceptions during implementation shall be submitted by the concerned person responsible for implementation. These shall be submitted through the Exception Form and sign-off on the same shall be maintained as per the below grid.

Risk Acceptance Criteria

Action	High/Medium	Low
Reviewer	Level 1 - BU CTO Level 2 - BU Compliance Team	BU CTO
Approver	BU COO	