Use of Mobile Devices
Standard Operating Procedure (SOP)

PURPOSE

New Brunswick Community College (NBCC) recognizes that mobile devices can be a valuable tool for business purposes. The purpose of this document is to establish procedures for the usage and management of mobile devices. NBCC Information Technology (IT) is responsible for the acquisition and management of all college-owned mobile devices.

SCOPE AND LIMITATIONS

NBCC's Use of Mobile Devices procedure applies to all mobile devices (Smartphones and Tablets, excluding Laptops), which are NBCC provided or personally owned (BYOD) and used to access or process NBCC Information.

1.0 DEFINITIONS

Not applicable.

2.0 IMPLEMENTATION

NBCC needs to ensure that when users are using mobile devices special care should be taken to ensure that business information is not compromised. The mobile device SOP should consider the risks of working with mobile devices especially in unprotected environments.

All NBCC owned smartphone and tablet devices shall mandatorily enroll in NBCC Intune Mobile Device Management (MDM) solution. The Intune MDM solution enables "containerization" on smartphones and tablets where NBCC data and applications are accessible only in a secure containerized space. Users are permitted to install personal apps on devices; however, no data transfer is allowed between NBCC apps and personal apps. In case of device loss or theft, the entire device will be wiped.

Personally owned (BYOD) mobile devices (smartphones or tablets) or home devices are allowed to access NBCC Cloud Services from Office365 with only Multifactor Authentication enabled and devices enrolled in NBCC Intune as a Personal Device. The Intune MDM solution enables "containerization" on personal mobile devices where NBCC data and applications are accessible only in a secure containerized space. NBCC does not control personal apps on devices however, no data transfer is allowed between NBCC apps and personal apps. In case of device loss or theft, only the NBCC containerized apps will be wiped.

NBCC IT will ensure that all mobile devices (tablets/smartphones) that are provided by the organization (NBCC) are recorded in the Asset Inventory. This should be done before device is handed to the end user.

All NBCC provided smartphones and tablets should be registered as corporate devices in Microsoft Intune MDM and the access rights should be provided to users as per the NBCC UserID and Access Management Procedure.

Any document appearing in paper form is uncontrolled and must be compared to the electronic version.

BYOD devices should be allowed to access NBCC email and other Office365 services with per-app control capabilities and enrolled as personal devices in Microsoft Intune MDM. NBCC resources are not allowed to be accessed from public store apps (Apple AppStore and Google PlayStore)

NBCC sets the controls applicable to business information stored or processed by mobile devices based on the information classification set out in the NBCC Data Classification Guideline.

NBCC IT ensures that "Security Awareness Training" covers the risks related to mobile devices and the mitigation steps and the user responsibilities.

The NBCC **Acceptable Use of Technology Resources** shall include the terms and conditions related to use of personally owned devices for accessing NBCC application and services waiving ownership of business data, allowing remote wiping of data by the organization in case of theft or loss of the device or when no longer authorized to use the service.

2.1 Login Security

Jailbroken or Rooted devices are not permitted to be access NBCC applications or Data.

For NBCC MDM managed apps, the default login for users/staff is Active Directory UserID and password. The access control and privileges follow the NBCC UserID and Access Management Process. The password follows the NBCC Password policy.

For smartphones and tablets, the unlock mechanism is a six-digit passcode. (Users can opt for biometric mechanisms as well).

2.2 Updates

For smartphones and tablets which are NBCC provided, the updates are managed via Intune MDM Solution. For personally owned devices, the updates are managed by the respective user.

2.3 Software and Apps

The NBCC approved applications will be deployed via Microsoft Intune MDM solution for both NBCC owned devices and personal (BYOD) devices.

For NBCC provided smartphones & tablets (as they are managed by Intune MDM) the users can install personal apps. However, in case of loss or theft there will be a full device wipe.

For BYOD devices, users are advised to install software only from trusted sources only (e.g. Google Play and Apple Appstore). Users are advised to contact IT helpdesk if they are not sure.

NBCC IT shall ensure that users are not able to access the NBCC resources using Public Store Apps.

2.4 Use of Untrusted Wi-Fi networks

NBCC owned devices (smartphones and tablets) when connected to untrusted, open wireless networks should have limited accessibility and able to use only limited apps i.e. only Outlook and Microsoft Teams. It is recommended that devices are configured so that they do not automatically connect to open networks. Also, mobile devices should be connected only to Wi-Fi networks with strong security mechanisms.

A trusted network is a network that meets the standards set out in the NBCC Security standards.

2.5 Use of Mobile Hotspots

Trusted mobile hotspots (e.g. your own personal hotspot or that of a trusted partner) other than NBCC official Wi-Fi are allowed as a means of accessing the Internet while mobile as long as they conform to standards set out in the NBCC Security Standards**.**

2.6 User Responsibilities

- The assignment and use of mobile devices are in support of departmental business practices.
- Users shall report the loss or theft of mobile device within 24 hours.
- User shall enroll their personal mobile devices in NBCC MDM in required to access NBCC Information like Email and Intranet.
- Users shall ensure that the NBCC mobile devices in his or her care are only accessed by those authorized to do so.
- Users shall ensure that sensitive information is not stored or exchanged from a mobile device.
- Users shall ensure that potentially harmful applications are not installed on mobile device.
- Users shall ensure that mobile devices are not unattended and hidden from shoulder surfing when using in a public place.
- Users shall ensure that only MDM Secure Apps are used to communicate official information.
- Users shall not unenroll Corporate provided devices from MDM.
- Users shall not contact the hardware or cellular service-provider directly. All initiation, change and cancellation of services shall be requested via NBCC IT.
- Users shall remove all personal accounts including pictures, videos, and documents from corporate owned devices before handing over devices to IT as a part of checkout process. NBCC is not responsible for personal data.

2.7 Management Responsibilities

- Ensure that all users including staff and faculty participate in the NBCC security awareness training.
- Track and retrieve wireless devices assigned to employees who leave NBCC as part of the regular checkout procedures.

3.0 OTHER RELATED DOCUMENTS

NBCC – ISMS – Acceptable Use of Technology Resources (2808.4750)