एन एम डी सी

NMDC

BRING YOUR OWN DEVICE POLICY

Author		**Document name**		**Date of first issue**	
Owner	C & IT Department	**Document ref. no.**		**Date of latest re-issue**	
Version	1.1	**Page**	1 of 10	**Date of next review**	
Issue Status	Under Review/ Live	**Security classification**	Internal use only	**Reviewer**	

एन एम डी सी

NMDC

BRING YOUR OWN DEVICE POLICY

VERSION CONTROL

Revision no.	Date of issue	Prepared by	Reviewed by	Approved by	Issued by	Remarks

एन एम डी सी

NMDC

BRING YOUR OWN DEVICE POLICY

OBJECTIVE

NMDC recognizes that mobile devices, such as smartphones, tablets and laptops are now important tools for the organization and supports their use to achieve business goals. Therefore the organization grants its employees the privilege of purchasing and using smartphones, tablets and laptops of their choosing at work for their convenience.

However, mobile devices also represent a significant risk to data security. A mix of corporate and employee owned devices accessing the organization's network and data, and the use of those devices for both professional and personal purposes, can subsequently lead to data leakage and system infection. If the appropriate security applications and procedures are not applied, they can be a conduit for unauthorized access to the organization's data and IT infrastructure. Security must be central to an organization's workforce mobility strategy in order to protect corporate data, safeguard its customers, intellectual property and reputation, maintain compliance, mitigate risk and ensure mobile security across all devices.

This policy outlines a set of practices and requirements for the safe use of mobile devices and applications. It is intended to protect the security and integrity of NMDC's data and technology infrastructure. NMDC's employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the corporate network to access & process work-related communications. NMDC reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

As a Bring Your Own Device program can only be successfully implemented if certain security policies are enforced, we would expect a Mobile Device Management solution to be a prerequisite for this policy

SCOPE

All mobile devices, whether owned by the organization or owned by employees, inclusive of smartphones, tablets and laptops, that have access to corporate networks, data and systems are governed by this mobile device security policy. Temporary employees will be managed on a case-by-case basis. By default, temporary employees issued with a NMDC email address will be treated as permanent employees. The scope of this policy does not include corporate IT-managed laptops.

Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk authorized by security management must be conducted.

Applications used by employees on their own personal devices which store or access corporate data, such as cloud storage applications, are also subject to this policy.

DEVICES COVERED

Current devices approved for Bring Your Own Device use are listed below along with the minimum system requirements:

एन एम डी सी
NMDC

BRING YOUR OWN DEVICE POLICY

- Android 4.1.2 (“Ice Cream Sandwich”) or higher Smart Phones and Tablets
- iOS 9.3 or higher iPhones and iPad
- Windows Mobile 8.1 or higher
- MacOS devices with TPM 2.0 and recent versions of MacOS
- Windows 10 devices with TPM 2.0 and up-to-date versions of Windows 10

Devices below these specifications will not comply with our policies and therefore will not be allowed to be used as BYOD. It should be noted that as technology improves and newer versions of operating system are introduced by vendors or vulnerabilities are discovered in existing operating systems this list is subject to immediate change and access maybe revoked (in some instances this may be without notice).

Devices that are not on the company’s list of supported devices are not allowed to connect to the corporate network.

POLICY RULES

Technical Requirements:

1. Devices must store all user-saved passwords in an encrypted password store.
2. Devices must be configured with a secure password that complies with NMDC’s password policy. This password must not be the same as any other credentials used within the organization.
3. Devices will be subject to the valid compliance rules on security features such as encryption, password, key lock, etc. These policies will be enforced by the IT department using Mobile Device Management software.
4. Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network. This includes the installation of mobile device management (MDM) software on all mobile devices that access the company network. Only devices managed by IT through Mobile Device Management Software will be allowed to connect directly to the internal corporate network.
5. NMDC will support the following mobile device features utilizing the MDM software:
    a) Configure access to corporate Exchange email accounts
    b) Configure access to personal email accounts
    c) Configure virtual private network (VPN) settings
    d) Configure Wi-Fi network settings
    e) Enable access to the corporate directory for use in composing emails
6. NMDC will not utilize the MDM software to:
    a) Track an employee’s current location or previous locations unless attempting to locate a lost or stolen device (lost devices will only be traced upon approval of the device owner)
    b) Access an employee’s personal emails, text messages or other messages
    c) Access contact information or other information stored on the device (personal or company)
    d) Access social networking or other applications installed on the device
7. Devices’ camera and video capabilities are disabled while connected to the corporate network
8. The following apps/software programs are allowed:

BRING YOUR OWN DEVICE POLICY

(a detailed list of apps/software programs, such as weather, productivity apps, etc., which will be permitted)

9. The following apps are not allowed: (apps not downloaded through iTunes or Google Play, etc.)

User Requirements/ Acceptable Use:

1. The company defines acceptable business use as activities that directly or indirectly support the business of NMDC.
2. Users may only load corporate data that is essential to their role onto their mobile device(s).
3. Devices may not be used at any time to:
    a) Store or transmit illicit materials
    b) Store or transmit proprietary information belonging to another company
    c) Engage in outside business activities
    d) Etc.
4. Users are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the company. Such websites include, but are not limited to
    a) All entertainment websites such as YouTube, Amazon Prime, Netflix etc.
    b) All social media websites such as Facebook, Twitter etc.
    c)
5. Users may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc.
6. Users are automatically prevented from downloading, installing and using any app that does not appear on the company's list of approved apps.
7. Users must report all lost or stolen devices to NMDC's IT Department immediately.
8. If a user suspects that unauthorized access to company data has taken place via a mobile device, they must report the incident in alignment with NMDC's incident handling process.
9. Devices must not be "jailbroken" or "rooted"* or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
10. Users must not load pirated software or illegal content onto their devices.
11. Applications must only be installed from official platform-owner approved sources.
12. Installation of code from untrusted sources is forbidden. If user is unsure whether an application is from an approved source, user must contact NMDC's IT Department.
13. Devices must be kept up to date with manufacturer or network provided patches. As a minimum patches should be checked for weekly and applied at least once a month.
14. Devices must not be connected to a PC which does not have up to date and enabled anti-malware protection and which does not comply with corporate policy.
15. Devices must be encrypted in line with NMDC's compliance standards.
16. Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify NMDC's IT Department immediately.
17. The above requirements will be checked regularly and should a device be noncompliant that may result in the loss of access to email, a device lock, or in particularly severe cases, a device wipe.

एन एम डी सी
NMDC

BRING YOUR OWN DEVICE POLICY

18. The user is responsible for the backup of their own personal data and the company will accept no responsibility for the loss of files due to a non-compliant device being wiped for security reasons.
19. (If applicable to your organization) Users must not use corporate workstations to backup or synchronize device content such as media files, unless such content is required for legitimate business purposes.

*To jailbreak/root a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.

Actions which may result in a full or partial wipe of the device, or other interaction by IT

1. A device is jailbroken/rooted – This can result in full or partial wipeout of data.
2. A device contains an app known to contain a security vulnerability (if not removed within a given time-frame after informing the user) - This can result in full or partial wipeout of data.
3. IT department detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure – This can result in full or partial wipeout of data
4. A device is lost or stolen – This must be reported within 24 hours to the IT Department and will result in complete wipeout of device data. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
5. A user has exceeded the maximum number of failed password attempts – This will result in user being locked out of the device. User must approach IT Department for unlocking of device.
6. User is terminated from employment – This must be reported immediately by Personnel Department to IT department and data will be completely wiped out.

Use of particular applications which have access to corporate data

1. Cloud storage solutions: NMDC supports the use of the following cloud storage solutions xxxxxx
2. The use of solutions other than the above will lead to a compliance breach and the loss of access to the corporate network for the user

Risks/Liabilities/Disclaimers

1. While 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.
2. The company reserves the right to disconnect devices or disable services without notification.
3. The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
4. The employee is personally liable for all costs associated with his or her device.
5. The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company 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.
6. NMDC reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

एन एम डी सी

NMDC

BRING YOUR OWN DEVICE POLICY

RESPONSIBILITIES

Corporate IT Head – Overall compliance to policy

Unit Head IT – Compliance to policy at each unit