Mobile Device Policy - Departmental and Bring Your Own Device (BYOD)

Purpose of this policy

The purpose of this policy is to provide high level directives on the use, deployment, and maintenance of mobile devices within the Department of Planning and Environment (the department) and any agency utilising our services with the intention to ensure that:

- All employees are aware of their individual responsibilities in relation to the use and security of mobile devices for the transmission and storage of information and access to the department's ICT assets.
- The risks introduced by using mobile devices are minimised and managed.
- The correct processes and procedures are developed and employed when using mobile devices and technologies.
- Mobile devices used for the department's purposes are protected by appropriate security measures consistent with the security requirements of the department's information.

This policy is written to be consistent with the ISO/IEC 27002:2013 Information Security Standard. It complements the Code of Ethics and Conduct, and supports the requirements set out within the Information Security Management System (ISMS) so that the department can achieve its information security objectives.

To whom this policy applies

This policy applies to everyone using departmental or BYOD Mobile Devices when accessing the department's information and ICT resources, including employees, individuals seconded from other organisations, volunteers, contingent or labour hire workers, and professional services contractors.

For the purpose of this policy, mobile devices comprise any equipment that connects to a network using a SIM card or similar device and accessing the department's information and ICT resources except Laptop computers. This includes but is not limited to satellite phones, mobile phones, tablets, telemetry devices, modems, photographic and recording equipment. Laptop computers and ancillary devices (such as smart watches) are specifically excluded under the scope of this policy. BYOD Mobile Devices is the practice of allowing employees to use their own mobile devices for work purposes.

Policy statements

Acceptance conditions

The use of any mobile device to access departmental systems or data requires acceptance of this policy (as detailed in the sections that follow), in addition to the following specific conditions:

- An employee using a BYOD Mobile Device must complete the registration process and adhere to this policy to access departmental information.
- The owner/user of any device must accept the installation of a department-controlled profile on the device. This profile will enforce certain security-related configuration parameters for department data and must not be overridden or otherwise subverted.
- The department may install Mobile Device Management (MDM) solutions on a Departmental Mobile Device without requiring the user's consent, provided the application is needed to satisfy an authorised business requirement and is intended to protect department data.
- A BYOD Mobile Device becomes a managed mobile device once MDM solutions have been installed with the user's consent.
- The user of the mobile device is responsible for ensuring the device software is updated regularly and in line with new operating system and software releases, to ensure security risks are not introduced to the department's infrastructure when connected.
- After the department-controlled profile is deployed, the managed mobile device is supported specifically for connectivity to approved departmental services such as departmental email (via Microsoft Outlook only) and Microsoft Teams. Under this approach, the department will only have control over departmental applications and data (e.g. Outlook email, Teams) with no visibility, control or potential impact to personal applications and data on the mobile device. For example, remote wipe capabilities will only apply to the department applications and department data on managed BYOD Mobile Devices.
- The department will accept no liability for functionality, serviceability or performance issues associated with any BYOD Mobile Device as there are numerous configurations of devices and software that can impact a device and be unrelated to the device being enrolled to MDM. Any responsibility of warranty will reside solely between the owner/user of the BYOD Mobile Device and the supplier/manufacturer.
- The department reserves the right to delete departmental information and applications on managed mobile devices and/or disable the device's access to departmental information at any time, at its sole discretion.
- If a device is found to contain malware and/or there is a risk to sensitive departmental data and/or systems, the department reserves the right to delete departmental information and applications from the managed mobile device.
- It is intended that the SIM card is not removed from the Departmental Mobile Device.
- The Departmental Mobile Device is intended for use by the employee.

Where the above terms are not accepted, access to departmental systems and data (e.g., Outlook email and Teams) will not be available from the mobile device.

Eligibility

- An employee may be eligible to have a Departmental Mobile Device provided if it is deemed necessary to their position, and at the managers discretion.
- The type of mobile devices offered by the department are at the discretion of Digital Information Office (DIO) so the department can ensure the devices are supported.
- The range of mobile devices available will be minimised to reduce support costs.

Use of mobile devices

- In order to connect to departmental infrastructure or services, users will be required to ensure acceptance of terms and conditions as detailed in this policy.
- A mobile device management (MDM) solution must be installed and enabled on all Departmental Mobile Devices, to enforce minimum security settings necessary to protect departmental systems and information stored or available on the mobile device. A MDM solution must be enabled on BYOD Mobile Devices where users wish to access departmental systems and data from their device.
- For BYOD Mobile Devices, department applications and data must be managed separately from personal application and data.
- Access to departmental information and applications will only be available through approved software (e.g., Outlook for email, Teams for messaging and collaboration) on managed mobile devices. On these mobile devices, any other applications may be installed at the user's discretion, but these other applications must not have access to department services or data.
- The MDM application on BYOD Mobile Devices may be removed by the owner of the device. The department reserves the right to remove the MDM application from the device at any time without prior notification and at its own discretion. Once the MDM application has been removed, department applications and data can no longer be accessed from the device.
- On Departmental Mobile Devices, removal of the MDM application must only be done by an authorised departmental ICT representative. As a part of this process, all departmental data stored on the device will be wiped and access to department systems will no longer be available.
- Repeated entry of invalid PINs will completely wipe any managed device after 10 attempts.
- Only devices running vendor supported products and applications with regular security updates can be used to access departmental systems and information.
- Jail-broken devices are prohibited from accessing or storing departmental systems or data.
- Users must apply mobile device operating system and application updates in a timely manner. In this context, checks and installs for updates must be set to automatic, or performed at least monthly.

- Licenced media (e.g., music) is permitted. However, any information which infringes copyright or any other form of intellectual property rights (e.g., other music libraries, movies etc.) must not be stored on any device owned by the department.
- Access to and storage of any material that could be considered, obscene, abusive, discriminatory, bullying or harassment, or may otherwise be considered illegal or unethical, is prohibited from any departmental device. Such use may result in disciplinary processes in accordance with the Code of Ethics and Conduct.

Misplaced, stolen, damaged or breached mobile devices

- The department expects all employees to take care of Departmental Mobile Devices. It is the employee's responsibility to take all necessary measures to ensure a device is not damaged, lost or stolen.
- The user of the mobile device must notify the mobile services group/ mobile service provider in the first instance immediately upon loss, theft, breach or suspected loss, theft, breach of a managed device. The department reserves the right to remotely wipe departmental applications and data or reset the device. In these circumstances, departmental services associated with the device must be disabled. For BYOD Mobile Devices, only the departmental applications and data will be wiped.
- Costs for lost or damaged Departmental Mobile Devices will be billed to the employee's cost centre.
- If the Departmental Mobile Device is faulty or damaged, an assessment will be made as to whether the device can be replaced under warranty.
- Hardware models change frequently, however the base functionality required for Departmental Mobile Devices is relatively static. Devices are expected to have an operational life of three to five years. Unserviceable devices will be repaired where economically feasible and devices that cannot be upgraded to the latest software must be replaced.
- Protective cases are provided with all Departmental Mobile Devices and must be used to shield the devices from undue wear, tear and damage.

Use of Devices Outside Home and Office – Local and Overseas

- Every effort should be made to not be leave Mobile Devices unattended in a motor vehicle or visible in a public space.
- The use of a mobile device while driving is illegal. Any employee fined for using their phone whilst driving will be personally liable for the infringement.
- Mobile Devices must be carried as hand luggage and/or in close personal proximity when travelling.
- Wi-Fi services at home and in department offices may be used to connect to departmental systems and data from mobile devices. Wi-Fi services provided outside these environments

(such as hotel, airport, coffee shop Wi-Fi) should be treated as untrusted and should be avoided wherever possible.

- Mobile and data access when travelling overseas is very costly. With manager approval, the Mobile Services Group/mobile service provider will arrange for the activation and subsequent deactivation of international roaming/dialling for departmental mobile plans as well as data packs on an "as needs" basis. International voice call and data service usage (e.g., internet, email, streaming etc) must only be used when essential. While overseas, personal use must be minimised otherwise the employee may be liable for excessive mobile usage fees. The department is not responsible for any costs incurred using BYOD Mobile Devices.
- Mobile data services may be used where home or department Wi-Fi services are not available. This applies both within Australia and when overseas (where data roaming has been enabled as above). Note that access to departmental applications and services is blocked by default from overseas locations unless specific arrangements are made before departure, through a request to the Mobile Services Group/ mobile service provider.
- Use of Bluetooth with mobile devices is approved, including in public places. However, initial pairing of mobile devices with peripherals (e.g. AirPods) should always be performed away from crowded environments to limit the potential for signal interception.
- Similarly, for department and BYOD Mobile Devices, employees must not use chargers borrowed from unknown persons or the use of public charging stations, to avoid risks associated with charger-based hardware attacks.

Protection of Information on Mobile Devices

- Every reasonable effort must be made to ensure that departmental information is not compromised using mobile devices in a public place. Screens displaying sensitive information (refer to NSW Government Information Classification, Labelling and Handling Guidelines) must not be seen by unauthorised persons.
- Departmental data may be stored on mobile devices from time to time, but this is expected to be only temporary, with the primary copy maintained within the department's approved records management system (e.g. CM9). Mobile devices are not to be used as the sole repository for departmental information. All departmental information stored on mobile devices must be regularly backed up to an appropriate and approved network location.
- Personal mobile data and backup solutions such as Dropbox, iTunes and iCloud must not be used to store departmental data either in raw or backup formats.
- Departmental Mobile Devices should be used by the employee. Wi-Fi hotspot functions should be turned off when not in use for business purposes and a difficult to guess password should be set.
- Information transported outside department's office environment on mobile devices must satisfy the requirements defined in the NSW Government Information Classification, Labelling and Handling Guidelines.

Purchase of Equipment and Ownership

- The department is the legal owner of all physical and electronic information, computing and communication technology resources created or acquired to conduct the department's business. For BYOD Mobile Devices, ownership applies to only the related departmental information, and specifically excludes the device itself.
- The department delegates to its employees, daily management responsibility and custodianship of information and ICT resources for their use, maintenance and protection. With best effort and due care, employees are responsible for upholding the department's policies to protect the department's information and ICT resources.
- Departmental Mobile Devices must be purchased through approved channels. Individuals or business units must not buy their own Departmental Mobile Devices unless they have written approval from Mobile Services Group, which is typically only provided in an emergency.
- If it is deemed appropriate and approved by management, an employee's private number may be brought onto the department corporate account once all personal fees and charges are paid by the end user to their current telecommunications provider. At the cessation of employment this number can be transferred back to the employee's personal account or future employer account with managers written approval.
- In the event of an employee leaving the department, all Departmental Mobile Devices and related equipment assigned to that employee must be returned to our mobile service provider or transferred to another employee prior to leaving the department. The mobile service will be disconnected on the last day of duty unless a transfer has been completed.

Usage and Service Charges

- To protect public interests in the use of public resources, employees have no inherent right to use the department's ICT resources for non-government purposes. To this end, Departmental Mobile Devices should be primarily used for authorised business purposes; however, limited personal use is permitted if it does not have an adverse impact on department use and services.
- Departmental Mobile Device usage will be subject to monthly review by managers and this data will be provided in reports. If it is found that an employee is using their device irresponsibly, the employee may have that device removed and be required to reimburse the department for calls or data consumption caused by excessive personal use. The individual's business unit may be charged for excess calls or data associated with personal use.
- Calls will be limited to mobile, local and STD numbers. Calls to overseas numbers require manager approval. Calls that attract a higher rate such as 1300 numbers are restricted. Calls that are competition lines, for gambling or questionable in view of the department's acceptable use policy are prohibited.

Monitoring

- Departmental Mobile Devices may be subject to monitoring that is consistent with the 'Monitoring' section of the DPE Acceptable Use Policy.
- The department reserves the right to similarly monitor activities in relation to departmental systems and departmental data access from BYOD Mobile Devices. Other systems and data access on BYOD Mobile Devices will not be subject to central monitoring.

Exemptions

- Exemptions to this policy must comply with the ISMS Exemption Request Management Standard.
- Exemptions must only be approved where it is technically, practically or financially infeasible to comply with this policy.
- Reviews of exemptions must be performed annually.

Failure to comply with this policy

Ethical and behavioural standards that employees are expected to demonstrate while working with the department are set out in the respective Code of Ethics and Conduct. If employees fail to meet those standards, corrective action may be taken in accordance with the respective Code of Ethics and Conduct.

Individuals who are not government sector employees such as volunteers, contingent or labour hire workers, professional services contractors and consultants may have their services, contract or agreement terminated immediately, or legal action could be taken if they are found to have violated this policy.

Review timeframe

The Chief Digital and Information Office will review this policy no later than 3 years from the date the document is approved. The document may be reviewed earlier in response to post-implementation feedback, changes to legislation, or as necessary.

Related documents

A full list of legislative requirements that may impact information security is maintained within the Information Security Management System (ISMS).

- ISO/IEC 27001: 2013 - Information technology - Security techniques - Information security management systems - Requirements
- ISO/IEC 27002: 2013 - Information technology - Security techniques - Code of practice for information security management

This policy should be read in conjunction with the following documents:

- DPE Cyber Security Policy
- Acceptable Use Policy
- ISMS Exemption Request Management Standard
- DPE Code of Ethics and Conduct
- NSW Cyber Security Policy
- NSW Government Information Classification, Labelling and Handling Guidelines

Policy metadata

Table 1. Policy metadata

Category	Description
Status	Final
Date of approval	23 March 2023
Approver	Chief Operating Officer
Group	Corporate Services
Division	Digital Information Office
Policy owner	Chief Digital and Information Officer
Document location	DPE Intranet
Next review date	April 2024
Associated procedure	N/A
Any additional applicability	Additional applicability will be considered in the future.
Superseded document	Mobile Communication Device Policy Bring Your Own Smart Device-Usage-Agreement DPIE Bring Your Own Smart Device App Protection Policies
Further information	cybersecurity@dpie.nsw.gov.au
Document Reference	POL23/1

Version control

Table 2. Version Control

Version	Date issued	Change
0.5	20/10/2022	Updated based on feedback received
0.6	1/12/2022	Updated based on feedback received by P&C, Industrial Relations, and Legal
0.7	20/12/2022	Updated following QA performed by Governance
0.8	15/02/2023	Updated based on feedback received by the COO

Version	Date issued	Change
0.9	8/03/2023	Updated based on feedback by the CDIO and the Office of the Chief Operating Officer/ removed markup – final draft for approval
1.0	24/03/2023	Approved/Final
1.1	29/08/2023	Updated scope to exclude ancillary devices

Appendices

Appendix 1 – Definitions (example)

Appendix 2 - Roles and responsibilities (example)

Appendix 1 – Definitions

Table 3 - Definitions

Term	Definition
Accountable Authority	As defined in Section 2.7 Government Sector Finance Act 2018
BYOD Mobile Device	The practice of allowing the employees of an organisation to use their own computers, smartphones, or other devices for work purposes.
Deletion	Deletion of information and/or applications on a BYOD device only affects departmental information and applications. Personal information and applications will always remain unaffected.
Departmental Mobile Device	A departmental device is provided to an employee by a department to support them in their daily work activities as required by their role. The departmental device is owned by the relevant department. While some personal use of the departmental device is permitted, the department may erase all departmental information from the device under certain scenarios, i.e. in case of a security breach.
Employee	Any individual employed, appointed, or otherwise attached to the Department, whether on an ongoing, temporary, contractor, casual, or voluntary basis This includes all senior executives and secondees from other agencies and may include contractors and employees of any firm or company contracted to perform work on behalf of the department subject to the nature of the policy and its application. Employee also includes those employed by the department who provide services to other entities.
GSF	*Government Sector Finance Act 2018* (NSW)
Head of Agency	Consistent with the *Government Sector Employment Act 2013* (NSW), a Head of Agency is defined for the purpose of this policy framework as: In the case of DPE – the secretary of the department In any other case – the Head of Agency listed in Part 2 or Part 3 of Schedule 1 of the GSE Act, such as chief executive, commissioner or chairperson. In practice, this represents the key person responsible for directing the affairs of the agency.

Term	Definition
Mobile Device	For the purpose of this policy, mobile devices comprise any equipment that connects to a network using a SIM card or similar device and accessing the department's information and ICT resources. This includes but is not limited to satellite phones, mobile phones, tablets, telemetry devices, modems, photographic and recording equipment). Laptop computers are specifically excluded under the scope of this policy.
Mobile Device Management (MDM)	Mobile device management is the process of securing, monitoring and supporting the use of mobile devices, such as smartphones and tablets, in the workplace. The function of MDM is to control data, configuration settings and applications on all mobile devices used within a company or organisation.
Personal information	has the meaning as defined in the Privacy and Personal Information Act 1988.
User	Employees, contractors, consultants and volunteers engaged by department agency who have access to any department's ICT resources.

Appendix 2 - Roles and responsibilities

Table 4: Roles and responsibilities

Roles	Responsibilities
All Employees	Responsible for compliance with this policy, and any supporting policies, standards and procedures. Reporting security incidents and any identified weaknesses.
Managers and Supervisors	The proper induction of new users, and to ensure that all personnel in their area are made aware of this policy and the consequences of breaching it.
Mobile Services Group	Approving devices and models acceptable for use as a Departmental Mobile Device. Coordinating and managing the purchase of Departmental Mobile Devices, departmental call and data plans and services, including international roaming services. Management of internal billing for telecommunications charges. Providing first level support for Departmental Mobile Devices, including the management of potentially lost, stolen, damaged or breached devices.
Chief Digital and Information Officer	Reviews and approves this policy (as delegated by the Executive Leadership Team via the Partnership Committee).
Chief Information Security Officer	Develops, maintains and improves this policy. Monitors and reports on compliance to this policy (effectiveness measurements). Reviews exemptions from this policy.

Roles	Responsibilities
Mobile Service Provider	Configuration of the mobile device management (MDM) solution in line with policy requirements of the department. Ongoing administration, monitoring and support the MDM solution on behalf of the department.