22.4. Non-Agency Owned Devices and Bring Your Own Device (BYOD)

Objective

22.4.1. Where an Agency permits personnel to supply their own mobile devices (such as smartphones, tablets and laptops), Official Information and agency information systems are protected to a level equivalent to an agency provided and managed office environment.

Context

Scope

22.4.2. This section provides information on the use and security of **non-agency owned or provided** mobile devices when used for official business. This is commonly known as Bring Your Own Device (BYOD). The use of agency owned devices is described earlier in Section 21.1 – Agency Owned Mobile Devices.

22.4.3. In the context of this section, a BYOD Network is any agency owned or provided network dedicated to BYOD. A BYOD Network is usually within an agency's premises but does NOT include networks and related services provided by commercial telecommunication or other technology providers.

22.4.4. BYOD will introduce a wide range of risks, including information and privacy risks, to an organisation, in addition to the existing ICT risks and threats. Agencies will need to carefully examine and consider the security, privacy, governance, assurance and compliance risks and implications of BYOD.

22.4.5. Mobile devices are a "soft" target for malware and cybercrime providing a further attack channel or vector for organisational ICT infrastructures and networks. Risks fall principally into the following categories:

- Data exfiltration and theft;
- Data tampering;
- Data loss;
- Malware;
- System outages and Denial of Service; and
- Increased incident management and recovery costs.

References

22.4.6.

Reference	Title	Publisher	Source
	Risk Management of Enterprise Mobility including Bring Your Own Device	ASD	https://www.cyber.gov.au/acsc/view-all-content/publications/risk-management-enterprise-mobility-including-bring-your-own-device
	BYOD Guidance: Device Security Considerations	GOV.UK	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/360960/BYOD_Guidance_-_Device_Security_Considerations.pdf (PDF, 235 KB)
	End User Devices Security and Configuration Guidance	NCSC, UK	https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device
NIST Special Publication 800-121, Revision 2, May 2017	Guide to Bluetooth Security	NIST	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf (PDF, 2.1 MB)
NIST Special Publication 800-46, Revision 2, July 2016	Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security	NIST	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf (PDF, 579 KB)
NIST Special Publication 800-114, Revision 1, July 2016	User's Guide to Telework and Bring Your Own Device (BYOD) Security	NIST	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf (PDF, 435 KB)

Rationale & Controls

Risk Assessment

22.4.7.R.01. **Rationale**

Commonly termed "Bring Your Own Device" (BYOD), personal use of mobile computing in an organisational environment is widespread and personnel have become accustomed to the use of a variety of personal mobile devices. BYOD can have many advantages for an agency and for personnel. At the same time, BYOD will introduce a range of new information security risks and threats and may exacerbate existing risks.

22.4.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4597]

Agencies MUST undertake a risk assessment and implement appropriate controls BEFORE implementing a BYOD Policy and permitting the use of BYOD.

22.4.7.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4598]

Agencies MUST take an integrated approach to BYOD security, covering policy, training, support, systems architecture, security, systems management, change management, incident detection & management and business continuity.

Applicability and Usage

22.4.8.R.01. **Rationale**

BYOD introduces number of additional risks and attack vectors to agency systems. Not all BYOD risks can be fully mitigated with technologies available today. It is therefore important that, where feasible, all the controls specified in this section are implemented.

22.4.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4623]

BYOD MUST **only** be permitted for agency information systems up to and including RESTRICTED.

22.4.8.C.02. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must Not** [CID:4624]

BYOD MUST NOT be used for CONFIDENTIAL, SECRET or TOP SECRET systems.

Technical Controls

22.4.9.R.01. **Rationale**

"Jail-Breaking" and "rooting" are terms applied to devices where operating systems controls have been by-passed to allow installation of alternate operating systems or software applications that are not otherwise permitted. This is a risky practice and can create opportunities for device compromise. Users may wish to alter settings to allow the download of personal apps. This can result in security setting violations.

22.4.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:4627]

Devices that have been "jail-broken", "rooted" or have settings violations MUST NOT be used for any agency business or be allowed to connect to any agency systems UNLESS this been specifically authorised.

BYOD Policy

22.4.10.R.01. **Rationale**

Technical controls fall into two categories: organisational systems and device controls. Protection for organisational systems will start with a risk assessment which guides the development of a secure architecture to support BYOD operations. Additional controls will need to be applied to individual devices. The privacy of user data should be considered. A user policy is essential.

22.4.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4630]

Agencies may identify additional policy provisions and controls that are required, based on their assessment of risk. Agencies MUST implement the additional controls and protocols before implementing BYOD.

22.4.10.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4631]

Agencies MUST implement a BYOD acceptable use policy, agreed and signed by each person using a BYOD device.

22.4.10.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4632]

The agency's policy MUST clearly establish eligibility of personnel for participation in the agency BYOD scheme.

22.4.10.C.04. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4633]

Personnel MUST have written authorisation (usually managerial approval) before a connection is enabled (on-boarding).

22.4.10.C.05. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4634]

Written authorisation MUST include the nature and extent of agency access approved, considering:

- time, day of the week;
- location; and
- local or roaming access.

22.4.10.C.06. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4635]

Procedures MUST be established for removal of agency installed software and any agency data when the user no longer has a need to use BYOD, is redeployed or ceases employment (off-boarding).

22.4.10.C.07. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4637]

Standard Operating Procedures for the agency's BYOD network MUST be established.

22.4.10.C.08. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4638]

Provision MUST be made for contractors and other authorised non-employees. It is at the agency's discretion whether this activity is permitted. The risk assessment MUST reflect this factor.

22.4.10.C.09. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4639]

Ownership of data on BYOD devices MUST be clearly articulated and agreed.

22.4.10.C.10. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4643]

Agency policies MUST clearly articulate the separation between corporate support and where individuals are responsible for the maintenance and support of their own devices.

22.4.10.C.11. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4644]

Agency policies MUST clearly articulate the acceptable use of any GPS or other tracking capability.

22.4.10.C.12. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4645]

Individual responsibility for the cost of any BYOD device and its accessories MUST be agreed.

22.4.10.C.13. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4646]

Individual responsibility for replacement in the event of loss or theft MUST be agreed.

22.4.10.C.14. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4647]

Individuals MUST be responsible for the installation and maintenance of any mandated BYOD-based firewalls and anti-malware software and for implementing operating system updates and patches on their device.

22.4.10.C.15. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4648]

The procedures for purchasing and installing business related applications on the mobile devices MUST be specified and agreed.

22.4.10.C.16. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4650]

The responsibility for payment of voice and data plans and roaming charges MUST be specified and agreed.

BYOD Infrastructure and System Controls

22.4.11.R.01. **Rationale**

The use of BYOD presents increased risk and threat to agency systems. Changes to an agency's security architecture are necessary in order to minimise and manage the increased risk and threat to agency systems, information and information privacy.

22.4.11.R.02. **Rationale**

It is important that the principles of separation and segregation are applied to any system architecture or design to assist in the management of risk in BYOD systems.

22.4.11.R.03. **Rationale**

BYOD devices will seek to establish multiple connections through Wi-Fi "hot spots", Bluetooth connection and simultaneous internet and cellular connections. This behaviour creates multiple simultaneous "back channels" which can provide attack vectors for malicious activities and is considered to be high risk.

22.4.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4655]

A security architectural review MUST be undertaken by the agency before allowing BYOD devices to connect to agency systems.

22.4.11.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4656]

The BYOD network segment MUST be segregated from other elements of the agency's network.

22.4.11.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4657]

Agencies MUST architecturally separate guest and public facing networks from BYOD networks.

22.4.11.C.04. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4658]

Network configuration policies and authentication mechanisms MUST allow access to agency resources ONLY through the BYOD network segment.

22.4.11.C.05. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4659]

Access to internal resources and servers MUST be carefully managed and confined to only those services for which there is a defined and properly authorised business requirement.

22.4.11.C.06. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4660]

Wireless access points used for access to agency networks MUST be implemented and secured in accordance with the directions in this manual (See Section 18.2 – Wireless Local Area Networks).

22.4.11.C.07. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4661]

Bluetooth on BYOD devices MUST be disabled while within designated secure areas on agency premises.

22.4.11.C.08. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4662]

Access Controls MUST be implemented in accordance with Chapter 16 – Access Control.

22.4.11.C.09. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4663]

Agencies MUST maintain a list of permitted operating systems, including operating system version numbers, for BYOD devices.

22.4.11.C.10. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4664]

Agencies MUST check each BYOD device for malware and sanitise the device appropriately before installing agency software or operating environments.

22.4.11.C.11. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4665]

Agencies MUST check each BYOD device for malware and sanitise the device appropriately before permitting access to agency data.

22.4.11.C.12. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4666]

BYOD MUST have a Mobile Device Management (MDM) solution implemented with a minimum of the following enabled:

- The MDM is enabled to “wipe” devices of any agency data if lost or stolen;
- If the MDM cannot discriminate between agency and personal data, all data, including personal data, is deleted if the device is lost or stolen;
- The MDM is capable of remotely applying agency security configurations for BYOD devices;
- Mobile device security configurations are validated (health check) by the MDM before a device is permitted to connect to the agency’s systems;
- “Jail-broken”, “rooted” or settings violations MUST be detected and isolated;
- “Jail-broken” devices are NOT permitted to access agency resources;
- Access to agency resources is limited until both the device and user is fully compliant with policy and SOPs;
- Auditing and logging is enabled; and
- Changes of Subscriber Identity Module (SIM) card are monitored to allow remote blocking and wiping in the event of theft or compromise.

22.4.11.C.13. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4667]

Intrusion detection systems MUST be implemented.

22.4.11.C.14. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4668]

Continuous monitoring MUST be established to detect actual or potential security compromises or incidents from BYOD devices. Refer also to Chapter 6 - Information Security Monitoring.

22.4.11.C.15. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4669]

Agencies MUST maintain a list of approved cloud applications that may be used on BYOD devices.

22.4.11.C.16. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4670]

Agencies MUST block the use of unapproved cloud applications for processing any agency or organisational data.

22.4.11.C.17.

Control System Classifications(s): All Classifications; Compliance: Must Not [CID:4671]

BYOD devices MUST NOT be permitted direct connection to internal hosts, including all other devices on the local network.

22.4.11.C.18. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:4672]

BYOD devices connecting to guest and public facing networks MUST NOT be permitted access to the corporate network other than through a VPN over the Internet.

22.4.11.C.19. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4674]

Bluetooth on BYOD devices SHOULD be disabled while within agency premises and while accessing agency systems and data.

22.4.11.C.20. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4675]

BYOD devices and systems SHOULD use Multi-factor (at least two-factor) authentication to connect to agency systems and prior to being permitted access to agency data.

Wireless IDS / IPS systems

22.4.12.R.01. **Rationale**

Devices will automatically associate with the strongest signal and associated Access Point (AP). A rogue AP may belong to another organisation in an adjacent building, contractor, customer, supplier or other visitor. Association with a rogue AP can provide a means for the installation of malware.

22.4.12.R.02. **Rationale**

Wireless IDS / IPS systems have the ability to detect rogue wireless AP's by channel, MAC address, frequency band and SSID. They can continuously monitor wireless networks and detect and block denial-of-service and adversary-in-the-middle wireless attacks. Establishing baselines of known authorised and unauthorised devices and AP's will assist in detecting and isolating any rogue devices and AP's.

22.4.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4679]

Agencies MUST implement a wireless IDS /IPS on BYOD wireless networks.

22.4.12.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4680]

Agencies MUST implement rogue AP and wireless "hot spot" detection and implement response procedures where detection occurs.

22.4.12.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4681]

Agencies SHOULD conduct a baseline survey to identify:

- All authorised devices and AP's; and
- Any unauthorised devices and AP's.

BYOD Device Controls

22.4.13.R.01. **Rationale**

Mobile devices are susceptible to loss, theft and being misplaced. These devices can be easily compromised when out of the physical control of the authorised user or owner. To protect agency systems it is important that BYOD devices are also secured and managed on an ongoing basis.

22.4.13.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4684]

Any agency data exchanged with the mobile device MUST be encrypted in transit (See Chapter 17 – Cryptography).

22.4.13.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4685]

Any agency data stored on the device MUST be encrypted (including keys, certificates and other essential session establishment data).

22.4.13.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4686]

The use of virtual containers, sandboxes, wraps or similar mechanisms on the mobile device MUST be established for each authorised session for any organisational data. These mechanisms MUST be non-persistent and be removed at the end of each session.

22.4.13.C.04. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4687]

Any sensitive agency data MUST be removed and securely deleted, or encrypted at the end of a session.

22.4.13.C.05. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4688]

Connections to the agency network MUST be time limited to avoid leaving a session "logged on".

22.4.13.C.06. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4689]

Communications between the mobile device and the agency network MUST be established through a Virtual Private Network (VPN).

22.4.13.C.07. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4690]

Agencies MUST disable split-tunnelling when using a BYOD device to connect to an agency network (See Section 21.1 – Agency Owned Mobile Devices).

22.4.13.C.08. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4691]

Agencies MUST disable the ability for a BYOD device to establish simultaneous connections (e.g. wireless and cellular) when connected to an agency's network.

22.4.13.C.09. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4692]

The use of passwords or PINs to unlock the BYOD device MUST be enforced in addition to all other agency authentication mechanisms.

22.4.13.C.10. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4693]

BYOD device passwords MUST be distinct from any agency access and authentication passwords.

22.4.13.C.11. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4694]

BYOD passwords MUST be distinct from other fixed or mobile agency network passwords (See Section 16.1 – Identification and Authentication for details on password requirements).

Additional Controls

22.4.14.R.01. **Rationale**

There are many new devices and operating system versions being frequently released. It may not be feasible or cost-effective for an agency to support all combinations of device and operating system.

22.4.14.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4697]

Agencies SHOULD compile a list of approved BYOD devices and operating systems for the guidance of staff.

22.4.14.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4698]

Agencies SHOULD consider the implementation of Data Loss Prevention (DLP) technologies.

22.4.14.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4699]

Agencies SHOULD consider the use of bandwidth limits as a means of controlling data downloads and uploads.

22.4.14.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4700]

Agencies SHOULD take legal advice on the provisions in their BYOD policy.