NSW Government

Mobile Device & Application Framework

Version 1.0

standards@finance.nsw.gov.au
ICT Services
Office of Finance & Services
McKell Building
2-24 Rawson Place
SYDNEY NSW 2000

CONTENTS

1. CONTEXT

1.1. Background

Developing whole of NSW government ICT technical standards is a key initiative of the *NSW Government ICT Strategy 2012*, driven by the ICT Procurement and Technical Standards Working Group and under the oversight of the ICT Leadership Group. This framework consists of a series of technical standards developed through these arrangements.

This framework contains standards to assist agencies when procuring mobility solution services. It aims to assist agencies to select the mobility solution that meets their business requirements, while ensuring there is a standard approach to mobility solutions procurement across government.

1.2. Purpose

This document provides information and technical guidance to agencies when procuring mobility solution services. It details the issues that need to be considered so each agency can identify the available options that best suit their business requirements as they define their agency specific strategy and approach, for example a mobility or BYOD strategy and policy.

1.3. Scope and application

This document falls within the framework of the *NSW Government ICT Strategy*, and applies to all NSW Government departments, statutory bodies and shared service providers. It does not apply to state owned corporations, but is recommended for guidance and adoption.

The document also supports the ICT Service Catalogue by defining the range of mobility services that may be made available to NSW Government agencies.

1.4. Fundamental principles

1. Standards are enduring and should not require modification as technology changes, however there is scope to modify them through the governance arrangements if necessary.
2. Standards are designed to add value, augment and be complementary to, other policies. The standards leverage principles defined in the *NSW Government ICT Strategy*, the *NSW Government Cloud Services Policy* and data and information management guidelines.
3. This document does not override nor circumvent the responsibilities of an agency nor any employee regarding the management and disposal of information, data, and assets.
4. Standards in ICT procurement must address business requirements for service delivery.

1.5. Data standards

The standards in this together with data and information management standards and in accordance with Premier's Memorandum M2012-15 *Digital Information Security Policy*.

NSW Government agencies must carefully consider their obligations to manage government data and information. Contract arrangements and business processes should address requirements for data security, privacy, access, storage, management, retention and disposal. ICT systems and services should support data exchange, portability and interoperability.

1.6. Additional considerations

Embracing a mobile device and application framework for employees does not just require consideration of technological matters. Other matters that need to be considered include financial, human resource, legal and risk management impacts. Be sure that issues such as payment for data network access, ownership of information and working hours/conditions are addressed.

Other matters for consideration are the Acts and policies listed below.

1.7. Reference documents

The following statutory rules and other NSW Government policy documents provide direct or related guidance the use of technology and the collection, storage, access, use and disclosure of data by NSW public sector agencies:

- *AS/NZS ISO 31000 Risk management - Principles and guidelines*
- *Electronic Transactions Act 2000*
- *Government Information (Information Commissioner) Act 2009*
- *Government Information (Public Access) Act 2009*
- *Health Records and Information Privacy Act 2002*
- *M2012-15 Digital Information Security Policy*
- NSW Government Cloud Policy
- NSW Government ICT Strategy 2012
- NSW Government Social Media Policy
- *TPP 09-05 - Internal Audit and Risk Management Policy for the NSW Public Sector*
- *Privacy and Personal Information Protection Act 1998*
- *Public Finance and Audit Act 1983*
- *Public Interest Disclosures Act 1994*
- Small and Medium Enterprises Policy Framework
- *State Records Act 1998*

This standard should also be used with agency-specific risk management frameworks and agency codes of conduct.

2. GOVERNANCE

2.1 Development of standards

The ICT Procurement and Technical Standards Working Group, chaired by the Office of Finance & Services, includes is made up of senior officers with technical expertise and a high level business perspective. It is responsible for the identification and development of the NSW Government ICT procurement and technical standards. The ICT Leadership Group, comprising Chief Information Officers and senior business managers from across government, is responsible for endorsing agreed standards.

2.2 Implementation of standards

NSW Procurement will facilitate the implementation of the standards by applying them to the goods and services made available through ICT Services Catalogue. The standards will also be available on the ProcurePoint web site.

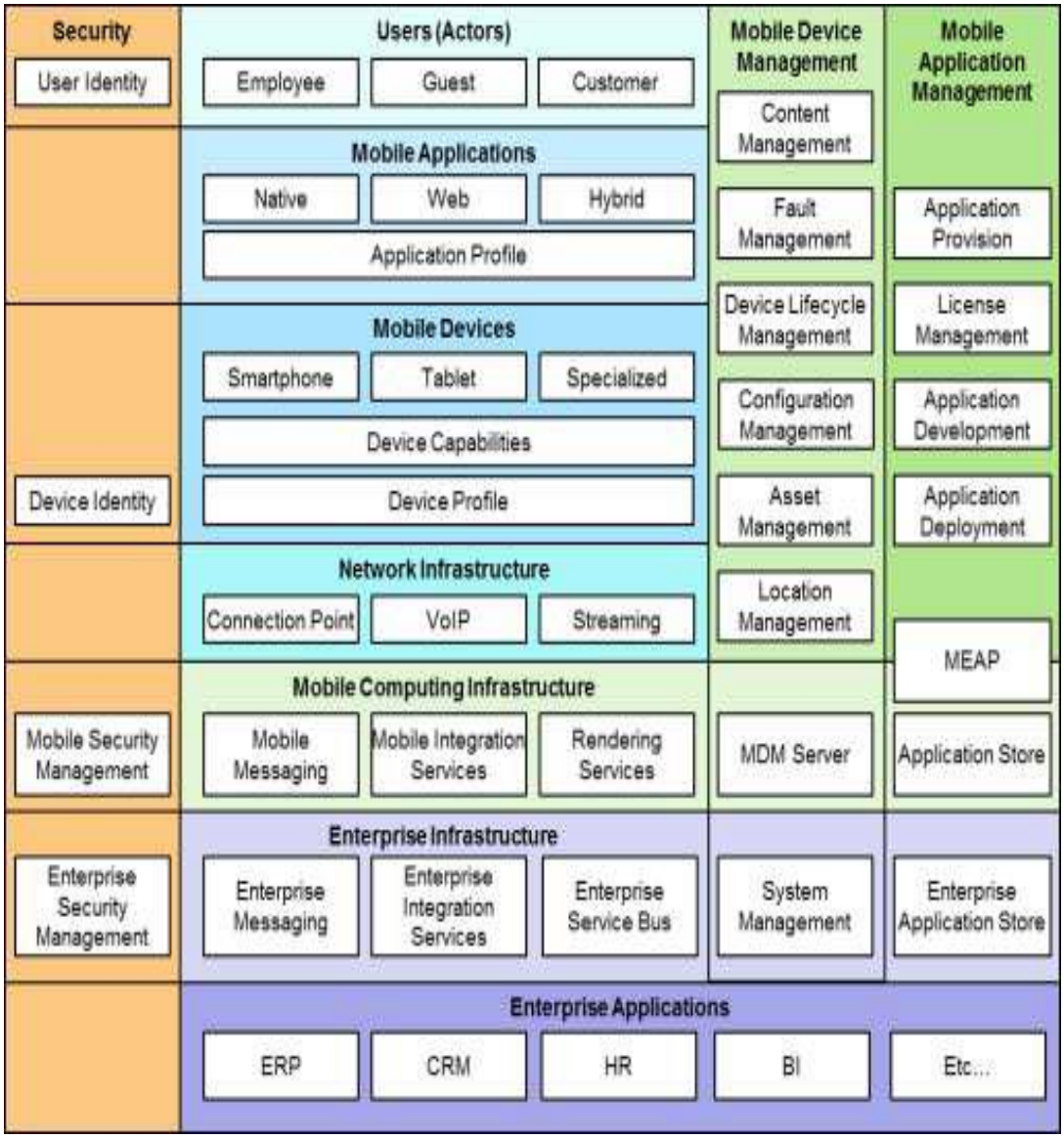
2.3 Review of standards

The ongoing review of current and new standards will be conducted by the ICT Procurement and Technical Standards Working Group. New standards and modifications to existing standards must be endorsed by the ICT Leadership Group.

3. STANDARDS

3.1 Overall architecture

This diagram illustrates the architectural elements necessary to support mobile device solutions, linking entities or users, equipment and infrastructure such as devices, applications, networks and processes such as security, management.


Security
User Identity
Users (Actors)
Employee
Guest
Customer
Mobile Device Management
Mobile Application Management
Content Management
Mobile Applications
Native
Web
Hybrid
Application Profile
Fault Management
Application Provision
Device Lifecycle Management
License Management
Mobile Devices
Smartphone
Tablet
Specialized
Device Capabilities
Configuration Management
Application Development
Device Identity
Device Profile
Asset Management
Application Deployment
Network Infrastructure
Connection Point
VoIP
Streaming
Location Management
MEAP
Mobile Computing Infrastructure
Mobile Security Management
Mobile Messaging
Mobile Integration Services
Rendering Services
MDM Server
Application Store
Enterprise Infrastructure
Enterprise Security Management
Enterprise Messaging
Enterprise Integration Services
Enterprise Service Bus
System Management
Enterprise Application Store
Enterprise Applications
ERP
CRM
HR
BI
Etc...

3.2 Mobile solution lifecycle management

This section describes a five phase life cycle model for agency mobile device solutions, involving everything from policy to operations. The use of a five-phase life cycle model is to help agencies determine at what point in their mobile device solution deployments a recommendation may be relevant. Agencies may follow a project management methodology or life cycle model that does not directly map to the phases in the model presented here, but the types of tasks identified and their sequencing are probably similar. The phases of the life cycle are as follows:

3.2.1 Phase 1 - Initiation

This phase involves the tasks that an agency will perform before it starts to design a mobile device solution. These include identifying the needs for mobile devices, providing an overall vision for how mobile device solutions would support the business requirements of the agency, creating necessary high-level strategy for implementing mobile device solutions, developing a mobile device security policy, specifying business and functional requirements for the solution and then conducting a risk assessment of solutions available or required.

3.2.2 Phase 2 - Development

In this phase, agencies specify the technical characteristics of the mobile device solution and related components. This is equally applicable to as a service offerings to ensure agencies select services that meet their general requirements, including the authentication methods and cryptographic mechanisms used to protect communications and stored data as required based upon the risk assessment performed in the Initiation phase. The types of mobile device clients to be used should also be considered, since they can affect the desired outcomes and/or policies. Care should be taken to ensure that the mobile device security policy can be employed and enforced by all client devices. Solution components are procured at the end of this phase.

Once agencies have established a mobile device security policy, identified mobile device needs, performed a risk assessment across the functionality to be delivered and completed other preparatory activities, the next steps are to determine which types, if applicable, of mobile device management (MDM) and mobile application management (MAM) technologies should be used. There are many considerations for selecting/designing a solution, most of which are generally applicable to any IT technology.

The following section focuses on the technical security considerations that are most important for selecting/designing mobile device management solutions. Major considerations include the following:

- *Application vetting and certification requirements*. This sets security, performance and other requirements that applications must meet, and determines how proof of compliance with requirements should be demonstrated. The security aspects of the mobile device solution design should be documented in the system security plan. Agencies should also consider how incidents involving the mobile device solutions should be handled and document those plans as well.

- *Architecture.* Selecting/designing the architecture includes the selection of mobile device management server and client software, and the placement of the mobile device management server and other centralised elements.

- *Authentication.* Authentication involves selecting device and/or user authentication methods, including determining procedures for issuing and resetting authenticators and for provisioning users and/or client devices with authenticators.

- *Configuration requirements*. This involves setting minimum security standards for mobile devices, such as mandatory host hardening measures and patch levels, and specifying additional security

controls that must be employed on the mobile device, such as a VPN client. Most as a service offerings will allow limited configuration options.

- *Cryptography*. Decisions related to cryptography include selecting the algorithms for encryption and integrity protection of mobile device communications, and setting the key strength for algorithms that support multiple key lengths.

3.2.3 Phase 3 - Implementation

In this phase, solutions are sourced to meet operational and security requirements, including the mobile device security policy documented in the system security plan, installed and tested as a proof-of-concept and/or pilot prior to activation in a production environment. Implementation includes integration with other security controls and technologies, such as security event logging and authentication services.

Aspects of the solution that will be evaluated for each type of mobile device include the following (note some items may not be applicable depending on the outcomes of the risk analysis):

- *Applications.* The applications to be supported by the mobile device solution function properly. All restrictions on installing applications are enforced.

- *Authentication*. Authentication is required and cannot be readily compromised or circumvented. All device, user, and domain authentication policies are enforced.

- *Connectivity.* Users can establish and maintain connections from the mobile device to their agency. Users can connect to all of the agency's resources that they are permitted to and cannot connect to any other agency resources.

- *Default Settings*. Agencies will carefully review the default values for each mobile device setting and alter the settings as necessary to support security requirements developed following the risk assessment. Agencies will also ensure that the mobile device solution does not unexpectedly "fall back" to insecure default settings for interoperability or other reasons. Agencies will fully secure each agency issued mobile device, in accordance with the agency's policies, before allowing a user to access it. Any already-deployed mobile device with an unknown security profile that is an unmanaged device, will be reviewed and appropriate action taken. BYOD will also be subject to a risk assessment before being granted access to agency environments.

- *Logging.* The mobile device solution logs security events in accordance with the agency's policies.

- *Management.* Administrators can configure and manage all components of the solution effectively and securely, in accordance with the agency's policies. The ease of deployment and configuration is particularly important. Another concern is the ability of users to alter device/client software settings, which could weaken mobile device security.

- *Performance*. All components of the solution provide adequate performance during normal and peak usage. It is important to also consider the performance of intermediate devices, such as routers and firewalls.

- *Protection.* Information stored on the mobile device and communications between the mobile device and the agency are protected in accordance with the established requirements.

- *Security of the Implementation*. The mobile device implementation itself may contain vulnerabilities and weaknesses that attackers could exploit. Agencies with higher security

needs may choose to perform extensive vulnerability assessments against the mobile device solution components. It is recommended all components be updated with the latest patches and configured following sound security practices. As a service providers do this as a matter of course. 'Jailbroken' and/or 'rooted' devices, terms commonly associated with iOS/Android devices respectively and also applicable to other operating systems, will be automatically detected to prohibit their use, where detection is feasible. Note: 'jailbroken' and/or 'rooted' are terms that refer to devices that have been tampered with to permit full access to the operating system, allowing the download of additional applications, extensions and themes that are unavailable through official means.

3.2.4 Phase 4 - Operations and maintenance

This phase includes security-related tasks that an agency performs on an ongoing basis or may require device owners to perform on BYOD models once the mobile device solution is operational, including log review and attack detection. As a service providers perform most of these requirements as part of their service offering, however they may only provide information that the agency needs to review and either act on or advise the service provider of changes that are required. Operational processes that are particularly helpful for maintaining mobile device security, and are to be performed regularly, include the following (again as a service providers provide these services):

- *Checking for upgrades and patches* to the mobile device software components, and acquiring, testing, and deploying the updates.

- *Detecting and documenting anomalies* within the mobile device infrastructure. Such anomalies might indicate malicious activity or deviations from policy and procedures. Anomalies should be reported to other systems' administrators as appropriate.

- *Ensuring that each mobile device infrastructure component in use in the agency (mobile device management servers, authentication servers, etc) has its clock synchronised* to a common time source so that its timestamps will match those generated by other systems.

- *Providing training and awareness activities for mobile device users on threats* and recommended security practices. Agencies will also periodically perform assessments to confirm that the agency's mobile device policies, processes, and procedures are being followed properly. Assessment activities may be passive, such as reviewing logs, or active, such as performing vulnerability scans and penetration testing.

- *Reconfiguring access control features* as needed based on factors such as policy changes, technology changes, audit findings and new security needs.

3.2.5 Phase 5 - Disposal

This phase encompasses tasks that occur when a mobile device solution or its components are being retired, including preserving information to meet legal requirements, sanitising media and disposing of equipment properly. Before a mobile device component permanently leaves an agency, the agency will ensure that any sensitive data is removed from the component (e.g. in the case of 'as a service' providers ensure the service agreement includes appropriate requirements, or in the case of BYOD the departing owner attests to meeting the requirements).

The task of scrubbing all sensitive data from storage devices such as hard drives and memory cards is often surprisingly difficult because of all the places where such data resides and the increasing reliance on flash memory instead of magnetic disks.

3.3 Mobility standards

This section describes mobility standards for NSW Government. It provides a set of minimum requirements for all NSW Government agencies regardless of their size and scale. In addition it describes a broader range of requirements to support mobility solutions across the spectrum of NSW Government agencies.

3.3.1 Use Case / Scenarios

'Use cases' for mobile device solutions that are anticipated in agencies are included in the table below. The corresponding requirement sections of this standard are ticked in the columns.

	Configuration mgmt															Security mgmt		Service mgmt			
Use Case / Scenario	Device hardware	Operating system	Network authentication	Business continuity	Password protection	Automatic device lock	Encryption	Device data segregation	Mobile telephony	Two factor authentication	Location services	Device hygiene	Lost and stolen devices	Mobile device disposal	BYOD software licensing	Mobile device management	Mobile application management	BYOD authority	Mobile device application control	Mobile device support	BYOD backup and restore
Notebook/desktop on premise (agency supplied)	✓	✓		✓	✓							✓	✓						✓	✓	
Notebook/desktop working remotely (agency supplied)	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓		✓	✓		✓	✓	
Notebook/desktop on premise (BYOD)	✓	✓		✓	✓		✓	✓		✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Notebook/desktop working remotely (BYOD)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tablet/smartphone (agency supplied)	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓		✓	✓		✓	✓	
Tablet/smartphone (BYOD)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mobile phone (agency supplied)	✓			✓					✓				✓							✓	
Mobile phone (BYOD)	✓			✓					✓				✓							✓	

3.3.2 Minimum requirements

The table below summarises the minimum requirements required to be in place for agencies to support mobility regardless of their size and scale. This table should be read in conjunction with the explanatory text in the rest of the section.

Function	Minimum requirement
Configuration management	
Operating systems	• All devices must use legitimate operation systems
Network authentication	• Minimum network authentication is to be the agency's End User Environment Director Service with a minimum two factor authentication required for external, 3G or internet access
Password protection/ User authentication	• All devices will support password authentication and automatic locking that must be used at all times.
Automatic device lock	• All devices will have the automatic lock enabled.
Device hygiene	• All devices, including BYOD, will have appropriate and up to date 'hygiene' solutions installed.
Lost and stolen devices	• Lost and stolen devices will be reported immediately to the agency's ICT service centre/desk.
Mobile device disposal	• Any agency data on the devices will be removed from all devices at the end of their life within the agency environment.
BYOD software licensing	• Operating systems and applications running on and/or required by BYOD will be the sole responsibility of the device owner.
Security management	
Mobile device management	• Agencies will conduct a risk assessment of the devices and nature of services the mobile devices need to access in order to inform a decision regarding use of an MDM platform.
Service management	
BYOD authority	• Owners of BYODs that are registered and used for BYO agree to surrender limited authority over the device for the sole purpose of protecting government/agency data and access on the device.
Mobile device application control	• Agencies will have the ability to push and/or remove agency supplied applications from devices (including BYOD) to enhance either security or manageability of the device.
Mobile device support	• Devices are supported by their owner/issuer.

3.3.3 Configuration management

Device hardware

Mobility devices can be any of the following:

- Mobile phone
- Smartphone
- Tablet
- Laptop/desktop
- Specialised (ruggedized laptop/tablet for example)

This list will grow as new technology is developed.

Agency provided devices

Agency provided mobility devices will be based on each agency's assessment of the best toolsets to meet business requirements and the supporting infrastructure currently implemented. Devices that are used exclusively in an agency's networked environment (i.e. Office) are not included within the context of these standards. Desktop devices supplied by agencies that are used off-site (e.g. in a home) are considered for the purpose of the mobility standards to be mobile devices as they access the agency network by similar means as other mobile devices.

BYOD considerations

BYOD device capabilities and device profiles need to be matched to business requirements/user scenarios. For example, if the staff member is primarily a consumer of information when mobile, the profile of a tablet or smartphone would be a good match. If the staff member is a "creator" of information, a laptop/desktop profile would be a better match.

As a general rule, any device may be considered for use as a BYOD provided it meets the minimum requirements of the agency. Agencies will advise staff as they allow specific devices to be considered BYOD. Devices that are not currently known to the agency need to be assessed. The burden of proof for meeting agency minimum requirements is the responsibility of the requester. The final decision on whether a device meets requirements will rest with whomever the agency nominates, normally the Chief Information Officer or similar.

Common Considerations

Operating systems

All devices must use legitimate operating systems – 'jail broken' or 'rooted' devices must not be used on agency/government networks.

The agency documented security policy must be enforceable. The agency chosen MDM solution could be used to block these devices.

Network authentication

Minimum network authentication is to be the agency's End User Environment Directory Service (e.g. Active Directory, e-Directory, etc.) with a minimum two factor authentication required for external, 3G or internet access.

Business continuity

When implementing a BYOD policy, agencies retain a degree of responsibility for business continuity in the event of loss or otherwise of an individual employee's device. Responsibility will be limited to ensuring a staff member can be productive while they replace or repair their device. Agencies need to consider the detail of such a policy and how it is implemented based on their specific requirements and service delivery priorities.

Password protection /user authentication

All devices must support password authentication - (numeric / alphanumeric / pattern swipe or similar) and automatic locking of access that must be used at all times.

The table below provides some examples of settings that can be used to support secure password authentication.

	Desktop/notebooks	Smartphone/tablet devices
Setting	Value	Value
Minimum password length	7 characters	4 digits
Maximum password attempts	4 attempts	4 attempts
Forbidden passwords	Popular: e.g. password, department Repetitive: e.g. 0000000, 2222222, Sequential: e.g. 1234567, 4567890	Popular: e.g. password, department Repetitive: e.g. 0000, 2222, Sequential: e.g. 1234, 7890
Password History	Not allowed to use previous x passwords	Not allowed to use previous x passwords
Security time-out	x minutes	x minutes

If a MDM solution is in place for the agency, all devices that are used remotely from an agency site should incorporate automatic retirement of the device from the MDM after maximum password attempts. Once the maximum number of password attempts has been reached without intervention, the device should be automatically retired from the MDM. Remote wipe of all agency data held within a 'container' on the device must be supported via the MDM platform where required, based upon risk analysis.

Automatic device lock

All devices will have the automatic lock enabled to ensure the device locks and requires a password to unlock the device after the defined period of idle time has elapsed.

Encryption

Encryption will be supported and enabled on all devices, including BYOD, where required based upon risk analysis. If the device has a disk drive (solid state or spinning) then it will be encrypted either by operating system or other means. Where possible, all data transmission will also be encrypted.

Device data segregation

Where devices support on-device data segregation, agency/government services will be separated from the remainder of the device. For example 'containers' – most smartphone and tablet devices support 'containerised', 'walled-garden' services. There may be other options which may also be considered subject to agency risk assessments.

Mobile telephony

Depending upon business requirements for flexibility and travel, mobile telephony devices will support quad-band to enable them to use multiple networks on a range of frequencies.

Two factor authentication / virtual private network

Support for both physical and virtual tokens will be provided on mobile devices and be supported by agency MDM solutions.

Location services

Mobile devices with GPS capabilities typically run what are known as location services. These services map a GPS-acquired location to the corresponding businesses or other entities close to that location. Location services are heavily used by social media, navigation, web browsers and other mobile-centric applications. In terms of agency security, mobile devices with location services enabled may be at increased risk of targeted attacks because it is easier for potential attackers to determine where the user and the mobile device are, and to correlate that information with other sources.

This can be mitigated by disabling location services or by prohibiting use of location services for particular applications such as social networking or photo applications. Users may also be trained to turn off location services when in sensitive areas. However, similar issues can occur even if GPS capabilities or location services are disabled. It is increasingly common for websites and applications to determine a person's location based on internet connection, such as a Wi-Fi hotspot or IP address range. Agencies need to consider whether location services are needed or not and implement the most appropriate solution for their requirements.

Device hygiene

All devices including BYOD must have appropriate and up-to-date 'hygiene' solutions installed. Device hygiene includes, but is not limited to, anti-virus, anti-spam, anti-spyware. For agency issued devices, this will be provided by the agency, for BYOD this must be provided by the device owner and will meet agreed minimum agency requirements.

Lost and stolen devices

Lost and stolen devices whether agency owned or BYOD may present a security risk to the agency, both from the device and network perspective. Lost and stolen devices will be reported immediately to the agency's ICT service centre/desk to allow appropriate action to be taken based upon the risk management plan for that agency. For example, agencies may have MDM solutions implemented to allow for agency provided devices to be completely wiped remotely and BYOD to have agency data held within a 'container' on the device wiped. For agency owned devices, a full wipe should be possible upon written request from the device owner and for BYOD it is up to the owner to execute a remote wipe using vendor supplied utilities.

Mobile device disposal

Any agency data on the devices should be removed from all devices at the end of their life within the agency environment. If an MDM solution is in place, all devices need to be deregistered from the MDM. Further, it is encouraged that any personal data should also be removed. For devices that have reached the end of life, consideration will be given to physical destruction, as for any other IT device. For BYOD, if it is intended the device will be passed by sale or gift to another person for future use the device will have some form of secure wipe performed beforehand.

BYOD software licensing

Operating systems and applications running on and/or required by BYOD are the sole responsibility of the device owner. Agency applications may be provided to the device through virtual application delivery such as Citrix or similar.

3.3.4 Security management

Mobile Device Management (MDM)

Agencies must conduct a risk assessment of the devices and nature of services the mobile devices need to access in order to inform a decision regarding use of an MDM platform. Where required, the MDM solution will at all times remain device agnostic to ensure it is able to support the widest

possible range of devices. Agencies are strongly advised to leverage MDM platforms to allow for centralised management of agency data regardless of who owns the device.

MDM software secures, monitors, manages and supports mobile devices deployed in Agencies. All tablets and smartphone devices, whether agency provided or BYOD used to connect to NSW Government will be supported by one of the following:

- Agency sourced MDM platform
- Blackberry Enterprise Server (BES)
- other solutions as they are developed and agreed by government from time to time.

MDM platforms are capable of wiping information from agency and BYOD devices upon their deregistration. Depending upon the combination of MDM platform, device manufacturer / type, operating system and OS version, either a full (all data) or selective wipe (container only) will be possible. The default wipe position for agency devices will be full, for BYOD it will be subject to device combination. Selective will be the default option.

Mobile Application Management (MAM)

MAM software services are responsible for provisioning and controlling access to agency developed and/or commercially available mobile apps used in business settings on both agency supplied and BYOD devices.

MAM solutions provide the ability to control the provisioning, updating and removal of mobile applications via an enterprise app store, monitor application performance and usage, and remotely wipe data from managed applications. Core features of mobile application management systems include:

- App delivery, Enterprise App Store
- App performance monitoring
- Crash log reporting
- App version management
- Push services
- Usage analytics
- App wrapping
- App updating
- User authentication
- User and group access control
- App configuration management
- Reporting and tracking
- Event management

MAM solutions are recommended to support extended use of the mobile devices beyond email/calendar tools and remote access to applications. Examples of extended use include dictating the use of additional applications, such as secure document stores or apps for performing business functions, such as records management. MAM will allow centralised control of the applications being used, simplifying support.

3.3.5 Service management

BYOD Authority

Owners of BYODs that are registered and used for BYO agree to surrender limited authority over the device for the sole purpose of protecting government/agency data and access on the device. The authority will be made either via a signed document that is stored on an appropriate system or by means of an equivalent e-form. This includes permission to wipe the device in the event of loss or disposal. This may include personal data, address books and/or e-mail depending on the data classification of information locally stored, the device and whether a MDM tool is used. The authority is to remain in place from the time the device is registered until it is deregistered.

Mobile device application control

Agencies will have the ability to push and/or remove agency supplied applications from devices, including BYOD, to enhance either security or manageability of the device. Agencies should inform (as appropriate) device holders when threats have been identified. If agency supplied applications are identified as being a threat, the application may be remotely removed via the MDM if one is in place. If applications that are non-compliant to agency policy are discovered on a device, access to the agency network and data is to be removed until such time as the non-compliant application is removed from the device.

Mobile device support

Devices are supported by their owner/issuer. Owners of BYOD have responsibility to support their own device: Agencies will not provide hardware, operating system or application support other than for applications they have provided.

Support	Agency issued	BYOD
Physical provisioning	Agency service desk	Device owner
Replacement of defective/damaged device	Agency service desk	Device owner
Operating system support including licensing	Agency service desk	Device owner
Application support of device including licensing	Agency service desk	Device owner
Agency provided/supported mobile applications	Agency service desk	Agency service desk
Agency provided/supported thin-client applications	Agency service desk	Agency service desk

Device connectivity / access	Agency issued	BYOD
Mobile internet (3G etc)	Agency service desk	Device owner
Home internet / broadband	Device owner	Device owner
VPN client	Agency service desk	Agency service desk
Agency wireless	Agency service desk	Agency service desk

BYOD backup and restore

Some BYOD are capable of backing up and restoring data and configuration settings. The owner of the device is responsible for any backing up and restoring of data and configuration settings of the device. Agencies need to establish rules and/or guidelines for locations they consider acceptable for backing up agency data and agency-related configuration files. Agency data must only be backed up to approved locations either within agency systems or approved cloud service locations/providers, for example, via a blacklist approach.

Telecommunications

To be provided in a separate standard under development.

Appendix 1

Use Case /Scenario Descriptions

Use Case / Scenario	Description
Notebook/desktop on premise (agency supplied)	Traditional approach to providing technology solution in the work environment.
Notebook/desktop on premise (BYOD)	Individually owned device used to access data and agency provided applications. Agency is responsible for ensuring that the device has appropriate safeguards in place to ensure the device(s) doesn't introduce technologies that result in risks to the business.
Notebook/desktop working remotely (agency supplied)	This could include working from home or another location including but not limited to teleworking centres, site-offices, travelling/mobile locations (e.g. trains, planes, hotels). All technology elements are provided by the agency.
Notebook/desktop working remotely (BYOD)	This could include working from home or another location including but not limited to teleworking centres, site-offices, travelling/mobile locations (e.g. trains, planes, hotels). All/most technology elements are provided by the individual.
Tablet/smartphone (agency supplied)	This could include working from home or another location including but not limited to teleworking centres, site-offices, travelling/mobile locations (e.g. trains, planes, hotels). All technology elements are provided by the agency.
Tablet/smartphone (BYOD)	This could include working from home or another location including but not limited to teleworking centres, site-offices, travelling/mobile locations (e.g. trains, planes, hotels). All technology elements are provided by the individual.
Mobile phone (agency supplied)	Agency provided mobile (non-smart) phone. Used to provide roaming telephone and SMS services.
Mobile phone (BYOD)	Individually provided mobile (non-smart) phone. Used to provide roaming telephone and SMS services.

DOCUMENT CONTROL

9.1 Document history

Status: Final

Version: 0.2

Approved by: ICT Leadership Group

Approved on: 3 October 2013

Contact: Shane Richards, ICT Services, Strategic Policy, Office of Finance and Services

Email: standards@services.nsw.gov.au

Telephone: 9372 7445

9.2 Review date

This standard will be reviewed in 12 months. It may be reviewed earlier in response to post-implementation feedback from departments.