Public Record Office Victoria
Standards and Policy

Recordkeeping Policy

Mobile Technologies and Recordkeeping

Issues Paper

Version Number: v1.0

Issue Date: 21/10/2013

Acronyms

The following acronyms are used throughout this document.

AGIMO: Australian Government Information Management Office; part of the Department of Finance and Deregulation, with responsibility to advise the Australian government and its agencies on a wide range of ICT issues.

AIMIA: Australian Interactive Media Industry Association

BYOD: Bring Your Own Device

DSD: Defence Signals Directorate, the information security branch of the Department of Defence. DSD is responsible, among other things, for the creation, maintenance and promulgation of the Information Security Manual, which complements the Protective Security Policy Framework (PSPF).

ICT: Information and Communication Technology.

PSPF: Protective Security Policy Framework.

Table of Contents

Copyright Statement

Disclaimer

General

The State of Victoria gives no warranty that the information in this version is correct or complete, error free or contains no omissions. The State of Victoria shall not be liable for any loss howsoever caused whether due to negligence or otherwise arising from the use of this Issues Paper. This Issues Paper should not constitute, and should not be read as, a legal opinion. Agencies are advised to seek independent legal advice if appropriate.

Records Management Standards Application

The PROV Records Management Standards apply to all records in all formats, media or systems (including business systems). This Issues Paper identifies records management risks that are specific to mobile technology use by government agencies, and identified within this paper as being major issues. Agencies are advised to conduct an independent assessment to determine what other records management requirements apply.

Use of Terminology

For the purposes of this document, the terms ‘record,’ ‘information’ and ‘data’ used throughout should be understood as ‘public record.’

Responding to this Issues Paper

Please respond to those questions or aspects of the issues paper to which you may have views about. In your response please identify both the section of the issues paper and the questions, issues and paragraphs to which you are responding. Additional ideas or comments on matters not addressed in the issues paper are welcomed. Please include them at the end of your response to a particular matter raised in the issues paper.

In responding to this issues paper agencies should be aware that PROV may be legally required to release the content and details of any response. If you have any concerns about information provided in your response, it is suggested that you seek legal advice.

Please email your responses to: Standards@prov.vic.gov.au.

The closing date for responding to the issues paper is: **22 November 2013**.

If you have any questions, pleases contact Alan Kong, Manager, Standards and Policy at alan.kong@prov.vic.gov.au or 03 9348 5720.

Executive Summary

The emergence of the mobile market is fundamentally changing the way government conducts its business and interacts with the public. This trend is by no means confined to Victoria or Australia. Internationally, governments have harnessed this technology to enhance the flexibility and efficiency of their business processes.

The use of mobile technology can improve and streamline government processes and also reduce operational costs. From a recordkeeping perspective, mobile devices allow information to be accessed and managed without being anchored to a set physical location or work station. However, any uptake of new technologies also creates new risks. These risks need to be managed.

This issues paper focuses on the aspects of mobile technology (including but not limited to Bring Your Own Devices (BYOD)) that have a direct bearing on the management of public records. This issues paper recognises the complexity of mobile technology and does not intend to examine policies relating to the technical or financial considerations of its use.

This paper proposes three recommendations to form the substance of a records management-oriented mobile technology policy for Victorian Government:

1. Agencies should assess the impact on the use of mobile technologies based on their existing business practices and needs. Identified risks such as those relating to data integrity and security should be addressed.

2. Agencies should cover any uses of mobile devices in their existing management and policy frameworks.

3. If BYODs are used for work within an agency, that agencies should consider a BYOD strategy aimed at mitigating information management issues associated with BYOD implementation.

This issues paper invites comment from Victorian Government agencies, and all local, national or international interested parties, in both public and private enterprise.

The consultation phase will conclude on **22 November 2013**. The comments received will inform an official policy from PROV regarding the records management component of mobile technology use.

1. Introduction

1.1. Purpose and scope

The purpose of this issues paper is to discuss the information management implications of the move towards using various kinds of mobile technology to perform the work of government.

This paper will consider:

- The context in which mobile technology is being adopted, and the strong benefits to government in moving towards increased mobile technology use
- Existing policy and guidance that has been produced to assist government in mobile roll-out
- The potential risks and key issues facing government information management posed by mobile technology use. Including, as a subset of these issues, the particular challenges posed by Bring Your Own Device (BYOD) strategies in government
- Recommendations for Victorian agencies to help ensure that information management needs are identified and met with the deployment of mobile technology.

Mobile technology, which is defined below, includes both Internet-enabled and Internet-capable devices (such as smart phones, tablets, laptops, handheld gaming devices and digital cameras) and non-Internet portable devices (such as handheld sound recorders, portable storage items, and non-digital photographic equipment).

As this paper is primarily concerned with the records management aspects of mobile technology use, it will not consider:

- The procurement or financial aspects of mobile technology use
- Broader questions of mobile strategy related to scale, reach or systematisation of government mobile device use
- Specific devices, apps or solutions, either as technical products or as repositories of records.

The subject of this paper is intrinsically linked to two other key issues areas in information management: managing the records of social media; and using the cloud for information management purposes. Most Internet-capable mobile devices use both social media and cloud applications, in some cases exclusively.

To provide the full context for this paper it is recommended that you are familiar with the following two PROV documents:

- Social Media Policy
- Cloud Computing Policy.

1.2. Definitions

Apps: Specialised programs downloaded onto mobile devices to deliver one or more specific services. Apps may allow local storage of data on the device, may act as an interface between a mobile device and data stored elsewhere, or may themselves serve as the repository for data (which is then typically stored on the device or in the cloud).

Bring Your Own Device (BYOD): A strategy allowing employees, business partners and other users to utilise a personally selected and purchased client device to execute enterprise applications and access data.[1]

Mobile technology: A generic term used to refer to the communication or recording of data via a variety of portable devices that allow people to create data wherever they are. Many, but not all, mobile devices are also connected via cellular or wireless networks, which allows for the transmission, sharing and accessing of data from remote locations.

Protective Security Policy Framework (PSPF): A framework created and maintained by the Federal Attorney-General's Department to provide a shared and comprehensive model for ensuring the security of government information. The PSPF comprises policies and requirements that apply to all agencies, as well as guidelines, tools, assessment templates and assistance with determining appropriate agency-specific information security requirements.

Syncing: An abbreviation of "synchronisation", this refers to the act of bringing two or more devices into harmony. This can involve transferring data so all devices will have the same files (and the same versions of all files); and making sure calendars, contact lists and apps are identical between devices. Syncing can be done manually, but is often established as an automatic feature, so that whenever a mobile device comes into contact with its paired system – either via the Internet or by being within wireless network proximity – syncing will occur without user intervention.

[1] Derived from the definition provided in the Gartner online glossary at http://www.gartner.com/it-glossary/bring-your-own-device-byod/ (Accessed 21/2/2013)

2. Context

2.1. Public records requirements

Public records safeguard the entitlements of the people of Victoria, ensure the efficient and equitable delivery of services, and protect the legal rights of the State of Victoria. The *Public Records Act 1973* consequently imposes a duty on the head of an agency to ensure that full and accurate records are made and kept of the business of the office. This requirement to manage public records applies equally in a mobile environment.

A public record is defined by the *Public Records Act 1973* as “any record made or received by a public officer in the course of his duties”[2]. It is important to note that “record” shares the definition of “document” provided in the *Evidence Act 2008,* which is “any record of information”[3], whether it be in writing, in visual form, a sound recording, any electronic file, communication or transaction which records information, or any physical object or thing upon which information is recorded.

Essentially this means that any information made or received by a public servant while performing their job is a public record, and needs to be treated and managed as such, regardless of its form, location, or method of access.

The creation, maintenance, management, and disposal of public records are regulated via the Public Records Standards. These documents provide agencies with set parameters and guidance within which records can be effectively managed.[4]

As the Victorian public sector embraces the range of opportunities offered by new technologies, it is prudent to consider how these technologies can enhance records management, and what considerations are relevant when rolling out systems and strategies.

2.2. Technological shift

In line with the global uptake of these technologies, public sector agencies’ use of the cloud, mobile technology, social media and associated technologies is rapidly advancing. This trend is expected to continue and expand, especially with respect to network-capable mobile devices. A recent Australian Interactive Media Industry Association (AIMIA) study into mobile device use in Australia predicts smart phone and tablet use to reach 86% and 70% respectively of the Australian population in the next 5 years[5].

In some cases, these changes are being strategically selected at enterprise or sector level for the cost and effectiveness advantages they offer. Many agencies are choosing cloud-based storage and application delivery services for these reasons.

However, in other cases, change is being driven by individual public officers, who are finding greater efficiencies in the use of these technologies. For

[2] *Public Records Act 1973*, (2) (a)

[3] *Evidence Act 2008*

[4] To view copies of the Public Records Standards please see the PROV website: <http://prov.vic.gov.au/government>

[5] AIMIA, 8TH Annual Australian Mobile Phone Lifestyle Index, September 2012, http://www.aimia.com.au/enews/AMPLI/AMPLI%202012%20Report_FINAL_upd_Oct.pdf accessed 23/3/13

example, the use of BYOD mobile technology is already underway in many areas. Individual public officers at all levels of government are using privately selected and owned mobile devices to both access organisational systems and create work notes and records that fall outside of the office system.

EXAMPLE

The recent Victoria Police Information Security Culture Survey, published in November 2012, revealed that 76% of responding police members use at least one personally-owned [mobile] device in an average week to capture and/or store law enforcement data. Personally-owned smart phones are being used by 45% of members. The reasons cited for doing so were convenience, accessibility and the lack of appropriate equipment provided by the police.

The report states that "the practice of using personal devices for operational policing is largely unmanaged and uncontrolled and poses significant information management and security risks."[6]

QUESTIONS:

Q1: What plans does your agency have for using mobile technology to perform work?

2.3. The benefits of mobile technology

Government business and program delivery can be substantially improved through the use of mobile technology, both to increase its responsiveness to emerging issues and to communicate effectively with the public.

The Australian Government has a stated commitment to improve the accessibility of government to citizens. This is expressed in Victoria through the government's new ICT Strategy[7]. To adapt a client-centric focus, agencies will often utilise social media channels and purpose-built mobile applications by way of sharing and receiving information with the public.

The freedom to perform government work outside the traditional office environment is greatly enhanced by the capacity and reach of mobile technology, enabling more government employees to work from home, from field locations and in less conventional time patterns. Mobile technology allows officers greater flexibility and innovation when conducting their work, increasing response rate and the ability to address emerging issues promptly.

QUESTIONS

Q2: To what extent does your agency currently use, or explicitly permit the use of, mobile technology to create, access and maintain the records of government business?

Q3 To what extent is ad hoc technology use already occurring?

Q4: How do you anticipate this will play out in the coming 5 years?

Q5: Does your agency currently use mobile apps to communicate with the public or deliver services?

Q6: How have the records of this activity been maintained?

[6] Commissioner for Law Enforcement Data Security, *Survey of Victoria Police Information Security Culture – Survey Results*, November 2012, p 8, http://www.cleds.vic.gov.au/content.asp?a=CLEDSBridgingPage&Media_ID=90896, accessed 10/4/13

[7] Victorian Government ICT Strategy, accessed via this link 21/10/2013: http://digital.vic.gov.au/

EXAMPLE

In September 2011 the Department of Health launched a free iPhone and iPad app to help Victorians take control of their health and wellbeing anytime, anywhere by delivering health information to mobile devices.

The app responds to citizen preferences to get health information online and on the go. In 2011, 74 per cent of Australians who used the internet looked for health and medical information and medical apps were also among the most popularly requested apps for development.

The mobile app delivers comprehensive, reliable and easy to understand information – all of which has been quality-assured by medical experts.

Since its launch, the app has been downloaded by over 83 000 people and received widespread consumer and sector acclaim – including being featured by Apple in the best apps of 2011 App Store Rewind Program. The app has a 4.5 star rating (out of 5) and was a winner in the 2012 Australian Mobile Awards.[8]

2.4. Data-centric policy responses: addressing the challenge

2.4.1. International government responses

The opportunities and challenges provided to government information management by new technologies, and mobile technologies in particular, have given rise to a range of policy and strategic responses from public sector agencies.

One such strategic response is the US Government's Federal Mobility Strategy, which was composed as part of the wider Digital Government Strategy announced in May 2012[9].

The US strategy focuses on both the capacity for mobile technology to improve outcomes and deliver efficiencies, and also on the need for this to happen in a secure, process-transparent environment.

[8] Cited in Victorian Government, *2013-14 Government ICT Strategy*, p 11, http://www.vic.gov.au/ictstrategy/wp-content/uploads/2013/02/Victorian-Government-ICT-Strategy-web.pdf, accessed 25/03/13

[9] The Mobility Strategy, which drew in responses from a wide range of stakeholders, had six key objectives:

- Incorporate the power and possibilities of mobility into Federal government efforts
- Build mobile technologies/services for reuse and share common services among agencies and public developers
- Efficiently manage mobile and wireless acquisition, inventory, and expenses
- Create a government-wide foundation to provide mobility services and functionality that are needed in all agencies
- Foster collaboration (among agencies, academia, industry, etc.) to accelerate mobility across government
- Establish governance structure for Federal mobility.

> "New expectations require the Federal Government to be ready to deliver and receive digital information and services anytime, anywhere and on any device. It must do so safely, securely, and with fewer resources".[10] (Digital Government Strategy)

In recent months, a key focus of implementing the Digital Government Strategy has been on creating a broad compliance framework for mobile devices and apps according to a technical capabilities document released by the General Services Administration (GSA)[11]. This move supports the release of the BYOD Toolkit12, a document featuring practical case studies of BYOD implementation and a suite of model policies for agencies to adapt to their own circumstances.

2.4.2. National government responses

The Federal Attorney-General's Office, the Australian Government Information Management Office (AGIMO) and the Defence Signals Directorate (DSD) have focused on providing frameworks within which government manages access to information.

The Protective Security Policy Framework (PSPF)[13] and the Information Security Manual (ISM)[14] work together to provide a set of requirements and actions designed to protect the security and useability of government data. Importantly, the PSPF is device-and-service-agnostic with regard to the security needs of information. Agencies are expected to make individual decisions about how they protect and manage their data, but the structure imposes uniformity and consistency around the determination of what data is to be protected, regardless of its location.

AGIMO has signalled its intention to produce a Mobility Strategy for the Australian public sector, which will canvass the broad issues associated with mobile device use and its potential. DSD has also released a high-level advice to executives considering BYOD strategies[15], and will shortly publicly release its detailed manual *Bring Your Own Device (BYOD) Considerations Manual,* which will follow the same theme as the *Cloud Computing Security Considerations Manual*16 in addressing big-picture issues of information security as well as practical methods to address them.

2.4.3. Victorian policy responses

Within the Victorian Government, the Council of Chief Information Officers has produced a range of policies and advisory documents on various aspects of information management and information security, some with direct relevance to the issues raised by mobile technology[17.]

[10] US CIO Council, *Digital Government: Building a 21st Century Platform to Better Serve the American People*, May 2012,p1, http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf, accessed 30/3/13

[11] https://cio.gov/digital-government-strategy-mobile-device-management/

[12] US CIO Council, *Bring Your Own Device: A Toolkit to Support Federal Agencies Implementing BYOD Programs*, August 2012, https://cio.gov/wp-content/uploads/downloads/2012/09/byod-toolkit.pdf accessed 30/3/13

[13] http://www.protectivesecurity.gov.au/pspf/Documents/PSPF%20document%20map.pdf

[14] http://www.dsd.gov.au/publications/Information_Security_Manual_2012_Principles.pdf?&updatedNov12

[15]DSD, Information Security Advice: BYOD Considerations for Executives, November 2012, http://www.dsd.gov.au/publications/csocprotect/byod_considerations_for_execs.htm
Accessed 1/04/13

[16] DSD, *Cloud Computing Security Considerations*, September 2012, http://www.dsd.gov.au/infosec/cloudsecurity.htm, accessed 27/3/13

[17] Please refer to Appendix 1 for a list of Victorian and interstate government advice

All of these documents affirm the Victorian Government's commitment to compliance with PSPF and the principles of the Information Security Manual (ISM) with regard to keeping government information safe (see list of policy advice and diagram at Appendix One).

The *2013-14 Victorian Government ICT Strategy*[18] identifies mobile technology as a key area of government expansion, offering better, more flexible information service delivery to the public. The strategy is built around the principle that better information systems can mean better government.

> "Government is an information-based enterprise and improving the way we manage and analyse data is central to improving service delivery and policy outcomes."[19]

The Strategy also flags the development of guidance for Victorian agencies on mobile technology implementation. This guidance is scheduled to be released by December 2013.

QUESTIONS:

Q7: Based on the policy and direction currently available in this area, what do you see as the main policy gaps for addressing the information management issues raised by mobile technology use?

Q8: Do you see a value in overarching / sector-wide policy and advice? If so, how prescriptive do you think it should be?

[18] Visit http://digital.vic.gov.au/ for more information

[19] Victorian Government, *2013-14 Government ICT Strategy*, p 7, http://www.vic.gov.au/ictstrategy/wp-content/uploads/2013/02/Victorian-Government-ICT-Strategy-web.pdf, accessed 25/03/13

3. Key records management risks

Mobile technology carries particular information management risks that are either particular to, or greatly magnified in, the mobile context. These risks can be broadly grouped as risks to the:

- **Security** of data. This class of risk covers not just inappropriate access to private or confidential material, but risks to the preservation of data in situations where mobile devices or apps make data loss more probable.
- **Quality** of data. The diffusing of government work across multiple devices, with limited central control over them, creates significant potential for data to be created and maintained in ad hoc ways that do not conform to agency expectations regarding metadata, titling and management.
- **Ownership / control** of data. Data that is generated or managed on mobile devices may be stored in apps or locations that make it difficult for the agency to access or manage the data outside of the app itself, allowing additional avenues for unscrutinised data leakage.

These three broad categories of risk are expanded in the following sections.

3.1. Unauthorised electronic access

Unauthorised electronic access can occur with any networked device, but these risks may be amplified in the case of mobile devices. Mobile devices are often used via public wireless connections, which may allow other users of the same public connection to "see" what is being accessed on the device.

While these risks may appear to be IT-centric, they also have implicit record management implications. The ability of agencies to fulfil their obligations with regard to maintaining public records securely and safeguarding citizens' privacy are affected when protections for data security and integrity are weakened.

EXAMPLE

The US-based Third Annual Benchmark Study on Patient Privacy & Data Security found that 94% of organisations had at least one data breach in the last two years. The average number for each participating organisation was four data breach incidents in the past two years.

The average number of lost or stolen records per breach was 2,769. The types of lost or stolen patient data most often included medical files, billing and insurance records.

81% permit employees and medical staff to use their own mobile devices such as smart phones or tablets to connect to their organisation's networks or enterprise systems. However, 54% of respondents say they are not confident that these personally owned mobile devices are secure.[20]

3.2. System breaches: Malware, viruses and other risks

IT systems that are managed centrally by IT staff can be systematically protected against hacking, viruses, malware attacks and other deliberate and unintended security breaches enabled by exposure to the Internet.

Extending this protection to mobile devices is made difficult for a number of reasons. Mobile devices are diverse in structure while the applications within

[20] Ponemon Institute, *Third Annual Benchmark Study on Patient Privacy & Data Security*, December 2012, http://www2.idexpertscorp.com/ponemon2012/, accessed 1/4/13

these devices are proliferating. The type of structure used and how it is used will influence the level of risk for system breaches to occur. For BYODs, it is often up to the discretion of the user to maintain adequate software upgrades and protection tools for their device.

Lack of good protection practices (such as anti-virus software) on a mobile device can compromise not only data stored locally on that device, but also the agency's main data storage, whether cloud or local server based. Malicious software can proliferate through the system when data is being transferred from a mobile device back to the agency dataset, especially if this transfer is accomplished automatically via syncing.

EXAMPLE

The State University of North Carolina study, the Android Malware Genome Project[21], found that 86% of Android malware uses a technique called repackaging, wherein a hacker downloads a popular application, decompiles it and then adds a malicious payload. The application is then recompiled, and put in the marketplace with a very similar name to the original product.

QUESTIONS

Q9: Does your agency have a BYOD strategy in place? If not, is there an implied or stated prohibition on the use of personally owned devices to access corporate information systems?

Q10: If your organisation uses, or intends to use, a BYOD approach, what hygiene controls (virus protection, updating cycle, patching) do you think it is reasonable to impose on device users?

3.3. Unauthorised physical access

When data is created or stored on a mobile device, the mobility of the device itself poses the risk of security breaches. Devices can be mislaid, inadvertently left behind in public areas, or stolen, more readily than a stable device that remains in the office.

The loss or theft of a mobile device, whether Internet capable or not, poses risks to the security of the data it contains. In the case of the device having been used as the primary creator or storage point for the data, it may also result in lost corporate data.

EXAMPLE

In December 2012, Human Resources and Skills Development Canada revealed the loss of a USB stick containing the personal information and social security numbers of 5,000 Canadians.

"We are currently analysing this incident with the view of preventing a similar occurrence in the future," a representative said.

The Canadian Privacy Commissioner's office is working with HRSDC in an effort to figure out what happened.[22]

[21] Yajin Zhou & Xuxian Jiang, *Android Malware Genome Project*, North Carolina State University, 2012, http://www.malgenomeproject.org/, accessed 1/04/13

[22] The Canadian Press, "Government USB Key With Personal Info Of Thousands Of Canadians Goes Missing", *Huffington Post*, 28/12/2012, http://www.huffingtonpost.ca/2012/12/28/government-personal-info-missing-usb-key-canada_n_2377503.html, accessed 31/03/13

3.4. Blurred distinction between personal and government data

Several risks exist when the line between personal and business information is blurred. These include:

- Mingled datasets, where messages, application data, or other kinds of information contain both personal and business information in a single object. This may be problematic when determining which information should be captured back to the agency's system.
- Personal use of the personal device that breaches information or other corporate policies. Even if these uses are made in private time, they have the potential to involve and compromise government data if they expose the device and its storage to external unauthorised access.

It may be difficult to remove and destroy memory components of mobile communication devices. This is particularly relevant where mobile devices are owned by the employee or are transferred to an external entity for reasons such as repair or replacement.

Another risk is posed to the personal data stored on the device if the agency requires the installation of certain security measures, such as the ability to remotely "kill" the device after a specified number of incorrect password attempts. There may be significant resistance from some employees to install these systems on devices that they own and use for personally significant matters when they understand the risk to their own data.

Personal devices can also be seized in legal discovery if the plaintiff has reason to believe there is relevant work information on them. This is a matter that may not be understood, or appreciated, by employees combining work and personal use in one device.

EXAMPLE

"One morning you wake up, reach for your iPad to check the email but it doesn't turn on. Your iPad is dead. Totally bricked. After a quick family investigation you realize that the little one tried to guess your password to play Angry Birds before you would wake up. Too bad the security policy enforced by the corporate email account triggered your iPad self-destruction to prevent sensitive corporate data from unauthorized access.

Angrier than those famous birds? Wait until you realize that the device itself can be brought back to life and your corporate data restored. But that your pictures, videos and songs are gone. Forever. (Note: the case above is based on a true story, my son's name is Luca.)" [23]

3.5. Version control

Version control of documents can prove challenging for agencies, especially if the agency is not using a shared collaborative workspace with a document check-in / check-out system. Individual workers can develop drafts on their mobile devices and those drafts are not captured within the agency's business system.

Some organisations manage the risk of losing control of versions of documents via automated syncing, whereby devices harmonise their datasets with the central data store either via the cloud (if cloud storage is in use) or when they are in the wireless vicinity of the office network.

[23] Cesare Garlati, "The Dark Side of BYOD: Privacy, personal data loss, and more", *Venture Bea*t, 28 March 2013, http://venturebeat.com/2013/03/28/the-dark-side-of-byod-privacy-personal-data-loss-and-more/ , accessed 1/04/13

While automated syncing can reduce the risk of versions of documents being lost because they are sitting on mobile devices, it is an imperfect system if not accompanied by training and information controls (such as file naming, folder structure or classification scheme). Syncing aims to harmonise folders with the same names and identities on all the linked devices; if files are created outside the specified folders, they are not automatically synced and may be missed.

3.6. Loss of control of data created via apps

Apps, which are one of the main ways in which mobile device users' access and create data, vary greatly in how they manage and store data. Many apps store the data associated with them within the app itself, either locally on the device's hard drive or sometimes in the cloud. While some apps are designed to facilitate data export to other formats, many are not.

This can create a range of records management problems for agencies:

- Data created in apps may not be able to be integrated into the agency's overall information management system, either because it cannot be extracted at all, or because it cannot be rendered into a shared format.
- Data created in apps may, either legally or by default, be considered the property of the app provider. This is not an acceptable position for public records of the state.
- Apps can become unavailable or be withdrawn from the market with little warning, sometimes taking data with them.
- Agencies face the difficulty of data potentially being created in a large number of apps selected by individuals based on their usefulness and functionality, without necessarily considering data retention issues raised by these activities.

4. Recommendations

PROV proposes the following three recommendations regarding the information management implications of mobile technology use in government

- Risk assessment for data
- High-level policy on mobile technology use
- BYOD strategy explicitly considers data management.

4.1. Risk assessment for data

PROV recommends that agencies use the PSPF assessment process (in addition to existing privacy policies, relevant retention and disposal authorities and other agency-approved risk assessment strategies) to determine the risks involve when accessing or using these records on a mobile device.

A great many public records are open to public inspection, and the mission of open government is to facilitate access to as many datasets as possible. However, some public records are not suitable for open access. Maintaining the privacy of individuals and the confidentiality of certain aspects of government business needs to be a core criterion in any decision making about how records are handled and managed.

When agencies are moving towards mobile technology for business delivery, it is prudent to assess:

- What additional risks mobile technology poses to data integrity and security
- How these risks might be mitigated
- What level of risk is acceptance for particular kinds of records, as it is probable that agencies will have records with different levels of security requirements.

4.2. High level policy on mobile technology use

PROV recommends that agencies use mobile technology to develop high level policy and governance to guide their use from an information management perspective. It is advisable that the policy should cover the following:

- How the use of mobile technology when creating, assessing or managing records complies with state and sector wide law, security and information management requirements. This includes relevant PROV Standards, SEC guidelines and policies, PSPF requirements, privacy obligations and any agency-specific or industry-specific guidelines.
- Device requirements; including virus protection, patching protocols and system basics.
- Any boundaries that the agency wishes to place on the nature and number of apps used on the device and the method by which corporate data is accessed.
- Education for staff using mobile devices regarding their responsibilities as public officers to keep full and accurate records of the business of their office, regardless of how it is produced.
- Technical issues where a decision point is required to help manage data security or maintenance, such as whether the organisation will auto sync all files from all devices, whether corporate IT will support all mobile devices.

4.3. BYOD strategy explicitly considers data management.

PROV recommends that agencies that employ or intend to employ a BYOD approach develop a BYOD strategy, policy, and / or procedure that explicitly consider records management needs, including:

- The responsibility of the device owner to maintain the device safely and securely
- Limitations (if any) on apps used to access, create and manage agency data
- Expectations around version control, syncing and device management
- Requirements for remote access to the device by agency IT staff, if needed.

QUESTIONS

Q11: Does your agency currently have, or is it intending to prepare, high level policy and guidance around the use of mobile technology?

Q12: Do you think the proposed recommendations are reasonable? If so, why? If not, in what way do they fall short or go too far?

Q13: Are there any other issues relating to recordkeeping and information management with mobile technology that we have not discussed in this paper?

5. Appendix One: Interstate & Victorian policy advice

5.1. National and Interstate policies

Key materials include:

- Advice from State Records NSW on messaging technologies
- Advice from State Records WA on Sanitizing Digital Media and Devices
- Advice from Tasmanian Archive and Heritage Office on Web 2.0 and social media records
- Advice from Territory Records Office on portable flash memory devices
- Advice from Territory Records Office on social networking and collaboration applications
- Checklist for the Cloud by National Archives of Australia
- Advice from Public Record Office Victoria on Social Media and recordkeeping
- Guidelines from Public Record Office Victoria on Cloud Computing and information management

5.2. Victorian policies

Policies include:

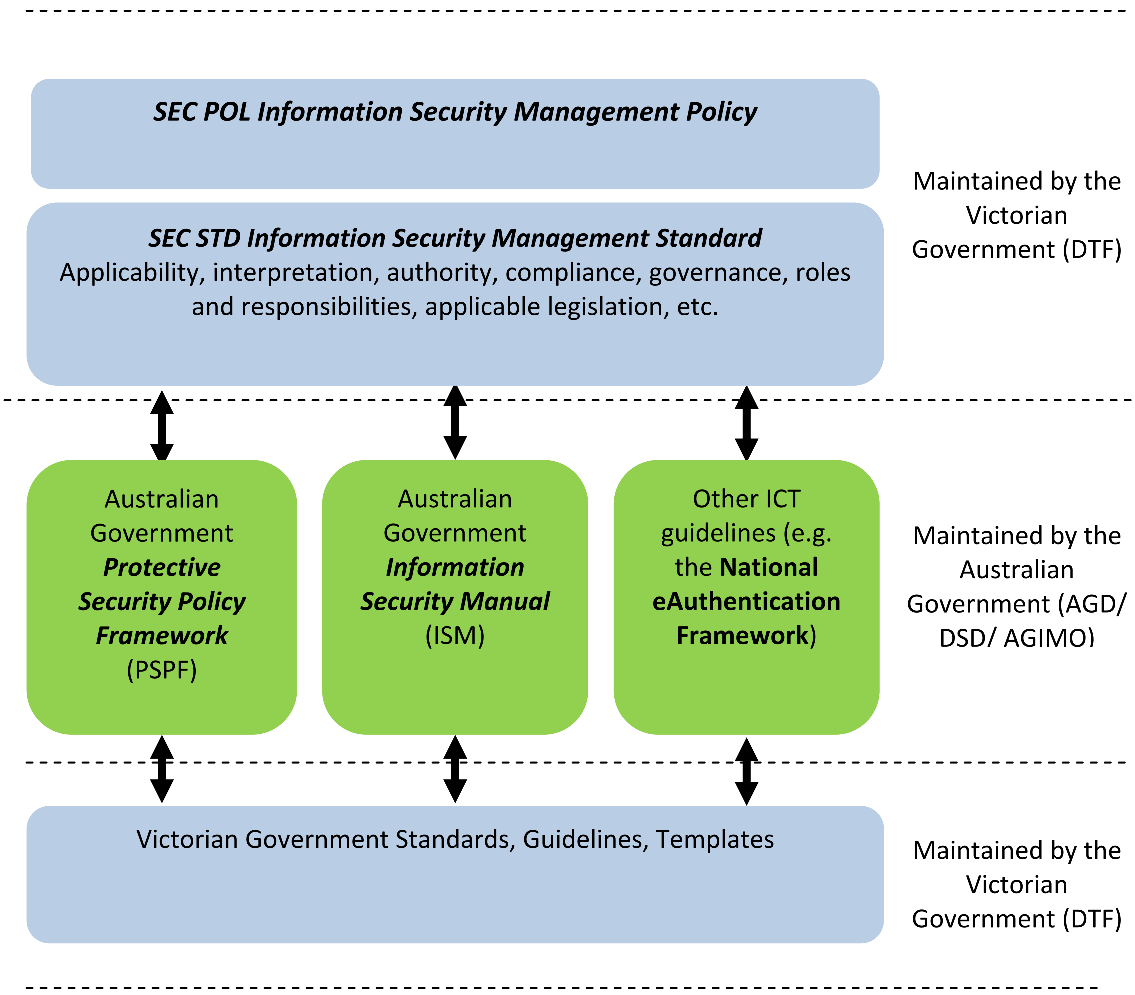
- *SEC POL 01 Information Security Management Policy – 2012*
  This policy establishes an overarching requirement for agencies to develop security management strategies in accordance with national plans.

- *SEC STD 01 Information Security Management Framework – 2012*
  This framework requires agencies to develop an agency-specific information security management framework (ISMF) consisting of an information and communication technologies (ICT) Risk Assessment Report, an Information Security Policy, An ISMF Self-Assessment Compliance Report, and an Incident Response Plan. These documents must consider and build in all the information services used by the agency, including mobile ones.

- *SEC GUIDE 06 Information security cloud computing security considerations guideline - December 2011 v1.0* [24]

[24] All these policies and guidelines can be found at https://www.dtf.vic.gov.au/CA257310001D7FC4/pages/policies-and-standards-information-security, accessed 4/03/13

The following diagram, from the Information Security Management Policy25, shows the relationship of the various documents:


SEC POL Information Security Management Policy
SEC STD Information Security Management Standard
Applicability, interpretation, authority, compliance, governance, roles and responsibilities, applicable legislation, etc.
Maintained by the Victorian Government (DTF)
Australian Government Protective Security Policy Framework (PSPF)
Australian Government Information Security Manual (ISM)
Other ICT guidelines (e.g. the National eAuthentication Framework)
Maintained by the Australian Government (AGD/ DSD/ AGIMO)
Victorian Government Standards, Guidelines, Templates
Maintained by the Victorian Government (DTF)

[25] Victorian Government , SEC POL 01 Information Security Management Policy – 2012, https://www.dtf.vic.gov.au/CA257310001D7FC4/pages/policies-and-standards-information-security, accessed 4/03/13, p 4

6. References

AIMIA, 8TH Annual Australian Mobile Phone Lifestyle Index, September 2012, http://www.aimia.com.au/enews/AMPLI/AMPLI%202012%20Report_FINAL_upd_Oct.pdf accessed 23/3/13

Australian Attorney-General's Department, *Protective Security Policy Framework: Document Map*, 2013, http://www.protectivesecurity.gov.au/pspf/Documents/PSPF%20document%20map.pdf, accessed 30/03/13

Australian Attorney-General's Department, *Protective Security Policy Framework: Information Security Policy*, http://www.protectivesecurity.gov.au/informationsecurity/Pages/default.aspx, accessed 31/03/13

Commissioner for Law Enforcement Data Security, *Survey of Victoria Police Information Security Culture – Survey Results*, November 2012, http://www.cleds.vic.gov.au/content.asp?a=CLEDSBridgingPage&Media_ID=90896, accessed 10/4/13

Defence Signals Directorate, *Cloud Computing Security Considerations*, September 2012, http://www.dsd.gov.au/infosec/cloudsecurity.htm, accessed 27/3/13

Defence Signals Directorate, *Information Security Manual*: *Principles*, September 2012, http://www.dsd.gov.au/publications/Information_Security_Manual_2012_Principles.pdf?&updatedNov12, accessed 31/03/13

Ponemon Institute, *Third Annual Benchmark Study on Patient Privacy & Data Security, December 2012,* http://www2.idexpertscorp.com/ponemon2012/*, accessed 1/4/13*

Public Records Act 1973, http://www.legislation.vic.gov.au/Domino%5CWeb_Notes%5CLDMS%5CPubLawToday.nsf accessed 3/6/13

US Federal Administration, *National Dialogue on the Federal Mobility Strategy: Draft Federal Mobility Strategy Outline*, January 2012, http://mobility-strategy.ideascale.com/a/pages/draft-outline, accessed 30/3/13

US CIO Council, *Digital Government: Building a 21st Century Platform to Better Serve the American People*, May 2012, p1, http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf, accessed 30/3/13

US CIO Council, *Bring Your Own Device: A Toolkit to Support Federal Agencies Implementing BYOD Programs*, August 2012, https://cio.gov/wp-content/uploads/downloads/2012/09/byod-toolkit.pdf accessed 30/3/13

Victorian Government, *2013-14 Government ICT Strategy*, http://digital.vic.gov.au/wp-content/uploads/2013/02/Victorian-Government-ICT-Strategy-web.pdf, accessed 25/03/13

Victorian Government , SEC POL 01 Information Security Management Policy – 2012, https://www.dtf.vic.gov.au/CA257310001D7FC4/pages/policies-and-standards-information-security, accessed 4/03/13

Victorian Government, SEC STD 01 Information Security Management Framework – 2012, https://www.dtf.vic.gov.au/CA257310001D7FC4/pages/policies-and-standards-information-security, accessed 4/03/13

Victorian Government, SEC STD 02 Critical Information Infrastructure Risk Management – 2012, https://www.dtf.vic.gov.au/CA257310001D7FC4/pages/policies-and-standards-information-security, accessed 4/03/13

Victorian Government, SEC GUIDE 06 Information security cloud computing security considerations guideline - December 2011 v1.0,

https://www.dtf.vic.gov.au/CA257310001D7FC4/pages/policies-and-standards-information-security, accessed 4/03/13

Yajin Zhou & Xuxian Jiang, *Android Malware Genome Project*, North Carolina State University, 2012, http://www.malgenomeproject.org/, accessed 1/04/13

END OF DOCUMENT