Public Record Office Victoria
Standards and Policy

Recordkeeping Policy

PUBLIC RECORD OFFICE VICTORIA

Mobile Technologies

Version Number: v1.0

Issue Date: 13/10/2014

PUBLIC RECORD OFFICE VICTORIA

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 Policy. Agencies are advised to seek independent legal advice if appropriate. This Policy should not constitute, and should not be read as, a legal opinion.

Records Management Standards Application

The PROV Records Management Standards apply to all records in all formats, media or systems (including business systems). This policy relates to mobile technology use by government agencies. 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.’

1. Executive Summary

The Protective Security Policy Framework (PSPF) assessment process (in addition to existing privacy policies, relevant retention and disposal authorities and other agency-approved risk assessment strategies) should be used to determine the risks involved when accessing or using corporate records on a mobile device.

High level policy and governance should be developed to guide mobile technology use from an information management perspective.

A Bring Your Own Device (BYOD) strategy, policy, and / or procedure that explicitly consider records management needs should be developed and implemented when employing or intending to employ a BYOD approach regarding mobile devices.

Justine Heazlewood

Director and Keeper of Public Records

2. Introduction

2.1. Purpose

The purpose of this document is to provide principles for making decisions and implementing actions about the use of mobile technologies for recordkeeping across the Victorian government.

2.2. Scope

This policy should be adopted by Victorian government agencies to support best practice recordkeeping regarding creating and keeping full and accurate records.

2.3. Background

Mobile technologies include 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).

2.4. Related Documents[1]

- Mobile Technologies and Recordkeeping Issues Paper
- Social Media Policy
- Recordkeeping Implications of Cloud Computing Policy
- Use Of Back Technology to Archive Policy

[1] Recordkeeping policies may be downloaded from the PROV website at the following link: <http://prov.vic.gov.au/government/standards-and-policy/policies>.

3. Policy Directives

3.1. Risk Assessment for Records

The Protective Security Policy Framework (PSPF)[2] assessment process (in addition to existing privacy policies, relevant retention and disposal authorities and other agency-approved risk assessment strategies) should be used to determine the risks involved when accessing or using corporate records on a mobile device.

Assessments may consider:

- Any additional risks that mobile technology poses to the integrity and security of records
- How these risks might be mitigated
- The level of risk that is acceptable for particular kinds of records, considering the requirements for different levels of security.

3.2. High Level Policy on Mobile Technology Use

High level policy and governance should be developed to guide mobile technology use from an information management perspective.

The policy may cover:

- How the use of mobile technology complies with state and sector wide law, security and information management requirements when creating, accessing or managing records. This includes relevant PROV Standards, SEC guidelines and policies[3], PSPF requirements, privacy obligations and any agency-specific or industry-specific guidelines.
- Device requirements; including virus protection, patching protocols and system basics.
- Any boundaries needed on the nature and number of apps used on the device and the method by which corporate records are 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 they are produced.
- Technical issues where a decision point is required to help manage record security or maintenance, such as whether corporate IT will auto-sync all files from all devices, or provide technical support for all mobile devices.

3.3. BYOD Strategy Explicitly Considers Records Management

A BYOD strategy, policy, and / or procedure that explicitly considers records management needs should be developed and implemented when employing or intending to employ a BYOD approach.

[2] Information about PSPF can be found on the Australian Government, Attorney-General's Department's web page: http://www.protectivesecurity.gov.au/Pages/default.aspx (accessed September 2014).
[3] SEC Guidelines may be downloaded from the Digital Victoria, Information Security web page: http://www.digital.vic.gov.au/resources/information-security/ (accessed September 2014).

Considerations for records management needs may include:

- 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 records
- Expectations around version control, syncing and device management
- Requirements for remote access to the device by agency IT staff, if needed.

4. Appendix

4.1. Acronyms

The following acronyms are used throughout the entirety of 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
ASD	Australian Signals Directorate, the information security branch of the Department of Defence. ASD is responsible, among other things, for the creation, maintenance and promulgation of the Information Security Manual, which complements the Protective Security Policy Framework (PSPF).
BYOD	Bring Your Own Device
ICT	Information and Communication Technology
PSPF	Protective Security Policy Framework

4.2. Definitions

Apps: Specialised programs downloaded onto mobile devices to deliver one or more specific services. Apps may allow local storage of records on the device, may act as an interface between a mobile device and record stored elsewhere, or may themselves serve as the repository for records (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 records.[4]

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

Mobile technology: A generic term used to refer to the communication or capture of records via a variety of portable devices that allow people to create records 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 records 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 records 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.

END OF DOCUMENT