Crime and Corruption Commission
QUEENSLAND

Queensland Government

Corruption Prevention Advisory July 2017

Management of public records

Advice for all employees of a public authority

In this advisory:

This advice highlights the risks and offences of poor records management practices within a public authority. It covers:

- Risk factors
- Corruption offences
- Strategies to prevent corruption
- Further information and resources on records management

Introduction

Openness and transparency in government and public authorities are in the public interest, and key to promoting integrity and accountability in the public sector. One critical aspect is diligence in creating, maintaining and disposing of public records.

Under the *Public Records Act 2002* staff of public authorities are obliged to manage public records responsibly, and the disposal of public records without authorisation from the State Archivist is a criminal offence.

Public authorities:

A public authority is defined under Schedule 2 of the *Public Records Act 2002*, and is deliberately comprehensive to ensure the preservation of all public records by Queensland agencies.

It includes Ministers and Assistant Ministers, Departments, the Governor, organisations created by a minister or through legislation, Commissions of Inquiry, Government Owned Corporations, officers of the court, and local governments.

Note: A public authority can also be referred to as an agency.

Public records:

A public record is any form of recorded information, created or received by, or created on behalf of a public authority which provides evidence of official business activities, and includes copies of or parts of a record.

Note: This is irrespective of the technology or medium used to generate, capture, manage, preserve and access those records.

Risk factors

Poor records management practices can result in:

- Insufficient or inadequate recording of decisions
- Lost records
- Inappropriate destruction of records
- Inappropriate access to records
- Minimal visibility and access to records.

This can expose your public authority to significant corruption risks:

- Lack of proper protocols in relation to recordkeeping means that staff are less likely to understand the importance of creating and capturing records of their business (actions and decisions) and keeping them safe and secure until they can legally destroy them or transfer them to Queensland State Archives. A lack of strictly followed protocols increases the potential and opportunity for corruption around decision-making and actions within public authorities.
- Inability of individuals to provide documentary evidence to account for their actions or decisions while carrying out the duties of a public authority may cause damage to the reputation of both the organisation and staff members. Insufficient or inadequate documentary evidence in an organisation is likely to result in ineffective or poor decision-making.
- Projects or activities may be put at risk when decisions cannot be validated through access to documentary evidence.
- An absence of public records significantly hinders an agency's ability to provide a rationale for its position, especially when undertaking legal processes such as seeking or responding to a court order.
- Inappropriate access to records may be for personal gain or to cause detriment to other people or the organisation.

Corruption offences

Inadequate management of public records can constitute corruption. It can also result in dismissal and/or civil legal action against the individual and organisation involved. Consequences can include:

- Being charged with and convicted of a criminal offence under the *Public Records Act 2002* if an individual unlawfully disposes of (including destroying, damaging, abandoning, transferring, donating, giving away or selling) a public record or any part of a public record. The maximum fine is 165 penalty units (equating to $20,814.75 as at 1 July 2017)[1] for an individual.
- Being charged and convicted of a criminal offence under the *Right to Information Act 2009* if an individual cannot, without reasonable excuse, produce the requested public records. The maximum fine is 100 penalty units for an individual.
- Being charged and convicted of various criminal offences under the *Queensland Criminal Code* including official corruption, computer hacking/misuse, misconduct in relation to public office, abuse of authority and other offences. These offences carry various penalties of imprisonment for up to 10 years.

[1] As at 1 July 2017 1 Penalty Unit = $126.15. The *Penalties and Sentences Act 1992* provides an annual mechanism to revise this figure, and users are advised to review the value of a penalty unit each year.

Strategies to prevent corruption

Internal controls are essential to reduce the risk of inaccurate public records being created or being disposed of improperly. Refer to the CCC Advisory: Information security and handling, and Queensland State Archives publications: Information Standard 40: Recordkeeping (IS40) and Information Standard 31: Retention and disposal of public records (IS31) for further information.

Responsibilities of CEOs and Public Authorities

Under the *Public Records Act 2002* the CEO must ensure that a public authority makes and keeps full and accurate records of its activities and has regard to any relevant policy, standard and guideline made by the State Archivist.

At a minimum public authorities must:

- Document the business, administrative and legal environment in which they operate, and identify the records which need to be created and managed within those contexts.
- Implement a strategic approach to recordkeeping that is endorsed by the agency's Executive Officer.
- Incorporate an assessment of recordkeeping compliance and performance into internal audit and/or business improvement process reviews.
- Act upon any compliance issues identified by reviews or audit processes to improve records management within the agency.
- Formally assign responsibility for recordkeeping activities to those conducting Government business.
- Communicate roles and responsibilities for records management across the organisation.
- Assign responsibility for recordkeeping to an appropriately skilled manager or senior administrative officer.
- Implement an identifiable records management program with documented policies, procedures and business rules.
- Implement recordkeeping systems secure from unauthorised access, damage and misuse.
- Implement processes to ensure records are created, stored and maintained systematically.
- Ensure records document the complete range of business undertaken by a public authority.
- Classify records in accordance with a Business Classification Scheme based on an analysis of the public authority's functions and activities.
- Manage the retention and disposal of records in accordance with IS31: Retention and Disposal of Public Records.
- Capture minimum recordkeeping metadata for all records in accordance with the Queensland Recordkeeping Metadata Standard.
- Ensure that staff members are encouraged to report suspected corruption. Staff play a crucial role in reporting and preventing the illegal alteration, access, release or destruction of public records.

Security measures

The facilities, materials and methods of public records management must support their preservation for as long as they are needed to satisfy the accountability, legal, administrative and financial needs of the government and expectation of the community. This includes ensuring digital records remain useable and accessible for as long as they are required to be retained in order to meet those needs

and expectations. Strategies should be put in place to protect records from unauthorised access, alteration, and accidental or intended damage or destruction. These may include:

- Establish effective and approved procedures for creating, maintaining and disposing of all public records.
- Ensure that staff capture public records on their recordkeeping system e.g. an Electronic Document and Records Management System.
- Ensure that there are adequate electronic security measures such as firewalls, anti-virus software and password access in place to prevent unauthorised access to public records.
- Ensure that all public records are securely stored at all times. Public records should be stored in a way that they are only accessed by those who require this information.
- Implement a business classification scheme[2] for public records with correct security clearances. This provides a reliable structure for ease of titling, locating, sharing and disposal of records.
- Ensure there are adequate procedures in place for employees who may be required to take records into a public area or to their private residence — e.g. requiring public records to be placed in a locked brief case when being taken outside of the office.
- Use a separation agreement that states the obligation of employees to maintain record confidentiality post separation.
- Immediately remove system access and other access tokens when employees, contract staff and third party service providers cease employment with your organisation.

Monitoring and compliance

- Make, maintain and protect all public records in accordance with the *Public Records Act 2002*.
- Ensure employees properly classify (Queensland Government Information Security Classification Framework) and store records in accordance with your organisation's policies and the government's requirement. This will ensure records are properly classified, stored, and disposed of according to the relevant Retention and Disposal schedule authorised by the State Archivist.
- Consider public record security breaches as a breach of your organisation's code of conduct. If such a breach is reasonably suspected to amount to corruption, refer it to the CCC and report lost or damaged records to Queensland State Archives.
- Ensure employees are aware of the consequences (disciplinary and legal action) related to failing to comply with record management policies, procedures and legislation.
- Ensure that regular audits (internal and external) on public records are conducted for the whole of the organisation. This is to ensure that staff are recording their actions and decision-making in performing their role as a public servant. This includes reviewing both digital and hard copy files.
- Ensure there is a good internal reporting system to help identify and prevent the illegal destruction of public records.
- Establish sound risk management strategies and practices, which encompass methods relating to identifying public record management risk areas.
- Record and report all actual and attempted breaches relating to public records.
- Promptly identify, report and rectify any weakness in protocols and procedures to prevent further breaches. Encourage self-assessment by employees in relation to their record management practices.

[2] See The Queensland State Archives Glossary which contains the definitions of terms and phrases used in recordkeeping and information management: http://archives.qld.gov.au/Recordkeeping/help/Pages/Glossary.aspx

- Implement methods of monitoring any breaches of electronic security. Regularly review protection systems to identify any limitations in these systems in combating misconduct.

Disposal

- Disposal of a public record without authorisation from the State Archivist or other legal authority or excuse is illegal under the *Public Records Act 2002*.
- Public authorities should use a retention and disposal schedule approved by the State Archivist, the requirements of which area clearly understood by staff.
- In most circumstances public authorities can implement an approved retention and disposal schedule without further reference to the State Archivist. Public authorities should contact Queensland State Archives before implementing a records disposal program if it has been subject to a *recent machinery of government change* or if the records were created before 1950.
- Ensure that your organisation is compliant with the digitisation disposal requirements set out in the General Retention and Disposal Schedule (September 2016) before implementing any digitisation processes involving the destruction of original paper records.
- Ensure your organisation is aware of and compliant with the Queensland State Archives' requirements when decommissioning business systems.
- Executive Officer (or delegate) approval must be provided prior to the disposal of records. Ensure the disposal is documented, IS31: Retention and disposal of public records provides guidance. Amongst other things, the disposal record must record the date of disposal, how the records were destroyed, and the names of the authorising officer and the person who destroyed them.

Further information and resources

- *Crime and Corruption Act 2001*
- *Electronic Transactions Act 2001*
- *Local Government Act 2009*
- *Public Records Act 2002*
- *Right to Information Act 2009*
- Australian and International Standard 15489
- Code of Ethical Standards, Legislative Assembly of Queensland 2004
- Crime and Corruption Commission: Advisory: Information security and handling
- Queensland Government Information Security Classification Framework
- Queensland Government, Information Standard 31: Retention and disposal of public records (IS31)
- Queensland Government, Information Standard 40: Recordkeeping (IS40)
- Queensland Ombudsman, The good decision making guide
- Queensland State Archives website
- Right to Information and Privacy Unit, Department of Justice and Attorney-General

Contact us

Please contact the Crime and Corruption Commission (Queensland) if you would like further detailed guidance and information on any aspect of this advisory.

Please contact Queensland State Archives if you would like further detailed guidance and information on any aspect of government recordkeeping.

Crime and Corruption Commission

Phone: 07 3360 6060
(Toll-free outside Brisbane: 1800 061 611)
Email: mailbox@ ccc.qld.gov.au

Web: www.ccc.qld.gov.au

Queensland State Archives

Phone: 07 3037 6630
Email: rkqueries@archives.qld.gov.au

Web: www.archives.qld.gov.au