Crime and Corruption Commission
QUEENSLAND

Corruption Prevention Advisory September 2016

Information security and handling

In this advisory:

- Major corruption risks
- Strategies to prevent corruption
- Further information and resources

Introduction

Open and transparent government is in the public interest and is key to promoting integrity and accountability in the public sector. According to the *Right to Information Act 2009*, information in the government's possession or under the government's control is a public resource and openness in government increases the participation of members of the community in democratic processes leading to better informed decision-making. This means the public must have the right of reasonable access to information in the government's possession or under its control unless, on balance, it is contrary to the public interest to provide that information.

In this context, 'information' generally includes physical and electronic forms of documents, files, letters, emails, recordings, images, the contents of databases or spreadsheets, and the copyright and intellectual property contained in documents, plans or other media.

The *Information Privacy Act 2009*, the *Public Sector Ethics Act 1994* (s. 9(c)) and the *Code of Conduct for the Queensland Public Service* (s. 4.4) also require that information be managed responsibly and in the public interest.

The *Right to Information Act 2009* (ss. 20–21) requires public sector agencies to make policy documents publicly available and to develop a 'publication scheme' by which it will make other information available to the public.

However, it is also in the best interests of the community that some types of information (e.g. personal or medical details and some types of commercially sensitive information) be kept confidential. Therefore, some agencies and some types of information are exempted from these requirements. All agencies require appropriate security and handling protocols for particular information which, because of its nature, must remain confidential for a specified period.

Major corruption risks

The misuse or 'leaking' of confidential government information can constitute corruption and may also be a criminal offence. Reckless or negligent conduct which results in the release of confidential information may also warrant disciplinary action against the responsible employee. Consequences may extend to dismissal, criminal prosecution or civil legal action against the individual and organisation involved.

Access to confidential information by an employee which is not for an official purpose may also constitute corruption and be a criminal offence. Employees must only access confidential information at their work for official purposes.

High risk information

The increasing use of electronic systems to collect, transfer and store information, and their vulnerability to internal misuse or external attack is a significant risk. Without adequate safeguards and monitoring, information can be moved very quickly and in enormous quantities. High-risk information includes:

- information classified by policy or legislation as sensitive, confidential or protected
- identity and other personal or financial information (including commercial-in-confidence material) privileged, proprietary or business information
- Cabinet-in-confidence material
- information which may cause harm, or could give an unfair advantage if lost, damaged or released without authorisation.

Strategies to prevent corruption

Every agency should have clear guidelines and policies about the use, handling and storage of electronic and hard-copy information, and the authorisations and processes required for its release.

These policies and procedures should:

- be linked (perhaps through your Code of Conduct) to your disciplinary policy and clearly identify the risks
- specify the penalties for improper use or disclosure of agency information
- provide comprehensive audit trails that make it easier to investigate breaches of information security, and help determine whether the misuse was inadvertent or deliberate.

There is also useful information and guidance on information security on the website of the Queensland Government Chief Information Office, including the Queensland Government's *Information Standard 18, Information security* which provides a useful framework for implementing information controls and protocols.

Confidential information: unauthorised access, disclosure and the risks of corruption in the Queensland public sector (CCC, May 2016[1]) outlines the findings of the CCC's audit into how agencies handle misuse of confidential information and contains examples of inappropriate access or use and risks of improperly using confidential information.

1 Crime and Corruption Commission webpage, Information for the public sector, *Confidential information: unauthorised access, disclosure and the risks of corruption in the Queensland public sector*: http://www.ccc.qld.gov.au/corruption/information-for-the-public-sector/confidential-information

Key areas to consider

- Classification of information
- Electronic security
- Physical access to and handling of information
- Mail security
- Disposal of confidential information
- Personnel

Classification of information

- Ensure that all agency information conforms with the *Queensland Government Information Security Classification Framework*.
- Establish guidelines to ensure that information is not over-classified or unduly restricted.
- When collecting personal information, ensure that it is necessary for, and directly related to, your organisation's legitimate functions or activities. Always adhere to state and federal guidelines regarding collection, storage, handling, distribution, protection and disposal of personal information.
- Clearly label files with their level of classification, and colour-code if necessary. Use appropriate headings such as 'not for public release'.
- Mark information that doesn't require a security classification as 'unclassified' to distinguish it from classified information.
- Ensure that all users of classified information observe procedural requirements for its use, storage, transmission and disposal.
- Observe a 'clear desk policy' for classified information as part of an effective lock-up procedure.
- Ensure that staff are aware that they do not 'own' work (such as reports, papers, spreadsheets, artwork or other special purpose documents) that they have created in the course of their employment. Intellectual property rights and copyright on those works are vested in the Crown, and they cannot be used externally without permission from the agency.
- Ensure employees are aware that staff found to have committed an information security breach may be liable to disciplinary and other action, including prosecution. If such a breach raises a reasonable suspicion that corruption has occurred, it must be referred to the CCC.
- Record all actual and attempted security breaches, and take steps to rectify any weakness in procedures to prevent further breaches.
- Periodically review the information flow within your organisation, and the status of information and its level of security.
- Establish a governance framework for the authorised release or reclassification of information.
- Make material that no longer needs to be protected accessible to the public easily and quickly, as required by the *Right to Information Act 2009*.

Electronic security

- Ensure that your organisation's security measures respond to changes in technology.
- Include firewalls and anti-virus software in network security measures to prevent unauthorised external access, and monitor firewall logs.
- Properly investigate all successful intrusions, particularly 'denial of service' attacks.

- Limit access to automated information systems to appropriate employees and work requirements, and establish clear access and audit trails. Ensure all users in the system have custom made rather than standard access profiles.
- Conduct system audits to monitor access and detect attempts at unauthorised access. Take prompt remedial action against any security breaches.
- Ensure computers are logged off or locked (e.g. with password-protected screen savers) when not in use. Properly maintain password security systems and/or other authentication procedures.
- Clearly communicate and enforce the importance of keeping passwords or PINs secure, and changing them regularly.
- Ensure your systems prohibit downloading non-approved software via disc, USB or the internet, and regularly scan your systems to ensure this has not occurred. This will assist in preventing 'key-stroke' logging software, 'trojans' and malware from entering your systems.
- Block emails with attachments containing executable programs to prevent backdoor network access to confidential information.
- Consider flagging protected or confidential documents so that they cannot be emailed outwards without an authorised override.
- Encrypt confidential electronic messages and attachments ensuring that the password to decrypt the message or attachment is not sent with the same communication.
- Advances in technology have provided business machines such as scanners and photocopies which will image and send documents digitally. If any of your business machines have this capacity ensure that if images are captured and cached, that the cache is cleared prior to the disposal of the machine from your agency.
- Analyse internet and email usage patterns and report suspicious patterns to management.
- Develop and maintain controls over the passage of information or software through organisational websites or internet portals (both inward and outward).
- Prohibit using or storing confidential or proprietary organisational information on home computing equipment. Develop a policy and guidelines on laptop security and what data can and cannot be kept on laptops.
- Regularly transfer all data on laptops to the network server, leaving them empty of non-essential material.
- Include disaster response procedures and information recovery techniques in your organisation's business continuity plan.
- Ensure those responsible for implementing disaster response procedures and recovering information remain up to date in their skills and the software and system platforms used by your organisation.

Physical access to and handling of information

- Adequately protect buildings according to the nature of your organisation's activities.
- Store confidential information securely at all times. Make, maintain and protect all confidential materials in accordance with the requirements of the *Public Records Act 2002*.
- Do not leave confidential information on unattended desks or in printers, photocopiers, fax machines or on whiteboards.
- Develop controls and authorisation processes for the copying of confidential materials.
- Lock individual offices when they are vacant.
- Conduct periodic after-hours checks where appropriate.

- Have an employee other than those responsible for securing the material conduct regular checks of confidential materials to ensure that they are properly handled and stored.

Mail security

- Develop and implement clear policies and procedures for handling incoming and outgoing mail with privacy or confidential markings.
- Clearly identify the proper recipient on all outgoing mail.
- Clearly mark the classification of 'confidential' mail, and ensure that it is adequately sealed. Use extra security precautions where required. These may include:
    - the use of two well sealed envelopes
    - delivery by safe hand (a system whereby a document is never out of the formal custody of a 'trusted person', and its movement from trusted person to trusted person is recorded. A 'trusted person' may be a reliable employee or a member of a law enforcement agency who is personally responsible for the safe keeping of the document).
    - use of receipts for classified material.
- Make mail with privacy or confidential markings available only to those who have a genuine claim to the information, and develop handling procedures for when an office is unattended and/or the addressee is unavailable.

Disposal of confidential information

- Do not dispose of any public record without authorisation or, where applicable, without careful consideration of the statutory requirements of:
    - *Libraries Act 1988* (Qld)
    - *Public Records Act 2002* (Qld)
    - *Protective Security Policy Framework* (Cwth)
    - Queensland State Archives: *General Retention and Disposal Schedule for Administrative Records*
- Ensure that your organisation has an approved retention and disposal schedule, and clearly communicate its requirements to all staff. There are General Retention and Disposal Schedules for a range of record types and also for government, industry, or activity segments available on the Queensland State Archives website.
- Shred confidential information when it is discarded. If shredders are not readily available to all staff, ensure proper management of material awaiting or en route to shredding.
- Establish effective procedures for maintaining, repairing and disposing of electronic equipment to ensure that confidential material cannot be accessed.

Personnel

- Ensure that staff are aware of and adequately trained in your organisation's policies, practices, standards and guidelines relating to information security, privacy legislation, and the ownership and appropriate use of intellectual property, during induction and at regular periods thereafter.
- Establish robust staff selection and screening processes.
- Consider using confidentiality notifications or implementing "click to acknowledge" confidentiality notices when employees log–on to your organisation's system, especially to sensitive sites or databases.
- Inform employees that the agency owns its internet and email systems, and therefore traffic on them is not private and may be monitored.

- Periodically review employees' knowledge of security procedures.
- Clearly communicate any changes in information security procedures to all employees.
- Ensure that senior management demonstrate their commitment to information management and protection by observing document classification requirements and security controls such as the 'clear desk' policy.
- Require agency employees and those employed in ministerial offices (advisors and ministerial officers) to sign a confidentiality agreement, as appropriate.
- Ensure that employees can distinguish between their individual generic skills and knowledge, and specific or restricted knowledge acquired during their employment with the agency, and that they can apply the appropriate policy requirements as appropriate.
- Ensure that confidential information is shared only on a 'need to know' basis.
- Discourage staff from discussing confidential information in any areas where it can be overheard (e.g. lifts, cafés, hallways).
- Require employees with access to confidential information to declare any personal and/or pecuniary interests that are likely, or could be perceived, to conflict with their official duties.
- Hold all levels of management accountable for the security of all information under their control. Educate employees on security and safe travel with laptops.
- Remind departing employees of their ongoing confidentiality obligations and of any restrictions imposed on them by contract or legislation. e.g. s. 70 of the *Integrity Act 2009* (Qld); s. 200 of the *Local Government Act 2009* (Qld); Public Service Commission Directive 15/14 Employment Separation Procedures.
- Immediately remove system and building access when employees leave your organisation.

Further information and resources

- *Queensland Government Information Security Classification Framework*
- Queensland Government *Information Standard 18, Information security*
- Queensland Public Service Commission: Directive 15/14 Employment Separation Procedures
- Queensland State Archives: *Retention and Disposal Schedules*
- Queensland State Archives: *General Retention and Disposal Schedule for Administrative Records*
- Queensland State Archives: *Managing public records when decommissioning business systems*
- Queensland State Archives: *Digital continuity* publications
- *Information Privacy Act 2009* (Qld)
- *Integrity Act 2009* (Qld)
- *Libraries Act 1988* (Qld)
- *Local Government Act 2009* (Qld)
- *Right to Information Act 2009* (Qld)
- *Public Records Act 2002* (Qld)
- *Public Sector Ethics Act 1994* (Qld)
- *Australian Government Protective Security Policy Framework*

Crime and Corruption Commission
QUEENSLAND

Please contact us if you would like further detailed guidance and information on any aspect of this advisory.

Crime and Corruption Commission

Level 2,
North Tower Green Square
515 St Pauls Terrace,
Fortitude Valley QLD 4006

GPO Box 3123, Brisbane QLD 4001

Phone: 07 3360 6060
(Toll-free outside Brisbane: 1800 061 611)
Fax: 07 3360 6333
Email: mailbox@ ccc.qld.gov.au
www.ccc.qld.gov.au