CORRUPTION PREVENTION ADVISORY

Misuse of confidential information

The aim of this advisory is to assist managers and agencies to address the corrupt behaviours associated with misuse of confidential information. The advisory will describe the drivers and consequences of misuse of confidential information, identify vulnerable or susceptible information, and propose strategies to frustrate attempts to misuse information.

Introduction

Improper access to and disclosure of confidential information by public sector employees is a serious concern for agencies and members of the public who are required to provide their personal information to agencies in return for services.

Unauthorised access to, and disclosure or misuse of, confidential information can have serious consequences. For the people whose information is accessed or disclosed to third parties without their knowledge or consent, such breaches were found to have had ongoing and long-lasting effects including stress, feelings of vulnerability, financial loss, and frustration with the difficulty of obtaining redress or adequate compensation. Additionally, agencies may incur serious reputational damage or loss of public confidence in their operations and be exposed to liability for failing to protect confidential information from misuse.

Agencies have identified that some of the main drivers of this behaviour were personal interest (curiosity), the desire to obtain a material benefit, relationships that could make some employees more susceptible to misusing confidential information, and an individual's personal circumstances.

Misuse of information can be corruption

Employees must only access confidential information at their work for official purposes.

The following conduct by employees may amount to corrupt conduct or a criminal offence:

- Accessing confidential information without authority
- Accessing confidential information without an official purpose
- Improper disclosure of confidential information
- Misuse of confidential information.

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.

Crime and Corruption Commission
QUEENSLAND

February 2022

High-risk information

High-risk information is information that, because of its content, is often a target for improper access and/or misuse. This might be because the information could give a person a commercial or other financial advantage, or it contains sensitive personal information that members of the public have a right to expect will remain confidential. Examples include:

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

When selecting strategies to prevent misuse of information, the degree of control and effort applied should be proportionate to the value of the information.

Strategies to prevent corruption

There are a number of key areas that are instrumental in preventing misuse of confidential information through unauthorised access to, or disclosure of, confidential information. All areas operate together to create a culture that reinforces the value of protecting confidential information from misuse and obstruct intentional misuse through organisational practices relating to confidential information. Those areas are:

- staff awareness of responsibilities and risks
- policies and procedures
- classification of information
- electronic security
- physical access to and handling of information
- disposal of confidential information.

Staff awareness of responsibilities and risks

- Agencies must make all staff aware of their obligations to correctly handle, store, access and release confidential information, and the penalties for failing to do so.
- As part of any recruitment or vetting process, ensure that screening of potential employees (including contractors) includes enquiries about their disciplinary history to identify anyone who has misused, or may be tempted to misuse, confidential information.
- Ensure that staff are aware of and adequately trained in, during induction and at regular periods thereafter, your organisation’s policies, practices, standards and guidelines relating to information security, privacy legislation, and the ownership and appropriate use of intellectual property (see “Policies and procedures” below).
- Depending on the nature of your agency, require employees (e.g. including those employed in ministerial offices) to sign a confidentiality agreement, as appropriate.
- 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, and put in place appropriate controls.

- 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.
- 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).
- Periodically review employees’ knowledge of security procedures.
- Inform employees that the agency owns its internet and email systems, and therefore traffic on them is not private and may be monitored.
- 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 use such knowledge appropriately.
- Remind departing employees of their ongoing confidentiality obligations and of any restrictions imposed on them by contract or legislation, e.g. section 70 of the *Integrity Act 2009* (Qld), section 200 of the *Local Government Act 2009* (Qld), and the Public Service Commission: *Directive 15/14 Employment Separation Procedures*
- Immediately remove system and building access when employees leave your organisation.
- Remind current staff that they are prohibited from supplying confidential agency information to former colleagues.

Policies and procedures

To guide the conduct of its employees, 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 access, use or disclosure of agency information, and
- 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 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.

Classification of information

- Ensure that all agency information conforms with the Queensland Government *Information Security Classification Framework*.
- 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”.

- Ensure that all users of classified information observe procedural requirements for its use, storage, transmission and disposal.
- 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.

Electronic security

Electronic systems that collect, transfer and store information without proper controls are vulnerable to misuse because information can be accessed and moved quickly and in large quantities. To address this, agencies should:

- 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.
- 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.
- 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.
- Analyse internet and email usage patterns and report suspicious patterns to management.
- Ensure that all business machines (such as scanners and photocopies used to capture and send documents digitally) have their memory caches cleared prior to disposal by your agency.

Physical access to and handling of information

Agencies must ensure that they store confidential information securely at all times. To prevent deliberate or opportunistic access to confidential information, agencies should:

- Make, maintain and protect all confidential materials in accordance with the requirements of the *Public Records Act 2002* (Qld).
- Ensure appropriate access restrictions are in place with respect to areas storing physical records.

- Ensure incoming and outgoing mail is appropriately marked as private or confidential and handled with appropriate custody controls (e.g. ensuring that it is appropriately sealed, hand-delivered and requires receipts).
- Ensure that staff know not to leave confidential information on unattended desks or in printers, photocopiers, fax machines or on whiteboards.
- Institute or maintain a “clear desk policy” for classified information as part of an effective lock-up procedure.
- 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.

Disposal of confidential information

- No agency should dispose of any public record without authorisation or, where applicable, without careful consideration of the statutory requirements set out in the *Libraries Act 1988* (Qld), the *Public Records Act 2002* (Qld), the Queensland State Archives’ *General Retention and Disposal Schedule for Administrative Records* and the *Australian Government Protective Security Policy Framework.*
- 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.

Further information and resources

- CCC (2020): *Operation Impala - A report on misuse of confidential information in the Queensland public sector*
- Queensland State Archives:
  - *Retention and Disposal Schedules*
  - *Managing public records when decommissioning business systems*
  - *Digital Continuity Publications*
- *Information Privacy Act 2009* (Qld)
- *Right to Information Act 2009* (Qld)
- *Public Sector Ethics Act 1994* (Qld)

Crime and Corruption Commission
QUEENSLAND

Contact details

Crime and Corruption Commission
GPO Box 3123, Brisbane QLD 4001

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

07 3360 6060 or
Toll-free 1800 061 611
(in Queensland outside Brisbane)

07 3360 6333

More information

www.ccc.qld.gov.au

mailbox@ccc.qld.gov.au

@CCC_QLD

CrimeandCorruptionCommission

CCC email updates
www.ccc.qld.gov.au/subscribe

Attribution: Content from this publication should be attributed as: *Crime and Corruption Commission: Corruption Prevention Advisory: Misuse of confidential information.*

Disclaimer of Liability: While every effort is made to ensure that accurate information is disseminated through this medium, the Crime and Corruption Commission makes no representation about the content and suitability of this information for any purpose. The information provided is only intended to increase awareness and provide general information on the topic. It does not constitute legal advice. The Crime and Corruption Commission does not accept responsibility for any actions undertaken based on the information contained herein.

Note: This publication is accessible through the CCC website: www.ccc.qld.gov.au