Crime and Corruption Commission
QUEENSLAND

November 2016

How to respond to a confidential information incident in your agency

A six-step guide for managers and supervisors

Queensland's public sector agencies handle a range of sensitive and confidential information. Under Queensland legislation, inappropriately accessing or disclosing such information can be either a criminal offence or a serious disciplinary matter.

This document is a practical guide to help public sector managers and supervisors respond effectively to any confidential information incident in their agency. It provides the necessary legal framework, key steps and supporting resources.

Remember, responding to an incident is more than just potential disciplinary action against an individual and a deterrent to others. It can also be an important learning opportunity for your agency as well as helping to protect the public interest and maintain public confidence.

Offences relating to confidential information

These offences involve the unauthorised access, use or disclosure of official or personal information entrusted to a public sector agency for the purpose of carrying out its functions.

Confidential information is misused when a public sector employee accesses information held by the agency — not to perform their normal lawful duties — but rather for **a private use and benefit**, either for themselves or another person.

This is unlawful, and it can be also a criminal offence, as spelled out in the Criminal Code, the *Police Service Administration Act 1990*, the *Local Government Act 2009,* the *Information Privacy Act 2009* and the *Public Interest Disclosure Act 2010*.

Examples of criminal offences (and corrupt conduct) relating to confidential information

- A health officer accessed confidential information about the health of a family member and subsequently disclosed it to another family member.
- An officer accessed a police database to check the personal details of individuals he had contacted via an internet dating site.
- An officer sourced criminal histories from a police database and supplied the information to a friend who was a private investigator.

1 Take action to contain the incident

Confidential information incidents need to be contained quickly to prevent escalation or cause further impact to individuals or the agency. Obviously, you will decide what action to take on a case-by-case basis — depending on how serious the allegation is and whether the subject officer works in a high-risk environment. For example, consider:

- Blocking or restricting the unauthorised access or disclosure of confidential information
- Monitoring user access to the information system or storage
- Reporting the incident to your Information Security area.

Resources

- For departments: Queensland Government Chief Information Office's Information Standard: Information security — IS18
- For statutory bodies: IS18 applies to statutory bodies as defined by the *Financial and Performance Standard 2009*

2 Make preliminary inquiries

Gather information, documents or reports from various sources associated with the incident. This information will be essential to your decision making and to achieving optimum outcomes — for the complainant, the subject officer and the agency. For example, consider:

- **The incident.** What type of information was accessed or disclosed, including its intrinsic value? How was it used?
- **Your agency's controls.** What controls are currently in place for your ICT and records management systems (e.g. security, access, authorisation, system passwords and warnings, etc.)?
- **The subject officer.** Do they have a history of allegations? If so, are they about control of information?
- **Key issues.** What information or evidence is needed to successfully resolve the allegation?

Potential evidentiary sources

- Further inquiries of the person making the allegation
- Policies and procedures relating to accessing, using, protecting and disclosing information
- Internal controls in the area associated with the incident
- System access logs, timesheets, rosters, swipe card access logs, duties of the subject officer
- Personnel record of the subject officer
- CCTV footage, email and phone records

3 Reassess the risks of the incident

Taking into account the preliminary inquiries you have made, further assess the risks of the incident in the existing climate to mitigate its potential impacts on an individual or your agency:

- Are your agency's information systems controls adequate?

Evidentiary sources

- Your agency's risk management framework

4 Decide how to deal with the complaint and manage the risks

A decision to take no action, take managerial action, or investigate a complaint will depend on factors such as:

- Is the allegation frivolous, vexatious or not made in good faith?
- How serious is it (consider high-consequence impacts, including on public confidence)?
- Did it occur in a high-risk environment (e.g. with very sensitive or valuable information)?
- Is there opportunity to identify and rectify systemic problems, policy and procedural deficiencies, and control deficiencies?
- Would an investigation be an unjustifiable use of resources?
- What was the CCC's assessment of the matter, if a notification of corrupt conduct was made?

You also need an appropriate strategy to deal with the conduct and address identified deficiencies — for example, develop a management action strategy or an investigation plan to cover:

- risks arising during the investigation to be identified, assessed and mitigated
- actions to ensure the management process or investigation is consistently focused
- stakeholders' expectations
- mitigation of corruption risks relating to the misuse of confidential information
- authorisation from the delegated decision-maker to proceed in dealing with the complaint.

The level of your strategy should be commensurate to the risk, complexity, nature and timing of the investigative or other resolution processes.

Objective standards of honesty and integrity — *Public Sector Ethics Act 1994*

- Integrity and impartiality (section 6)
- Promoting the public good (section 7)
- Commitment to the system of government (section 8)
- Accountability and transparency (section 9)

Review against relevant standards

1. Is there sufficient evidence to support your conclusion and substantiate the allegations? Prepare an outcome (or an investigation) report — with allegations, methodology, findings and recommendations.
2. Are your recommendations appropriate to the seriousness of the allegations, in light of your agency's Code of Conduct, any standard of practice, policies and procedures? Ensure you have assessed the evidence against objective standards of honesty and integrity (including how reasonable members of the community would view it), not by subjective criteria.
3. Consider "grounds for disciplinary action" (see s. 187 *Public Service Act 2008*).
4. For QPS members: consider the Standard of Practice and the purpose of police discipline as set out in the *Police Service Administration Act 1990* and the *Complaint and Client Service Reporting Guideline*.

5 Implement your decision

When the evidence is assessed, your agency should:

- recommend and take disciplinary actions, if any
- recommend and take non-disciplinary actions, if any
- provide a final outcome to the subject officer, if necessary
- if the matter was dealt with as corrupt conduct, respond to the complainant under section 42(7) or 44(5) of the CC Act.

6 Prevent future incidents

Whether or not the allegations are proven, in the final stage focus on identifying particular gaps in your agency's internal controls or practices that expose it to an identifiable risk of corruption. This can be viewed at a business area level or an organisation-wide level, subject to the nature and seriousness of the allegation.

Your agency is best placed to identify deficiencies in its own systems and operations. This knowledge can be used to particularise risks, identify possible controls, and develop appropriate remedies. This includes balancing prevention costs against corruption risks.

Resources

For further information on the appropriate steps in responding to information security allegations, see the CCC's *Corruption in focus: a guide to dealing with corrupt conduct in the Queensland public sector*.

For information about ICT generally and information security, go to the Queensland Government Chief Information Office website, <www.qgcio.qld.gov.au>.

Remember

At any step, if you have a reasonable suspicion that corrupt conduct may have occurred, you must notify the CCC.

Crime and Corruption Commission
QUEENSLAND

Information on this and other CCC publications can be obtained from:

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