INTEGRITY COMMISSION TASMANIA

Managing confidential and protected information

Many public sector organisations are custodians of sensitive, confidential or protected information. You are responsible for the security of that information by managing classified records following their associated procedure.

Classifications of work information

Public sector organisations in Tasmania must comply with the Tasmanian Government Information Security Policy1. This Policy aims to provide a consistent approach to managing information security risks across the Tasmanian Government.

The accompanying Manual assists public sector organisations in implementing appropriate risk management procedures according to the Policy. The Manual defines five information security classification levels:

Classification	Definition
Public	Information that has been authorised by the owner/custodian for public access and circulation
Unclassified	Unclassified information that may need to be protected and controlled and is not to be considered public information
X-in-confidence	Information that, if compromised, could cause limited damage to the State, the Government, commercial entities or members of the public The 'X' refers to the audience, for example: ▼ Staff-in-confidence (such as personnel files, recruitment information, grievance or disciplinary records) ▼ Executive-in-confidence (such as sensitive financial reports, strategic plans, government matters) ▼ Commercial-in-confidence (such as tender responses, designs and government research)
Protected	Information that, if compromised, could cause damage to the State, the Government, commercial entities or members of the public For example, compromise could: endanger individuals and private entities, work substantially against government finances or economic and commercial interests, substantially undermine the financial viability of major organisations, impede the investigation or facilitate the commission of serious crime, and/or seriously impede the development or operation of major government policies.

Highly Protected	Information that requires a substantial degree of protection Compromise of the information could cause serious damage to the State, the Government, commercial entities or members of the public. For example, compromise could threaten life directly, seriously prejudice public order, and/or substantially damage government finances or economic and commercial interests.

Principles of protecting classified information

Your public sector organisation will have information security procedures for preparing, processing, storing, archiving, disposing, and transmitting each information classification. The procedures will also prescribe how the information may be discussed.

For example, the following principles are likely to be covered in the procedures:

- General safeguarding
  - all information other than 'public' information is restricted from the view of the public
  - only those that have agreed to protect it are allowed to view the information
- Safeguarding of electronic information
  - access to computer systems containing classified information is restricted to only those that are under an obligation to protect the information
  - employees' logins and passwords are not shared with others
- Restricted distribution
  - distribution of classified information is restricted to those who have a legitimate need to know it

Abuse of work information

Abuse of work information occurs whenever information is accessed, shared, altered or created for any purpose other than to perform your work duties.

Unauthorised access occurs whenever you access work information for any purpose other than to perform your work duties.

Serious misconduct

The following conduct by employees may amount to serious misconduct:

- accessing confidential or protected information without authority
- accessing confidential or protected information without an official purpose
- improper disclosure of confidential or protected information, or
- misuse or abuse of confidential or protected information.

Breaching confidentiality or protection in the public interest

Public sector employees may come across classified information they believe should be shared to inform public debate. However, information is kept confidential or protected for many reasons, including to protect an individual's privacy.

It is vital that sensitive information is protected, and you do not release it if you are not authorised to do so, even if you believe the information is in the public interest.

CASE STUDY

In 2012, a Department of Defence graduate recruit was given access to confidential and classified defence information. Approximately eight months into their employment, they downloaded a document classified SECRET and took it home before posting two pages of material to an online forum.

The graduate believed that the public should be aware of the information, and published two pages of a report online alongside the statement, “I release what I feel should be in the media”.

The recruit’s actions were discovered by a former Department of Defence employee who reported it, and the Australian Federal Police were able to track the internet protocol (IP) address of the original forum post by the offender.

The graduate was sentenced to one year in prison.

Extracted from misuse of information report, IBAC[2]

Consequences of breaches

Abuse of work information can have serious consequences. For the people whose information is accessed or disclosed to third parties without their knowledge or consent, breaches can have ongoing and long-lasting effects.

These can include stress, feelings of vulnerability, financial loss, and frustration with obtaining redress or adequate compensation. A breach of confidentiality may even put them in a dangerous situation.

Additionally, the public sector organisation may experience reputational damage or loss of public confidence in its operations. It may also be liable for failing to protect classified information from abuse.

Consequences for the perpetrator may extend to dismissal, prosecution or civil legal action against the individual and organisation involved.

CASE STUDY

A Queensland Emergency Services Inspector had privileged knowledge about the tender process for a contract. The inspector shared the quotes he had received from other potential contractors with a friend, and asked if the friend could "do any better".

The inspector was sentenced to three years' imprisonment, for the breach of confidentiality and other associated misconduct.

Extracted from 'Prevention in focus' report, Queensland CCC[3]

How to prevent breaches

Before you share information, ask yourself:

- Have I been authorised to share this information?
- Am I sharing this information with someone authorised to access and use it?

If you answer **no** to either of these questions, do not proceed.

If you still feel uncertain, seek advice from your manager about accessing and sharing information appropriately in your circumstances.

---

[1] www.dpac.tas.gov.au/__data/assets/pdf_file/0007/509470/Tasmanian_Government_Information_Security_Policy_and_Manual_-_REVIEW_PENDING.pdf

[2] www.ibac.vic.gov.au/docs/default-source/research-documents/unauthorised-access-and-disclosure-of-information-held-by-the-victorian-public-sector.pdf?sfvrsn=d76fc48_6

[3] www.ccc.qld.gov.au/sites/default/files/Docs/Publications/CCC/prevention-in-focus-procurement-fraud-attracts-prison-sentence-2019.pdf

The Commission can help

We are available to provide support and assistance with identifying, reporting, investigating, managing and preventing misconduct: prevention@integrity.tas.gov.au or 1300 720 289.

For more Misconduct Prevention resources go to www.integrity.tas.gov.au/resources