1. Introduction

1.1. Background

[1] The last thirty years have seen significant advances in technology, and a corresponding increase in public sector reliance on – and access to – personal and sensitive information.

[2] In the modern world, information abuse is a risk in all public sector organisations. Information abuse is when an employee either accesses information to which they are not entitled, or misuses information gained by virtue of their employment.[1] Most public sector employees have the capacity to abuse information in some respect.

[3] Information abuse can have serious adverse ramifications for organisations, not least because of the potential for the erosion of public trust. Abuse of information by public sector employees is therefore a source of continuing focus for integrity agencies across Australia.

[4] The Integrity Commission (the Commission) had for some time considered that it should investigate how Tasmanian public sector organisations manage information and allegations of information abuse by their employees.

Why Tasmania Police?

[5] Although this report will be valuable for many public sector organisations, its focus is on Tasmania Police.

[6] Police organisations are more reliant on information, and on their employees handling information appropriately, than most public sector organisations. From its annual audits of police complaints, the Commission had identified that this may be an issue that could be handled better by Tasmania Police.

[7] The Commission has conducted four full annual audits of complaints against police.[2] For a range of reasons, we decided that in future these audits would be conducted less frequently, and that the Commission would occasionally undertake own-motion investigations into particular police misconduct issues. We decided that the first of these own-motion investigations would be into allegations of unauthorised access to, and misuse of, information.

[8] The way in which Tasmania Police views information abuse is important not only in terms of the police service itself, but for the entire Tasmanian public sector. This is because it is not only police that have access to personal and sensitive information. For example, employees in Transport (part of the Department of State Growth) and in the Tasmania Prison Service (part of the Department of Justice) also have access to this kind of information.

---

[1] Terminology about abuse of public sector information may vary depending on the circumstances. For the sake of simplicity, this report uses the phrases 'unauthorised access to information' and 'misuse of information'. The term 'information abuse' is used as a global phrase to cover both unauthorised access to, and misuse of, information.

[2] These reports can be access on our website at <www.integrity.tas.gov.au/reports_and_publications/reports>.

- requires users of restricted databases to enter passwords and agree to an acknowledgement of use on login, and
- performs alert monitoring of selected records and transactions on databases.

[150] However, it did seem apparent from the Commission's audit of files that officers are not automatically logged out of one of the main police databases (IDM). This means that, in theory, they can (unknowingly) be logged in for days. Additionally, one officer did not realise that they could log out of one of the other police databases (ICE).

Alert monitoring

[151] Integrity Commission audits indicate that Tasmania Police routinely puts 'flags' (alert monitoring) on prominent database entities. For example, if a famous Tasmanian is charged with a criminal offence, a flag is set up on the relevant database entries. These flags trigger an alert to Professional Standards when accessed by an employee. Checks are then done to see if the access was authorised.

Reasons for access

[152] A number of Tasmania Police databases require the user to enter a RFA. Like other police services, Tasmania Police has had difficulty communicating the importance of the RFA process to its employees. It is now trying to raise awareness about the importance of RFAs as part of recruit training and through its audits. As explained below, audited employees are told in a formal letter if their RFAs could be improved.

Police-issued mobile computing devices (tablets)

[153] Many Tasmania Police officers have a personal work-issued tablet that they may use as they see fit, including by taking it home. From the tablet, they can access a range of police databases. There are obvious risks involved in this, including the inadvertent disclosure of information by forgetting to lock the tablet.

[154] The organisation has a policy on the use of the tablets that acknowledges and intends to mitigate these risks. The tablets are password protected. The Commission was told that officers are not allowed to let other people use them, although that is not specified in the policy. The policy does state several times that the tablets may be audited, including remotely. It also states that officers are responsible for ensuring that 'any departmental systems including the police intranet is not accessed or viewed' by persons not employed by the Department.

Removing and restricting access rights

[155] It is not common practice for Tasmania Police to restrict its officers' access rights. This includes officers that have been suspended or are under investigation for abuse of information, and officers that are on long term leave. Access restrictions have been imposed in very rare cases, for example when there is a public safety risk.

[156] The reason for Tasmania Police's reluctance to restrict access and/or restrict potential for communication with colleagues is because:

- even when an employee is suspended for alleged information abuse, the allegation is still unproven
- in nearly all cases, officers need access to information to do their job – if access were to be restricted, in many cases they would need to be reallocated or stood down even when this is otherwise unnecessary, and
- Tasmania Police wants its officers to feel part of the organisation, even when on long-term leave, and so encourages them to maintain their communications with the organisation.

[157] One of the files audited by the Commission as part of this investigation involved the alleged leaking of information by a disgruntled officer on long-term leave. Tasmania Police's assessment of this allegation was that it was unproven. However, the Commission considered that – on the balance of probabilities – the officer did access and leak the information. Had the officer's access rights been restricted, the information would not have been leaked. During the investigation, Tasmania Police advised that it is unrealistic to sever an officer's access to his workplace whilst on leave, as the allegation remained under investigation, and in any event, the matter at hand did not warrant suspension of the officer (which is when station access and IT access – by tablet removal – would be denied. Further, the finalisation of this particular matter occurred after the officer was no longer a member of Tasmania Police, and therefore the Code of Conduct could not apply to the officer, in so far as the application of sanctions under the *PS Act*.

Access to information awareness plan and system audits

In December 2016, the Tasmania Police executive approved the '*Access to Information Awareness Plan*'. This was shortly after the Commission discussed information abuse with the then Professional Standards commander as part of its annual audit process.

One key aspect of the plan was to remind employees of their responsibilities through the *Tasmania Police Gazette*, the intranet and posters. The most substantive part of the plan was to commence a proactive audit program of police officer access to databases. In the past, audits had only been undertaken on a reactive basis, for example when a complaint was received. A pilot audit program was run in July 2017.

The audit program is currently ongoing. Tasmania Police aims to audit about 50 randomly selected police officers per month, meaning that every officer – up to and including the Commissioner – would get audited once every two years. The same program has also been initiated for State Service employees working in Tasmania Police.

The audits involve a general check of each officer's access over the preceding month. If any issues are detected, a more in-depth search of the officer's accesses is undertaken. A check is also performed to see if any other officer is accessing information about that officer.

Audits are also undertaken on accesses to information about prominent persons.