ICAC
Independent Commission
Against Corruption
SOUTH AUSTRALIA

Integrity Spotlight

V1.0 – January 2023

Advisory

Information management systems require robust controls to prevent information being improperly accessed, edited, disseminated or deleted.

Audit logging

State and local government agencies store large volumes of information about South Australians and government business. Information is a valuable asset that is vulnerable to improper use.

Public officers can be motivated to misuse official information for personal or commercial gain, or to cover up wrongdoing. Information can be improperly accessed out of curiosity, or used for identity theft, blackmail and other criminal activity.

Information management systems require robust controls to prevent information being improperly accessed, edited, disseminated or deleted. Audit logging is one control to mitigate the risk of misuse. It must sit alongside other security measures, staff education and training, and clear policies and procedures on information security.

This advisory complements the Commission's advisory on confidentiality and the misuse of information.[1]

[1] Independent Commission Against Corruption, Integrity Spotlight: Confidentiality and misuse of information (Guide, 2022). https://www.icac.sa.gov.au/education/education-resources/integrity-spotlight-confidentiality-and-misuse-of-information

What is audit logging and why is it necessary?

Audit logs record user activity within information systems, including:

- details of specific events (such as access to a record, device or premises, or instances where a record is created, modified or deleted)
- the date and time of the event
- details of the user responsible for the event (where a unique log-in or access card is used)
- the relevant location or device.

Audit logs can be used to determine whether users are complying with policies and procedures and to investigate allegations of information misuse.

If systems cannot be audited or audit logging capabilities are not fully enabled, wrongdoing may go undetected and unaddressed.

For example, the Commission examined allegations that a public officer working in the health sector edited the ‘free text’ section of a patient’s medical notes to cover up prior wrongdoing. The capability to log changes to ‘free text’ fields had been deactivated by system administrators because it took up too much space in the system. This prevented a full investigation of the allegations.

> If systems cannot be audited or audit logging capabilities are not fully enabled, wrongdoing may go undetected and unaddressed.

What can agencies do?

The Code of Ethics for the South Australian Public Sector is the primary source of guidance for public sector employees on the use of official information. Local government employees have a duty under the *Local Government Act 1999* to protect confidential information.

All agencies should have policies and procedures that reinforce these expectations. Such policies and procedures should be regularly communicated to staff. Staff should be informed about how system use is logged and audited. This can deter information misuse.

Public sector policies and procedures should align with the South Australian Information Classification System and the criteria specified in the whole of government Protective Security Framework (SAPSF), the ICT, Cyber Security and Digital Government Strategy 2020-2025 and the South Australian Cyber Security Framework (SACSF).

Public authorities should also develop, maintain and promote clear policies regarding conflicts of interest.

Audit logging should be one aspect of an agency's broader strategy for maintaining the integrity of the information it holds. It is not possible to proactively monitor all occasions of information access by public officers. However, there are a number of steps that can be taken to prevent and detect information misuse.

These include:

- providing employees with an induction and quarterly reminders on their obligations for handling official information
- ensuring that information management systems are capable of recording user activity
- developing and maintaining an audit schedule for reviewing audit logs, as well as reviewing logs in response to allegations of misuse
- ensuring users only have access to the information they need to undertake their role, and that access is reviewed when a user's role changes
- restricting the ability to access, edit or delete audit logs
- having system warnings that are triggered when a user attempts to access sensitive information, along with reminders that user access is recorded
- incorporating escalation mechanisms for certain user activity, such as a user searching for their own name or attempting to access information that is particularly vulnerable to misuse (high profile or vulnerable clients, matters of media interest or significant projects).

Resources

Independent Commission Against Corruption advisory on confidentiality and misuse of information
ICT, Cyber Security and Digital Government Strategy
The South Australian Protective Security Framework (SAPSF)
The South Australian Information Classification System
Code of Ethics for the South Australian Public Sector
South Australian Cyber Security Framework
Premier and Cabinet Circular PC012 – Information Privacy Principles Instruction

CONTACT US

☎ **GENERAL ENQUIRIES**
(08) 8463 5191

LEVEL 1, 55 CURRIE ST
ADELAIDE SA 5000

@ICAC_SA

ICAC.SA.GOV.AU

ICAC
Independent Commission Against Corruption
SOUTH AUSTRALIA