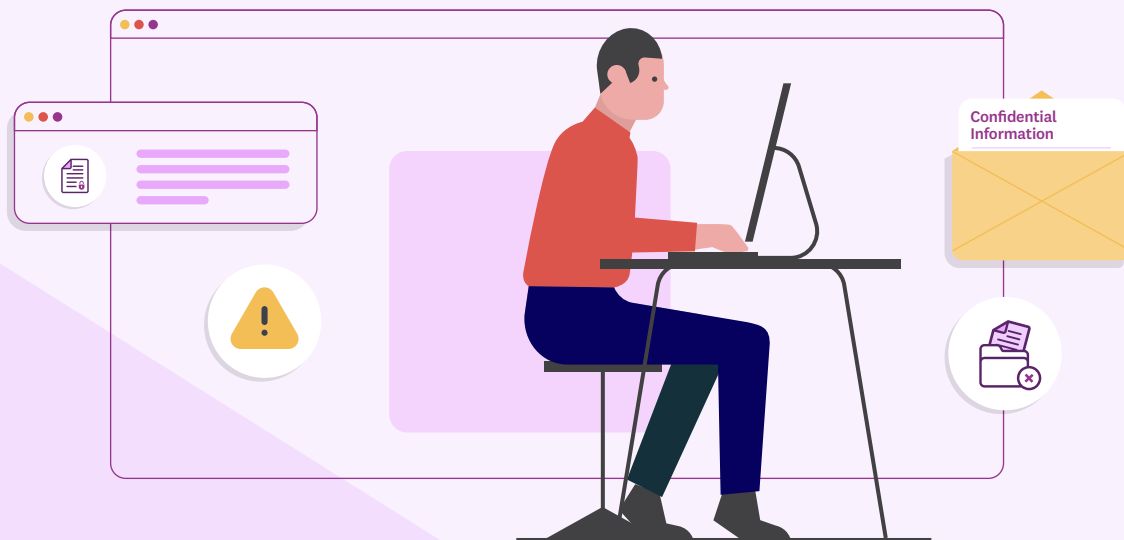




Leaking of confidential information

Guidance material – integrity scenario

This guidance material presents an ‘integrity scenario’ which is intended to assist in public sector training regarding integrity risks, highlighting the importance of maintaining rigorous information integrity and ethical standards in the Victorian public sector. By addressing the root causes of information misuse by strengthening governance and oversight, promoting a culture of integrity, and taking decisive action against misconduct, organisations can safeguard public trust and effective service delivery.

The situation

A senior data analyst in a Victorian emergency services agency prided themselves on their commitment to public safety and ethical conduct. Their role involved managing sensitive information crucial for coordinating responses to natural disasters, accidents and medical emergencies. However, the analyst became involved in a situation showing how small misjudgements paired with a poor integrity culture can, over time, leave organisations vulnerable to corrupt behaviour.

At the agency, the analyst and their colleagues often discussed high-profile emergencies and incidents, curious about the details and outcomes. One day, a colleague of the analyst mentioned accessing the agency’s restricted database to look up information on a recent celebrity car accident. The colleague assured the analyst it was harmless, just a ‘perk’ of their job.





How did the misconduct start?

After some hesitation, the analyst decided to access the restricted database, justifying it as a one-time occurrence. The personal details and medical outcomes they could access fascinated the analyst and, over time, their casual access to the restricted database became more frequent.

They checked on incidents involving acquaintances or interesting events, viewing it as a 'benefit' of their role. The analyst also began to share their findings with a few trusted colleagues, creating a small circle of informal information sharing. The practice was widespread and went unaddressed, leading to the perception that it was acceptable.

The analyst did not see it as a serious violation, since they or other colleagues did not get into trouble. The agency's lax approach to monitoring data access reinforced their belief that it was not a big deal. This normalisation of behaviour set the stage for more serious misconduct.

How did it escalate?

The serious corruption began to escalate when the analyst observed a colleague using their access to obtain information on sensitive medical cases and inquired about it. The colleague initially accessed information related to the celebrity car accident and later began using similar tactics to obtain data on other sensitive medical cases. The colleague then explained that they were helping a friend in the insurance industry by providing insights into potential claims. They suggested the analyst could do the same, mentioning it as an easy way to earn favours or gifts.

Initially uncomfortable with the idea, the analyst dismissed it. However, the constant exposure to casual misuse of data and the allure of favours eventually eroded their initial resistance. The analyst started providing occasional updates on certain cases to acquaintances in exchange for small favours or gifts, justifying it as harmless assistance.

However, the impact was far-reaching. Victims of emergencies, whose personal information was leaked, faced breaches of privacy and potential financial harm.

The analyst's misuse of agency data was uncovered during an external audit by a cybersecurity firm hired by the agency. The subsequent investigation led to the analyst's and several colleagues' termination and prosecution. The agency faced intense scrutiny, prompting a comprehensive review of its data management practices and internal controls.

Lessons learned

- Strengthen data access controls to ensure only authorised personnel handle sensitive information.
- Conduct routine audits to promptly detect and prevent data misuse.
- Offer a secure whistleblower system for safe misconduct reporting.
- Provide training to reinforce the importance of ethical data handling.
- Promote a workplace culture that values integrity in managing data.

This product was prepared based on findings from research and stakeholder consultations from IBAC's 2024 Public Sector Strategic Assessment. It is representative and created for educational purposes only. Any resemblance to real persons, organisations, or incidents is purely coincidental.

If you experience or suspect public sector corruption, report it to IBAC



Fill out the secure online form to report at www.ibac.vic.gov.au



If you have difficulty accessing the online form, call us on **1800 422 284** for further assistance.



If you need help with translation, call Translating and Interpreting Service on **13 14 50** or visit www.ibac.vic.gov.au/mylanguage