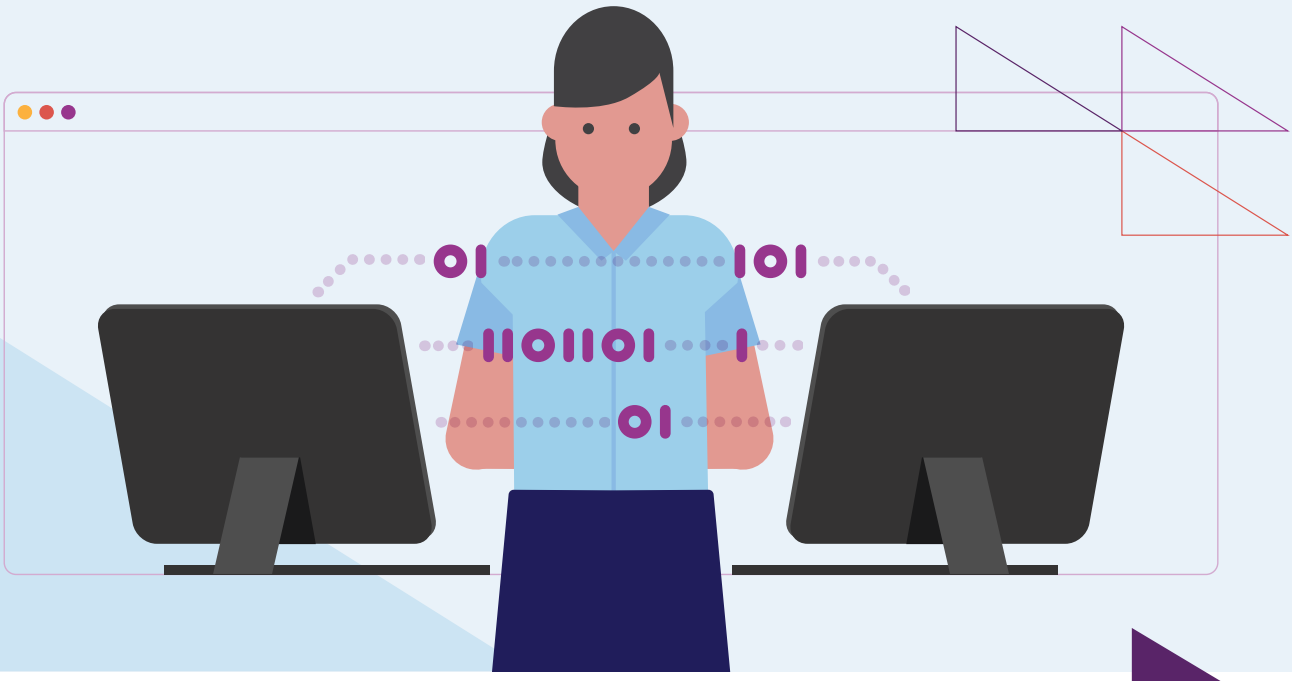

Misuse of artificial intelligence in the public sector

Guidance material – integrity scenario

This guidance material presents an 'integrity scenario' which is intended to assist in public sector training regarding integrity risks, illustrating how unregulated use of artificial intelligence (AI) by a public servant can lead to corrupt practices, including timesheet fraud. It highlights the risks of a lack of clear policy and governance, when AI is used without proper oversight. When used ethically and responsibly, AI can be a useful tool to support work in the public sector. However, this integrity scenario demonstrates how a policy officer's intention to reduce their workload led to the unauthorised use of AI and corrupt behaviour, breaching confidentiality and compromising integrity.

The situation

A policy officer at a Victorian Government agency was responsible for producing detailed reports on various agency activities. Initially, the policy officer used their expertise to create these reports, working long hours to complete them.

As their workload increased, the policy officer discovered a public, non-secure AI tool that could assist with data analysis and report creation. Intrigued by its capabilities, they began experimenting with it to supplement their work.

How did the misconduct start?

The policy officer knew the use of this AI tool was not authorised, but the agency did not have clear governance for AI use. At first, the policy officer used the AI tool sparingly, mainly to generate initial drafts or analyse complex data sets. To do so, the policy officer had to input confidential data and information into the non-secure AI tool. They were impressed by the tool's efficiency and output quality, so continued its use while pretending the work was their own.

Strengthening Victoria's Integrity
ibac

Over time, the policy officer noticed that their supervisors and colleagues rarely questioned the AI-generated content, assuming it was the result of the officer's work. This realisation led to the policy officer relying more heavily on AI to reduce their workload, until their work was almost entirely generated by the AI tool, which did not maintain department privacy or security.

To cover up their misuse of AI, the policy officer added fabricated details to the reports to make them appear as though they had been personally reviewed and validated. This included inserting generic comments and annotations that suggested the reports had been peer reviewed. When questioned about discrepancies in the reports, the policy officer provided vague explanations and shifted the blame to data issues or reporting inaccuracies, rather than admitting to the use of AI.

Additionally, the policy officer adjusted their work records to indicate that they had spent significant time working on the reports. This involved creating false entries in time logs and email records to mislead their supervisors about their actual work activities. They also limited their interactions with colleagues and avoided situations where their lack of involvement could be observed.

How did it escalate?

As the policy officer became overconfident in their ability to use the AI tool without detection they began not returning to work after lunch and neglected their work responsibilities while the AI tool generated outputs that mimicked human behaviour.

Their extended absences raised concerns among colleagues who advised their manager, but due to weak monitoring systems, these issues were not promptly addressed.

The policy officer's confidence in their ability to avoid detection allowed their actions to remain hidden for several months.

The problem came to light when the AI tool inadvertently included information protected under the *Privacy and Data Protection Act 2014*, prompting a supervisor to investigate. When questioned, the policy officer admitted their unauthorised use of the AI tool, and failure to review the reports it generated, leading to inconsistencies and inaccuracies. This further uncovered their efforts to hide the AI-use, including fraudulent timesheets.

The policy officer faced severe disciplinary action. They were terminated from their position due to gross misconduct and breach of trust, which damaged public confidence in the integrity of the agency by exposing vulnerabilities in the oversight and accountability processes.

Lessons learned

- Develop clear policies outlining acceptable AI use and require staff to sign off on them annually.
- Roll out mandatory training sessions on AI ethics and the consequences of misuse, tailored to your organisation.
- Advise public servants on best practices for using AI, including a dual sign-off process, requiring both the user and a peer to validate the content.
- Introduce random checks on AI-related activities – such as searching browser histories for use of common AI tools – to ensure compliance with ethical standards.

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 similarities 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 **1300 735 135** 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**