WESTERN AUSTRALIA

CCC | Corruption and Crime Commission

Report on Risks to Confidential Information Control in the Public Sector

08 May 2025

ISBN 978-1-7637189-4-4

This report and further information about the Commission can be found on the Commission Website at www.ccc.wa.gov.au.

Corruption and Crime Commission

Postal Address: PO Box 330 Northbridge Post Shop WA 6865	**Email:** info@ccc.wa.gov.au **Twitter:** @cccWestAus
Telephone: (08) 9215 4888	**Office Hours:** Monday to Friday 8.30 am to 5.00 pm

Special Needs Services

If you have a speech or hearing difficulty, contact the Commission via the National Relay Service (NRS) on 133 677 and ask for (08) 9215 4888, or visit the NRS website, www.relayservice.com.au.

If your preferred language is other than English, contact the Translating and Interpreting Service (TIS) for assistance on 13 14 50. TIS provides a free, national telephone interpreting service available 24 hours a day, seven days a week. TIS also provides on-site interpreters for face-to-face interviews by contacting 1300 655 082.

CCC | Corruption and Crime Commission

Image credit: This artwork was painted by Corruption and Crime Commission staff under the guidance of Justin Martin from Djurandi Dreaming.

TABLE OF CONTENTS

INTRODUCTION

[1] Public officers have access to sensitive information in order to perform their duties. This is particularly so for the Department of Finance (Finance). Strong controls are necessary to maintain confidentiality. One officer exploited weaknesses in controls to download and keep restricted information. This report is a reminder to all government departments about serious misconduct risks when controls are insufficient.

[2] Finance is a central agency that provides leadership and strategic advice across the public sector to support the delivery of services throughout Western Australia.

[3] This report concerns the actions of a former senior officer (Officer) at Finance.

[4] In March 2023, Finance notified the Commission[1] that the Officer had downloaded confidential information from Finance's computer system to a USB before leaving to take up a position in the private sector.

[5] To constitute serious misconduct under s 4(b), a public officer must have acted corruptly to benefit themselves or another person, or cause detriment to someone. Corruption has been held to include conduct that includes moral impropriety in public administration, or some perversion of the proper performance of the duties of office.[2]

[6] Serious misconduct under CCM Act s 4(c) requires a public officer to have committed an offence punishable by 2 or more years' imprisonment while acting or purporting to act in his or her official capacity. The offence that the Commission's investigation focused on is the offence of the unlawful use of a computer system contrary to *Criminal Code* s 440A.

[7] The Commission undertook a cooperative investigation with Finance, named Operation Stremoy, to investigate the Officer's actions. The cooperative agreement worked well. As part of Operation Stremoy the Commission exercised its statutory powers to compulsorily acquire records and examine relevant witnesses.

[8] At the conclusion of the investigation the Commission formed no opinion of serious misconduct against the Officer. However, the Commission's investigation identified serious misconduct risks in relation to the policies and procedures at Finance aimed at protecting confidential information,

[1] *Corruption, Crime and Misconduct Act 2003* (CCM Act) s 28.
[2] *Independent Commission against Corruption v Cunneen* (2015) 256 CLR 1 at [76] per Gageler J, *State of Western Australia v Burke (No 3)* [2010] WASC 110 at [74].

and Finance's use of USBs; risks which may also be applicable to other departments and agencies.

[9] A serious misconduct risk is considered to be conduct, circumstances or lack of governance that may expose an entity to financial or other harm or loss.

[10] Before the report was finalised, the Commission gave copies of a draft report to Finance and the Officer. Each responded. Where the Commission accepts their submissions, the draft report has been amended accordingly.

[11] The Commission recommends that:

a. Finance review and enhance the confidentiality agreement its employees are required to sign to make it abundantly clear that employees are required to maintain confidentiality and abide by the non-disclosure requirements of official information acquired in the course of their duties, as set out in Finance's Code of Conduct; and

b. Finance consider implementing a procedure by which departing staff are reminded of their obligation not to disclose any confidential information once they leave.

[12] In its response to the draft report Finance has accepted the recommendations. It has:

- reviewed and enhanced the confidentiality agreement for its employees; and
- implemented a procedure by which departing employees are reminded of the ongoing confidentiality obligations once they leave.

CHAPTER ONE

Actions by an officer downloading sensitive documents

[13] The Officer was a long-serving Western Australian public officer.

[14] After resigning from his position at Finance, and before leaving, the Officer downloaded 591 documents from Finance's computer system to a USB. The documents were a mix of personal and Finance documents. Some Finance documents contained highly sensitive Government information, including a Cabinet decision sheet, Cabinet submission and budget submission.

[15] The Officer downloaded the documents on five separate occasions in the last month of his employment. All of the downloads occurred either on the weekend or after normal business hours. The Officer was not in the Finance office when he downloaded the documents.

[16] In evidence to the Commission, the Officer accepted that he downloaded the documents. The Officer's evidence was that he commonly worked outside of business hours,[3] so it cannot be said that he was not working when he downloaded the documents.

[17] The last download occurred after normal business hours on the Officer's last day of employment at Finance. The Officer sought, and was granted, approval from his manager to keep his Finance-issued laptop over the weekend for the purpose of finalising some administrative tasks.

[18] Finance was unaware of the downloads when they occurred. Finance did not actively monitor the use of USBs in its computers. Finance became aware of the downloads as part of a proactive approach to monitor downloads of exiting employees. It notified the Commission.

[19] During his examination, the Officer said that he downloaded the documents for the purpose of giving them to the person who was taking over his role.

[20] The Officer said: [4]

> *There were some files that I wanted to save for the person taking on my role so they could access them at a later stage and so on.*

[3] Officer transcript, private examination, 18 July 2024, p.25.
[4] Officer transcript, private examination, 18 July 2024, p.28.

[21] He again confirmed that he: [5]

> *…downloaded a number of records, as you have shown, with the intention of providing all those records to [the person who took over his role] so [they have] them in one spot.*

[22] Contrary to his stated intention, the Officer never gave the downloaded records to his replacement.

[23] The Officer told the Commission that he did not give the USB to the person who took over his role because he lost it and, when he subsequently found it a few months later, he destroyed it.[6] The Officer said he destroyed the USB because he realised there were files on it that 'probably shouldn't be in my possession in the first instance'.[7]

[24] The Commission heard evidence from the Officer and other witnesses that:

a. there was an inconsistent practice of saving documents to Finance's record-keeping system, TRIM,[8] meaning that it could not be said with certainty that the documents the Officer downloaded were saved to TRIM;

b. there was inconsistent practice as to the naming protocol for documents saved to TRIM[9] and TRIM was not easily searchable unless the document number or file number was known.[10] As a result, it could not be said with certainty that the documents the Officer downloaded would be able to be located if the documents had been saved to TRIM;

c. the person taking over the Officer's role was not fully across what the Officer was working on in the months preceding the Officer's departure,[11] and was not familiar with some of the documents the Officer had downloaded;[12] and

d. there was not a 'really structured handover discussion'[13] or 'formal handover package'[14] between the Officer and the person taking over his role.

---

[5] Officer transcript, private examination, 18 July 2024, p.45.
[6] Officer transcript, private examination, 18 July 2024, p.29-30.
[7] Officer transcript, private examination, 18 July 2024, p.30.
[8] Witness 1 transcript, private examination, 23 August 2024, p.5-6.
[9] Witness 1 transcript, private examination, 23 August 2024, p.5-6.
[10] Witness 1 transcript, private examination, 23 August 2024, p.6-7.
[11] Witness 1 transcript, private examination, 23 August 2024, p.11.
[12] Witness 1 transcript, private examination, 23 August 2024, p.23.
[13] Witness 1 transcript, private examination, 23 August 2024, p.15.
[14] Witness 1 transcript, private examination, 23 August 2024, p.18.

[25] The Commission also heard evidence that casts doubt on the Officer's reason for downloading the documents, including that:

a. it would be unusual to use a USB as a way of sharing documents with colleagues, the common practice within Finance being to email links to documents on TRIM;[15]

b. although there was not a 'really structured' handover, there was a handover consisting of meetings and emails;[16]

c. the person taking over the Officer's role was a long-serving Finance employee who felt confident taking on the role,[17] and was familiar with (and either had a copy of or knew how to find on TRIM) some of the documents the Officer had downloaded;[18] and

d. the Officer did not at any point during the handover tell the person taking over his role that he was going to give them documents on a USB.[19]

[26] It is difficult to accept the Officer's reason for downloading the documents in circumstances where:

a. he downloaded personal documents, as well as Finance documents, onto the USB (although he said he was going to remove the personal documents before handing over the USB);[20]

a. despite the Officer's evidence that it was not unusual to use USBs at Finance,[21] the only time he used a USB in the 6 months preceding his departure were the five occasions on which he downloaded the documents;

b. at no point between starting to download the documents and leaving Finance did the Officer mention to the person taking over his role that he was downloading documents for the purpose of handing them over, despite there being a handover of the role in the form of meetings and emails during that time; and

c. the Commission heard evidence that some of the downloaded documents contained information that would be commercially valuable to the private sector.[22] The Officer admitted that at least one

[15] Witness 1 transcript, private examination, 23 August 2024, p.8.
[16] Witness 1 transcript, private examination, 23 August 2024, p.13-19.
[17] Witness 1 transcript, private examination, 23 August 2024, p.16.
[18] Witness 1 transcript, private examination, 23 August 2024, p.20 and 22.
[19] Witness 1 transcript, private examination, 23 August 2024, p.19.
[20] Officer transcript, private examination, 18 July 2024, p.91.
[21] Officer transcript, private examination, 18 July 2024, p.29.
[22] Witness 3 transcript, private examination, 17 July 2024, p.16, 22-23.

of the documents he downloaded related to work in which his new employer would have been interested.[23]

[27] The Commission's opinion is that, on the balance of probabilities, the explanation the Officer gave for downloading the documents is implausible. However, there is no evidence of an unauthorised purpose for which the Officer downloaded the documents.[24] In order to establish an offence of unlawfully using a computer system under *Criminal Code* s 440A, a person's use of a computer system, such as TRIM provided by Finance, must have been unauthorised or not in accordance with any authorisation. In this case, while it is difficult to accept the Officer's evidence, there is no evidence that he was acting otherwise than in accordance with his authorisation to access and deal with the documents for a purpose related to his role. There is no evidence that he downloaded the documents for personal gain, or to benefit his new employer, or cause detriment to Finance or anyone else.[25] There is also no evidence that the Officer disclosed any confidential information to his new employer or to anyone else.

[28] An opinion of serious misconduct, though having no legal consequence, may have other damaging effects. It assesses evidence on the balance of probabilities, applying the caution of seriousness in *Briginshaw v Briginshaw* (1938) 60 CLR 336. The Officer's actions in downloading the documents do not reach the threshold for an opinion of serious misconduct.

[23] Officer transcript, private examination, 18 July 2024, p.37.
[24] *Criminal Code* s 440A and CCM Act s 4(c).
[25] CCM Act s 4(b).

CHAPTER TWO

Serious misconduct risks

[29] In addition to considering whether the Officer engaged in serious misconduct, the Commission considered the serious misconduct risks arising from the circumstances in which the Officer's conduct occurred.

Finance's policies and procedures relating to confidential information

[30] As with all government organisations, Finance has policies designed to keep information confidential. Finance's Code of Conduct provides: [26]

> *As employees we are required to maintain confidentiality and abide by the non-disclosure requirements of official information acquired in the course of our duties.*

[31] Finance's Acceptable Use Policy states that Finance personnel must: [27]

> *[O]nly access computing resources that they are authorised to use, and not seek to gain, or gain unauthorised access to information, resources or entities that are not required for the purpose of fulfilling their duties and responsibilities.*

[32] Users are required to acknowledge that they have read and will abide by these policies when accessing Finance's computer system. The Officer accepted that he would have been required to acknowledge that he had read and would abide by these policies to log in to his Finance-issued laptop.[28] The Officer also accepted that he knew Cabinet documents needed to be handled in a highly confidential manner.[29]

[33] During the investigation, Finance provided to the Commission a copy of its confidentiality agreement that employees were required to sign upon commencing employment.[30] The confidentiality agreement required employees to acknowledge, by signature in the presence of a witness, the following:

> *I understand that during my work with the Department of Finance I may be required to deal with confidential information.*
>
> *I also understand that in accordance with the Department of Finance Code of Conduct I am not permitted to publicly comment, either verbally, written or transmitted in any form on such matter or matters relating to the Department of Finance clients, the public service or Crown business which has become known to me in the course of my work with the Department of Finance, including after my employment has ceased with the Department.*

[26] 00940-2023-0045 - Finance Code of Conduct January 2023, p.6.
[27] 00940-2023-0044 - Acceptable Use Policy and Guidelines, p.2.
[28] Officer transcript, private examination, 18 July 2024, p.27.
[29] Officer transcript, private examination, 18 July 2024, p.33.
[30] 00940-2023-0180 - Confidentiality Agreement.

[34] This agreement did not adequately inform employees of their obligation to maintain confidentiality. The first part merely required employees to acknowledge that they understand they may be required to deal with confidential information, with no express obligation to keep that information confidential, and the second part contains a restriction on making public comment.

[35] Finance issues exit surveys to all exiting employees and managers complete an exit checklist when employees leave. However, Finance does not conduct exit interviews with departing employees and told the Commission that 'it appears no clear discussion occurred [with the Officer on exit] about confidentiality obligations'.[31] By failing to conduct exit interviews or remind departing employees of their confidentiality obligations, Finance is missing an important opportunity to ensure ongoing confidentiality obligations stay front of mind for departing employees.

[36] The ease with which the Officer downloaded and removed from Finance premises Cabinet documents also raises cause for concern. The Government Cabinet Handbook states that 'Ministers have primary responsibility for maintaining satisfactory security systems for Cabinet documents in their areas of responsibility, including the extent to which others have access to them'.[32] All Ministers and public sector agencies should consider whether appropriate controls are in place for the security of Cabinet documents.

[37] In response to this report, Finance told the Commission that it:

a. has started classifying emails and Office 365 documents to ensure that information, including sensitive information, is appropriately labelled, which is consistent with the WA Government's Information Classification Policy;

b. has a new information management project which will further safeguard sensitive information;

c. will complement these measures with training, awareness sessions and educational materials for staff;

d. has reviewed and enhanced the confidentiality agreement for its employees; and

e. has implemented a procedure by which departing employees are reminded of their ongoing confidentiality obligations once they leave.

[31] Finance email to the Commission dated 11 November 2024.
[32] Department of the Premier and Cabinet, Western Australia Government, 'Cabinet handbook', (11 July 2024) Ch 3.

Finance's policies and procedures relating to use of USBs

[38] At the time the Officer downloaded the documents, Finance did not have a policy governing the use of USBs or the downloading of documents to USB. Since the Officer's conduct (but not because of it), Finance implemented a policy that USBs need to be encrypted for usage.[33] The technology Finance has adopted to ensure USBs are encrypted works by automatically encrypting any USB inserted into a Finance-issued laptop. This includes USBs personally supplied by Finance staff. Finance has not implemented a policy prohibiting the use of personal USBs. Further, Finance does not record the provision of Finance-issued USBs to staff.

[39] The Commission heard evidence that the use of USBs in Finance is common, and that Finance still uses USBs to share information externally with other parties who may not have the same technology as Finance.[34]

[40] In its 'FAQ - Secure USB Drives' document, Finance states that '[s]ensitive information should not be copied on USB drives', and refers readers to its Information Classification Policy and Acceptable Use Policy for more details.[35] In this document, Finance also recommends that Microsoft Teams and SharePoint be used for sharing files with an external party instead of USB, subject to the sensitivity of the information being shared.

[41] The use of USBs without appropriate controls provides a method of taking documents (including confidential documents) away from the workplace and poses a serious misconduct risk. Public sector agencies should consider their need for the continued use of USBs, particularly given the availability of secure file sharing platforms, against their appetite for the risk of potential misuse of USBs. All public sector agencies should consider what controls are required to protect against, and mitigate the risk of, the misuse of USBs in their agency.

Recommendations

[42] The Commission considers that the wording of Finance's confidentiality agreement and the lack of any reminders about post-employment confidentiality obligations are serious misconduct risks.

[43] The Commission **recommends** that:

a. Finance review and enhance its confidentiality agreement to make it abundantly clear that employees are required to maintain

[33] Witness 2 transcript, private examination, 16 July 2024, p.10.
[34] Witness 2 transcript, private examination, 16 July 2024, p.19.
[35] 00940-2023-0181 - FAQ - Secure USB Drives.

confidentiality and abide by the non-disclosure requirements of official information acquired in the course of their duties, as set out in the Code of Conduct.

b. Finance consider implementing a procedure by which departing staff are reminded of their obligation not to disclose any confidential information once they leave.

[44] As indicated, Finance has accepted the recommendations. However, the recommendations may be considered more widely to all Government agencies that deal with confidential material.

CONCLUSION

[45] The allegation of serious misconduct in this matter concerns a long-serving senior public officer who downloaded 591 documents from Finance's computer system to a USB after resigning from Finance and prior to taking up a position in the private sector. Some documents contained highly sensitive Government information, which the Officer accepted he knew should be treated confidentially.

[46] The Officer told the Commission that he downloaded the documents for the purpose of giving them to the person who was taking over his role.

[47] The Commission's opinion is that, on the balance of probabilities, the explanation the Officer gave for downloading the documents is implausible. However, the Commission has been unable to establish that the Officer acted otherwise than in accordance with his authorisation to access and deal with the documents for a purpose related to his role. For this reason, the Commission has not made a finding of serious misconduct against the Officer.

[48] However, the Commission has identified the following serious misconduct risks arising from the circumstances in which the Officer's conduct occurred:

a. the use of USBs without appropriate controls;

b. the wording of the confidentiality agreement that all Finance employees are required to sign; and

c. the lack of any reminders by Finance to departing employees about ongoing confidentiality obligations.

[49] The Commission acknowledges that Finance has implemented stricter controls over confidential material and fully cooperated with the Commission's investigation.