Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Guidance on Employee Departure or Transfer

Published: 2024-07-22

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT48-47/2024E-PDF
ISBN: 978-0-660-73507-8

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Orientation concernant le départ et la mutation des employés

Guidance on Employee Departure or Transfer

Issue

Departing employees often leave behind vast amounts of information, in both physical and digital formats, without ensuring the proper disposal of it or without transferring it to an appropriate steward. This practice can lead to a loss of information.

Note: In this document, “employee” means anyone working for the Government of Canada (GC), including casual employees, temporary help, consultants and contractors. “Departures” may be permanent (for example, leaving the public service or transferring to a new department) or temporary (for example, extended leave, secondment, parental leave or language training). This guidance applies to both permanent and temporary departures.

Context

This guidance provides information management (IM) best practices for departing employees in support of section 4.3 of the *Directive on Service and Digital*.

All information assets created or acquired during the course of employment with the GC, regardless of format or medium, belong to the Crown.

Departing employees are responsible for ensuring that any information of business value they have created, collected and stored in the course of their work is organized, categorized, disposed of or stored in the appropriate repository for continued use and management after their departure.

It is the responsibility of each employee to determine:

- what information is of business value and to safeguard it
- what information is transitory and to discard it

Additional guidance is available in Appendix E of the *Guideline on Service and Digital* to assist with this decision-making process.

Guidance for employees

Employees and managers should follow their department's departure procedures. In order to ensure that all activities have been completed prior to departure, employees and managers are encouraged to use the checklists provided in Appendix A and Appendix B of this guidance. In the absence of formal procedures, departing employees are to implement the following best practices.

1. Review email accounts (inbox, sent, deleted and personal folders) (see section 1 of Appendix A):

- Information of business value must be transferred to a corporate repository.
- Transitory information must be deleted.
- When departing employees have an "@canada.ca" email address, personal information such as resumés and contact lists may be left in the email account when they are transferring to another department with "@canada.ca" email addresses. See *Guidance on Email Management for Employees* for more information. In all other instances, personal information must be deleted.

2. Review the information holdings stored on the following (see section 2 of Appendix A):

- computer hard drives
- personal and shared network directories
- CDs, USB keys, portable hard drives and other removable storage media
- mobile devices, including instant messages
- any other networks the departing employee may have used

In accordance with the *Policy on Service and Digital*, any material that contains information of business value must be saved to a corporate repository that is accessible to other employees of the department and assigned appropriate access rights, notably considering the information's security categorization and other employees' need for access.

Digital material that contains transitory information or personal information (for example, photos, resumés) should be deleted.

All personal digital storage locations (for example, personal drives, hard drives) should be emptied.

3. Review all storage space at your onsite work location (for example, file cabinets, bookshelves, desks, and other authorized secure physical storage devices). Physical records that contain information of business value must be retained for ongoing operations and transferred to a manager or designate, or sent to the department's corporate records management unit for long-term management. Physical records identified as transitory information should be disposed of (see section 3 of Appendix A).

4. Departing employees may want to take copies of certain information with them. Examples of such information are:

- their digital contact list
- their digital calendar
- personal email messages and personal information

If there is doubt about what information can be released to a departing employee, managers should consult their department's IM specialists.

5. In cases where an employee leaves suddenly and cannot organize, file and clean out information holdings, responsibility for those tasks falls to the employee's manager and should be carried out within 15 days.

Guidance for departments

1. As part of formal departure procedures, departments should include an attestation from employees stating they have transferred all information of business value from their email account to a corporate repository.

2. Departments should ensure that employees are aware of their IM responsibilities prior to departure. Best practices for employees have been incorporated into the checklists in Appendix A.

3. Departments should ensure that managers are aware of their IM responsibilities in relation to departing employees. In particular, departments should ensure that managers are aware that in cases where an employee leaves suddenly and cannot organize, file and clean out information holdings, responsibility for those tasks fall to them to complete within 15 days. Best practices for managers have been incorporated into the checklists in Appendix B.

4. Departments should ensure that dormant and deactivated email accounts from departing employees are managed effectively, including the transfer of information of business value to a corporate repository and the appropriate disposition of that information. Deactivated accounts should be deleted as soon as possible once all information of business value has been transferred to a corporate repository.

Further information

A departure checklist for employees is available in Appendix A. Appendix B includes a checklist for managers to complete upon an employee's departure or transfer.

Office of the Chief Information Officer
Treasury Board of Canada Secretariat
Email: ServiceDigital-ServicesNumerique@tbs-sct.gc.ca
Toll-free: 1-877-636-0656
TTY: 613-369-9371 (Treasury Board of Canada Secretariat)

Appendix A: Information Management Checklist for Employees

Before you leave, you should do the following:

1. Information in digital formats

- Review all digital storage locations (for example, local drives, network directories, USB keys, cloud storage, mobile devices and other networks you may have used).
- Ensure that all information of business value (documents, email, instant messages, datasets, maps, photographs, videos and so on) are transferred to an appropriate corporate repository.
- Ensure that access rights are appropriately assigned for all documents in the corporate repository.
- Assign a trustee for continued management of documents transferred to the corporate repository and ensure that the trustee has appropriate permissions to access the documents being transferred. See your manager for direction on choosing a trustee.
- Provide information about everything you leave, explaining why it will be needed.

- Remove password protection on digital information or give your passwords to your manager.
- Delete transitory information.
- Remove all personal information (for example, resumés, contact lists).
- Obtain approval for all information that you want to take with you.
- Empty all personal digital storage locations.
- Confirm cleanup of your digital information with your manager.

Email

- Review all email folders (for example, inbox, sent, deleted and personal folders) and email archives (for example, personal storage folders).
- Transfer all email messages that contain information of business value to a corporate repository.
- Delete transitory email messages.
- Cancel or forward subscriptions and request to have your name removed from distribution lists.
- Confirm cleanup of your email account with your manager to ensure that no departmental information remains in your email account.

2. Information in physical formats

- Review all authorized secure physical storage devices (for example, filing cabinets) and physical documents.
- Transcribe any information of business value contained in your diaries or notebooks and place it into an appropriate corporate repository.
- Ensure that all information of business value (documents, books, maps, photographs and so on) for ongoing operations are transferred to your supervising manager or designate for continued management.
- Dispose of all transitory information.
- Remove all personal information (for example, resumés, photos) from your onsite work location.
- Obtain approval for all information that you want to take with you.

- Return all material borrowed from departmental libraries or from the Records Management Unit.

Appendix B: Information Checklist for Managers

Before an employee's departure (or immediately following an unexpected departure), managers should ensure that the following activities have been completed.

Ensure that employees are aware of their IM responsibilities prior to departure.

1. Information in digital formats

- Confirm that all information stored on digital devices (for example, local drives, network directories, USB keys, cloud storage, mobile devices and other networks the employee may have used) has been reviewed.
- Confirm that all information of business value has been transferred to an appropriate corporate repository.
- Confirm that the employee has provided information about everything they leave for their successor, explaining why it will be needed.
- Confirm that access rights have been appropriately assigned for all of the employee's digital documents in the corporate repository.
- Confirm that a trustee has been assigned for continued management of the employee's digital documents in the corporate repository.
- Confirm that all transitory information has been deleted.
- Review and approve any information that the employee wants to retain.
- Confirm that all personal digital storage locations have been emptied.

Email

- Confirm that all information in the employee's email folders (for example, inbox, sent, deleted, personal and archive folders) has been

reviewed.
- Confirm that all email messages that contain information of business value have been transferred to a corporate repository.
- Confirm that all transitory email messages have been deleted.
- Confirm that the employee’s name has been removed from any distribution lists.
- Review and approve the employee’s retention of any information remaining in the email account (for example, personal email messages, contact lists).

2. Information in physical formats

- Confirm that all of the employee’s physical documents have been reviewed.
- Confirm that any information of business value contained in the employee’s diaries or notebooks has been transcribed and placed into a corporate repository.
- Confirm that all information of business value for ongoing operations has been transferred to the manager or designate for continued management.
- Confirm that all transitory information has been disposed of.
- Review and approve information that the employee wants to retain.

[ISBN: 978-0-660-73507-8]

Date modified:
2024-07-26