Summary of the Privacy Impact Assessment for Public Posting

April 24, 2025

1. Title of the Program

Expense claim management and administration software system for DC employees and temporary workers provided by the Emburse Chrome River platform (the "**Program**").

2. Description

The Program involves the use of the Emburse Chrome River online cloud-based platform and mobile application (the "**Platform**") that is owned and operated by Emburse, Inc.. The Platform facilitates the submission, review, tracking, and reimbursement of expense claims by the Data Subjects within Canada and internationally.

The Platform collects, uses, discloses, and retains certain personal information about DC employees and temporary workers (collectively, the "**Data Subjects**") to facilitate the submission, review, tracking, and reimbursement of expense claims by DC, namely:

- *Basic Information:* name (first, middle, last, and preferred), personal contact information (email and home address).
- *Sensitive Information:* signature (if included on a submitted receipt), physical attributes (height, weight, disability if needed for travel or accommodation purposes), and driver's license number.
- *Financial Information:* bank account information and the last four digits of credit card numbers (only if included on an employee submitted receipt).
- *Work Information:* employee ID numbers, position / title, business unit, direct reports and delegates, length and reasons for leave (ex: parental leave), email address, phone number, and office location.

(collectively, the "**PII**")

The Program, including implementation of the Platform, is already complete and is in use by DC.

3. Why a Privacy Impact Assessment was Completed

Pursuant to the Treasury Board Secretariat Policy on Privacy Protection and the *Privacy Act*, RSC 1985, c P-21, DC is required to complete a privacy impact assessment for this Program (a "**PIA**") as personal information is collected, used, stored, and disclosed pursuant to the Program.

4. Additional Information

Risk No.	Risk Description	Affected Privacy Principle(s)	Risk Level	Mitigation Measures
1.	DC cannot control what PII the Data Subjects submit given the autonomy Data Subjects have over the type and sensitivity of PII they input into the Platform.	Limiting Collection	Medium	*Mitigation:* Add to Platform a caution about uploading sensitive PII into the Platform (ex: credit card numbers, identification numbers, etc.) *Responsible Party:* DC *Target Completion Date:* Q4 2025
2.	Lack of documented employee privacy training procedures increases risk of a privacy breach.	Safeguards	Medium	*Mitigation:* Document employee privacy training. *Responsible Party:* DC *Target Completion Date: Q4 2025*
3.	Limited audit trail functionality which would have to be supplemented by manual processes.	Safeguards	Low	*Mitigation:* Ensure strong privacy protocols, training, and monitoring of use to limit unauthorized access and regular tracking of disclosures to ensure all disclosures are permitted and recorded. *Responsible Party:* DC *Target Completion Date:* Q1 2026 and ongoing
4.	PII will be accidentally mismatched, resulting in the reimbursement of the wrong Data Subject.	Limiting Disclosure	Low	*Mitigation:* Ensure regular monitoring and auditing of reimbursements to ensure that payments go to the right Data Subjects and to identify and remedy mismatches as soon as possible. *Responsible Party:* DC *Target Completion Date:* Ongoing with planned start date of Q1 2026.
5.	Private third-party access to the Data Subject's PII.	Accountability Limiting Collection Limiting Disclosure	Low	*Mitigation:* Conduct due diligence and security assessments on service providers and prepare PIA, ensure adequate contractual protections. *Responsible Party:* DC *Target Completion Date:* Complete

Risk No.	Risk Description	Affected Privacy Principle(s)	Risk Level	Mitigation Measures
6.	Using Delegates means more people are involved and creates added risk of breach or loss.	Limiting Collection	Low	*Mitigation:* Ensure Delegates are trained in their roles and only use Delegates where the pre-existing working relationship exists between a Delegate and Data Subject. *Responsible Party:* DC *Target Completion Date:* Q1 2026
7.	There is no just-in-time Privacy Notice on the Platform.	Limiting Collection	Low	*Mitigation:* Add acknowledgement of the DC Employee Privacy Policy as part of the caution about inputting sensitive PII into the Platform to be developed in response to Risk #1. *Responsible Party:* DC *Target Completion Date:* Q4 2025
8.	PII will be lost or mis-linked during the transfer from the Platform to SAP ByDesign.	Limiting Use	Low	*Mitigation:* Ensure regular auditing and maintenance of the digital automated export import data transfer process to ensure continued accuracy and no bugs. *Responsible Party:* DC *Target Completion Date:* Ongoing

5. Related Personal Information Banks (PIBs)

The relevant PIBs are as follows:

- PSU 931/PRN 914/RDA 99/004 Accounts Payable
- PRN 914 Financial Management

No additional PIBs need to be created for this PIA.

6. For More Information about this Privacy Impact Assessment

For more information about this PIA, please contact:

Delegated Privacy Official:	Margot Spence Executive Director, Legal and Chief Privacy Officer spence.margot@destinationcanada.com