ELECTRONIC MONITORING POLICY

ADP Canada Co. ("ADP") uses technological resources, including the internet, in its daily operations and values transparency with its associates regarding its electronic monitoring practices. This Electronic Monitoring Policy ("Policy") explains the circumstances under which ADP may engage in electronic monitoring (including the types of devices that may be monitored), and the purposes for which information collected through electronic monitoring may be used by the company. This Policy supplements information provided in the GSO Secure Communications Standard.

1. Scope

This Policy applies to all associates, full-time or part-time, regardless of position, as well as temporary workers, independent contractors and consultants who are assigned to perform work for ADP in Ontario. For purposes of this Policy only, all such users of ADP's electronic systems are referred to as associates.

2. Monitoring of Electronic Systems

ADP provides electronic systems to facilitate ADP's business. Because of the nature of its business, ADP handles sensitive information which includes personal, financial, tax, payroll and benefits administration information. ADP takes its obligations to protect sensitive information seriously, and stringently monitors its electronic resources to ensure proper use and prevent data security issues. **Associates should not expect privacy when using company-provided devices and/or communication and information systems, nor when engaging in publicly-accessible online activities.**

3. Data Collected from ADP Electronic Systems

ADP engages in electronic monitoring of employees, including as follows:

- **Card/Key Entry Access** – ADP collects information regarding personnel use of key cards or other physical security devices to provide access to ADP facilities, elevators, floors and areas with keyed access.

- **Continuous Video Surveillance** – such surveillance is used throughout ADP offices, including at main entry/exit points, hallways, loading docks, parking lots and decks, and other workplace sensitive areas (but not in private locations, such as individual offices or restrooms).

- **Telephone Use and Voicemail** – ADP collects information regarding inbound and outbound calls made by personnel and their duration. Voicemail is accessed and reviewed by authorized ADP personnel as needed for the purposes described below. Certain types of calls are recorded or monitored in real time, subject to additional notices provided to you for the applicable situations (for example, customer service calls or internal training calls).

- **Email and Work Calendars** – Authorized ADP personnel access and review emails or calendars as needed for the purposes described below.

- **Instant Messaging Applications –** ADP reviews the use and content of any instant messaging applications or services and any company forum as needed for the purposes described below.

- **Use of Documents and Data** – ADP reviews records of access to and actions taken on documents, files and other data on network shares, databases, applications, ADP cloud resources, collaboration tools, or other repositories as needed for the purposes described below.

- **Internet Use** – ADP collects information regarding sites visited, time and duration of visit, and volume of data transferred to or from the site, and specific files transferred.

- **Network and Remote Access** – ADP collects date, time, and location of network login, count and duration of remote connections, and access to network resources.

- **Downloads** – ADP collects the details of files and downloads of data from network resources to local devices.

- **Data Loss Prevention (DLP)** – To safeguard the confidentiality and integrity of ADP and client information, ADP uses a DLP solution that monitors and blocks specific activities involving certain types of sensitive data (e.g., Social Insurance numbers, T-4 Employer Identification Numbers, credit or debit card numbers, or bank account numbers) on ADP-issued systems, including (a) saving such data to portable media, (b) printing documents containing such data, (c) emailing such data to recipients outside ADP, and (d) transmitting such data outside ADP's systems and networks.

- **Public Online Activity** - ADP may review associates' publicly-accessible activities and interactions online, including publicly visible activities on social media platforms and forums as needed for the purposes described below.

Collected information may be reviewed and used as needed, for purposes including: determining compliance with ADPs policies; conducting investigations, audits or compliance reviews; managing performance; complying with ADP's legal obligations, including in litigation matters and in response to lawful requests from government agencies; exercising or defending a legal claim; responding to a client need; maintaining business continuity; locating information; determining proper utilization and resource allocation, including collecting usage, traffic, and response statistics; maintaining data security; investigating and fixing IT problems; managing emergency, workplace safety and security, and crisis situations; or for any other business purpose, consistent with applicable law.

In certain situations, ADP may engage in forms of electronic monitoring other than those outlined above or for purposes not listed above, in accordance with applicable privacy laws. For example, ADP may need to monitor other associate activities, including without advance notice, in order to comply with third party contractual obligations regarding data security.

4. Greater Legislated Right Prevails

If any applicable legislation confers a greater right or benefit than this policy with respect to the matters described herein, the legislation will apply.

5. Prohibited Behaviour

Associates must not attempt to interfere with, circumvent, or otherwise misuse the electronic monitoring implemented by ADP. Doing so will result in discipline, up to and including termination of employment or assignment (including for cause). Retaliation against an individual who, in good faith, reports a concern in accordance with this Policy is strictly prohibited.

6. Questions

ADP encourages all associates to discuss questions or concerns regarding this Policy with their manager or Human Resources Business Partner.