b

IT129   
Employee Monitoring Policy

|  |  |
| --- | --- |
| Status | Final |
| Version | 1.00 |
| Classification | Confidential |
| Owner | Razvan Anghelidi, Directory of IT |
| Address | 1705 Tech Avenue, Unit 3, Mississauga, ON, L4W 0A2, Canada |

*Statement of Confidentiality: This document and supporting materials contain confidential and proprietary business information of Signifi Solutions Inc. These materials may be printed or photocopied for use internally and must not be shared with other parties.*

[Document Control iii](#_Toc61981394)

[Audience 4](#_Toc61981395)

[Scope 4](#_Toc61981396)

[Policy Statement 4](#_Toc61981397)

[Scope 5](#_Toc61981398)

[Compliance 13](#_Toc61981399)

[Enforcement 13](#_Toc61981401)

[Update 13](#_Toc61981402)

[Revision History 13](#_Toc61981403)

All rights reserved

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of Signifi Solutions Inc. (from now on, Signifi). The information contained in this document is proprietary to Signifi and may not be used or disclosed except as expressly authorized in writing by Signifi.

Trademarks

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Document Control

The electronic version of this document is recognized as the only valid version.

Approval History

|  |  |  |
| --- | --- | --- |
| APPROVER(S) | TITLE/DEPARTMENT | APPROVED DATE |
| Shamira Jaffer | CEO | October 7th, 2022 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Document Sensitivity Level

Confidential

Audience

This policy covers all individuals working at all levels and grades, including senior managers, officers, directors, employees, consultants, contractors, trainees, associates, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as employees or staff in this policy) that reside in Ontario, Canada.

Scope

All staff are expected to always comply with this policy to protect the privacy, confidentiality, and interests of our company and our services, employees, partners, and customers.

Policy Statement

This Policy identifies the circumstances in which Signifi engages or may engage in electronic monitoring of employees, directly or indirectly, and the purposes for which the information obtained through the electronic monitoring may be used.

Background

Amendments to the Employment Standards Act, 2000, require all Ontario employers with over 25 employees, to prepare a written policy concerning electronic monitoring of employees and to provide a copy of that policy to all employees.

The Policy must outline the following:

* if, how, and in what circumstances electronic monitoring occurs;
* the purposes for which information obtained through electronic monitoring may be used; and
* the date the policy was prepared and the date of any changes made.

The amendments do not establish a right for employees not to be electronically monitored, nor create any new privacy rights for employees.

Definitions

Electronic Monitoring: includes all forms of monitoring of employees that is done electronically throughout the workplace, directly or indirectly, whether continuously, episodically, or on an as needed basis.

Electronic Monitoring at Signifi

Computing and access resources are provided to certain Signifi employees to perform their duties. Signifi reserves the right to electronically monitor employees, directly or indirectly, at its discretion. Employees should not expect absolute privacy in relation to their use of Signifi resources and should not assume that any use of Signifi resources is exempt from electronic monitoring in accordance with this policy.

As of the date of this Policy, electronic monitoring may be performed directly or indirectly, whether continuously, episodically, or on an as needed basis, through the following assets, systems, services, equipment, and devices:

* Office/Microsoft 365 including all their components
* Drive/storage contents of the Signifi computing devices
* Teams, Zoom video conference
* Coro Security Software
* DocuSign software
* Email
* Endpoint Central IT management software
* ScreenConnect remote desktop software
* Software and internet usage
* Firewalls, switches and other network devices
* Freshdesk and JIRA ticketing systems
* Badge access system
* Other third-party systems like accounting, HR
* CCTV/NVR video recording
* Photocopier
* Phone system
* QuickBase asset management system
* Social media accounts belonging to Signifi
* Windows logs

This list is not exhaustive and may be updated as policies, practices, and procedures change, or as assets, systems, services, equipment, and devices are upgraded or replaced.

How Obtained Information May Be Used

Information obtained through electronic monitoring may be used for all purposes consistent with Signifi’s responsibilities as a business, and any Signifi policy, practice, or procedure.

Such purposes include but are not limited to Signifi performing the duties it was contracted for by its clients, to employee safety, to protection and security of the Signifi’s data, resources and assets, monitoring employee compliance with applicable policies and procedures, and complaint response.

Other purposes may include:

* Workforce management
* Operational auditing, monitoring, and reporting
* Health and safety monitoring
* WSIB or Ministry of Labour investigations
* Coaching and quality improvement
* Labour Relations-related investigations
* Privacy complaints, monitoring, and auditing
* Security incidents, including workplace violence, thefts, vandalism, and threats
* IT or HR related investigations
* Regulatory reporting
* Data review and pattern monitoring
* Resolving technical issues
* As evidence for forensic investigations on behalf of Signifi or an authorized third party such as law enforcement agencies or other government bodies
* Responding to data privacy requests, litigation-related requests, or otherwise as required by law.

Information obtained by Signifi through electronic monitoring shall be collected, maintained, and dispersed in accordance with Signifi’s responsibilities as a business, and any policy, practice, or procedure.

Related Policies and Procedures

This Policy is to be read, implemented, and interpreted with other related policies and procedures, including but not limited to:

* IT100 Acceptable Use Policy
* IT125 Social Media Policy
* IT103 Information Security Policy
* IT104 Access Control Policy
* IT110 Confidentiality Policy
* IT119 - Physical Security Policy
* HR101 Misconduct Policy
* HR102 Record Checks Policy
* HR103 Employee Handbook

Compliance

This policy will be officially monitored for compliance by the IT department director and may include random and scheduled inspections.

Enforcement

All instances of non-compliance will be reviewed by the employee’s department director. The department director, with the assistance of the Human Resources department, has the authority to impose disciplinary actions, up to and including termination of employment or contractual agreement.

Update

This policy and all supporting documentation will be reviewed and updated annually or upon material changes to Signifi business rules, technology processes, organizational goals, or information security objectives to ensure its continuing suitability, adequacy, and effectiveness.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| VERSION | DATE | SUMMARY OF CHANGE | CHANGED BY |
| 1.0 | 2022-10-04 | First version | Razvan Anghelidi |
|  |  |  |  |
|  |  |  |  |