Use of Digital Monitoring Technology in the Workplace Policy

PURPOSE

[Company Name] (“the Company”) is committed to balancing workplace efficiency, security, and privacy. The purpose of this Policy is to outline how digital monitoring technology (e.g., computer activity logs, video surveillance, email monitoring, access control systems) is used within the workplace, the circumstances under which monitoring may occur, and the safeguards employed to protect employees’ privacy and personal information.

SCOPE

This Policy applies to all full-time, part-time, contract, and casual employees of the Company who are covered by the relevant privacy, employment, and data protection legislation in their province/territory of work or by federal laws if they are federally regulated. It also applies to contractors, visitors, or anyone who accesses the Company’s premises, networks, or computer systems. In the event of a conflict between this Policy and local legislation, the greater right or benefit to the individual will apply.

DEFINITIONS

- **“Digital Monitoring Technology”**: Any system or tool used to collect, analyze, or record electronic data about user activity, such as keystroke monitoring, email filtering, video surveillance, or network access logs.
- **“Personal Information”**: Any information about an identifiable individual that’s subject to privacy laws (e.g., PIPEDA or equivalent provincial legislation).
- **“Legitimate Business Purpose”**: A valid reason for collecting or monitoring data that furthers the Company’s operational, security, or compliance needs, as permitted by law.

ELIGIBILITY

All employees, contractors, and other authorized users of the Company’s systems or premises are subject to this Policy regarding digital monitoring activities. By accessing or using the Company’s equipment or networks, individuals acknowledge the

Company’s right to conduct lawful monitoring.

LENGTH OF LEAVE
Not Applicable. This Policy addresses technology use and monitoring rather than a leave of absence.

APPLICATION & NOTICE REQUIREMENTS

1. **Notification of Monitoring:**

- The Company will inform employees and authorized users in writing (e.g., upon hire or through periodic reminders) that their activities on Company-owned devices, networks, or premises may be monitored for legitimate business purposes.
- Signage may be posted where video surveillance is used, in accordance with local privacy and/or employment standards legislation.

1. **Scope and Purpose of Monitoring:**

- Monitoring will only be conducted to the extent necessary for security, performance, compliance, or other legitimate business purposes (e.g., preventing unauthorized access, investigating misconduct, protecting confidential information).
- Monitoring methods may include—but are not limited to—video surveillance, access card logs, network traffic analysis, and email or file access logs.

1. **Restrictions and Privacy Protections:**

- The Company will not collect more personal information than is required for the stated purpose.
- Wherever practicable, personal information gathered through monitoring will be minimized, de-identified, or aggregated to reduce privacy impacts.

JOB PROTECTION

Employees will not be penalized or terminated solely for raising concerns about privacy or the use of monitoring technology in good faith. The Company will investigate any such concerns and address them in accordance with applicable law and this Policy.

CONTINUATION OF BENEFITS

Not Applicable. This Policy does not address employee benefits or compensation.

RETURN TO WORK

Not Applicable. This Policy concerns digital monitoring, not a leave or return process.

CONFIDENTIALITY

All data collected through digital monitoring will be stored securely and accessed only by those with a legitimate need to know (e.g., IT administrators, investigators, or designated management personnel). The Company will handle any personal information collected in accordance with applicable privacy laws, ensuring it is protected from unauthorized access, use, or disclosure.

NON-RETALIATION

The Company strictly prohibits retaliation against any individual who, in good faith, questions or challenges the Company’s monitoring practices, reports a potential breach of privacy, or exercises legal rights regarding personal information. No employee’s job status, benefits, or opportunities will be jeopardized by raising such concerns.

POLICY ADMINISTRATION

The [HR Department/Designated Manager/Privacy Officer] is responsible for:
• Administering this Policy consistently.
• Ensuring the Company’s monitoring practices comply with applicable privacy and employment laws.
• Staying informed about legislative changes and updating the Policy accordingly.
• Handling questions or complaints about monitoring practices or data handling.

[Company Name]
Effective Date: [Insert Date]
Authorized by: [Name, Title]
Date: [Signature Date]

How to Use This Template

1. **Adapt and Customize:** Tailor this Policy to the specific forms of digital monitoring technology in use at your organization, considering local legal requirements for notification, consent, and data protection.
2. **Review with Legal Counsel:** Confirm that the Policy aligns with applicable employment standards, privacy legislation (e.g., PIPEDA, provincial privacy acts, or the Privacy Act if federally regulated), and data protection laws.
3. **Communicate to Employees:** Publish the final Policy (e.g., in an employee handbook, on the intranet, via email), conduct training if necessary, and require employees to acknowledge their understanding of the Company’s monitoring practices.

Table of Jurisdictional Differences

Legislation governing workplace privacy and monitoring varies across provinces/territories and federally regulated sectors. Always consult the most recent privacy, data protection, and employment standards laws for precise requirements.