| **Effective Date:** | **Version Number:** | **Last Revised:** |
| --- | --- | --- |
|  |  |  |

## Purpose of the Workplace Monitoring Policy

**[ORGANIZATION]** (the “Company”)is committed to maintaining a transparent and fair workplace. Through this Workplace Monitoring Policy (“Workplace Privacy Policy”) **[ORGANIZATION]** will communicate the organization’s intent to monitor its employees, provide information about the categories of data collected, inform employees about how their data will be secured and used, and clarify workplace privacy expectations when using organization IT assets.

This policy contains references to the policies, procedures, and practices that will be followed by **[ORGANIZATION],** its representatives, and any of its present or future subsidiaries when collecting, using, or disclosing the personal information of an identifiable individual that is a present, future, or former employee of **[ORGANIZATION].**

**This Workplace Monitoring Policy constitutes a notification in accordance with [PRIVACY LEGISLATION]. By acknowledging this policy, employees of [ORGANIZATION] consent to the workplace monitoring and surveillance practices outlined herein.**

### Definitions

#### Video Surveillance

“**Video Surveillance”** refers to surveillance by means of a camera that monitors or records visual images of activities on organization-owned property. Video surveillance does not include the capture of audio.

#### Computer Monitoring

**“Computer Monitoring”** refers to the practice of collecting user activity data on organization-owned computers, networks, and other IT infrastructure. This data includes, but is not limited to, web browsing history, files downloaded, data input, network traffic, logons to corporate systems, interactions with data, peripheral device usage, and information about the employee’s computer.

#### Employee

**“Employee”** collectively refers to any directors, officers, managers, employees, other representatives, and agents including consultants and independent contractors of **[ORGANIZATION].**

#### Data Collection

**“Data Collection”** refers to the automated or manual processing of employee data. This includes the collection, use, and storage of employee data such as computer activity data and other forms of personal information.

#### Personal Use

**“Personal Use”** refers to an employee using organization-owned devices, networks, and other assets for personal tasks such as non-work web browsing and sending personal emails.

#### Personal Information

**“Personal Information”** refers to any data collected about an identifiable individual. This includes obfuscated data that, when combined with other information, could identify the individual.

## Scope of This Workplace Monitoring Policy

This policy applies to any directors, officers, managers, employees, other representatives, and agents including consultants and independent contractors of **[ORGANIZATION],** where applicable by law.

### Policy Enforcement

Corrective actions with regards to violations of this policy are subject to **[ORGANIZATION]’s** disciplinary policies. Depending on the severity of the violation, corrective actions may include placement on an employee Performance Improvement Plan (“PIP”), legal action, or employee termination. For more information, please refer to **[OTHER POLICY]**

## Privacy Statement: Expectation of Privacy in the Workplace

This section will outline the privacy rights and expectations that employees of **[ORGANIZATION]** will have during their employment.

Monitoring employee computer usage is an essential part of enforcing policies, maintaining a respectful work environment, and ensuring that IT assets that are owned and managed by **[ORGANIZATION]** are used safely and appropriately.

For that reason, outside of the rights granted by **[PRIVACY LEGISLATION],** **employees must not expect privacy when using [ORGANIZATION] systems.** While all personal information collected by **[ORGANIZATION]** will be used fairly and appropriately as per this policy, all activities that take place via organization-owned IT assets should be considered monitored.

### Personal Use of Company Assets

**[ORGANIZATION]** recognizes that its employees may occasionally desire to use organization-owned systems for personal tasks during their normal course of business. This may include non-work web browsing, making personal phone calls, or sending emails from personal accounts.

Occasional personal use is permitted, however, to the fullest extent of the law **[ORGANIZATION]** reserves the right to monitor personal use of organization-owned assets to the same extent that it monitors business use. Employees must operate under the assumption that all traffic over organization-owned networks is monitored and conduct themselves accordingly.

All personal use of organization-owned equipment and systems must abide by **[ORGANIZATION]’s** Acceptable Use Policies.

### Personal Electronic Equipment

For employees who are permitted to use personal electronic equipment for work purposes (“Bring Your Own Device” or “BYOD”), **[ORGANIZATION]** will make every reasonable effort to not monitor the activities that take place on that device.

**Employees participating in the BYOD program will be monitored when accessing the organization’s IT infrastructure, cloud-based applications, and other resources.** For example, data collection will occur when personal electronic equipment is used on organization-owned wireless networks, virtual private networks (“VPN”), and any other interaction from personal electronic equipment with organization-owned IT systems.

**[ORGANIZATION]** reserves the right to inspect personal devices that are used by employees for work purposes if doing so is deemed necessary to maintain the security, confidentiality, and integrity of the organization, its systems, and the data that is in our custody.

**[ORGANIZATION]** reserves the right to remotely wipe all organization-owned data from personal electronic equipment. This will most commonly occur when a BYOD-eligible employee is no longer employed by **[ORGANIZATION]** or personal electronic equipment is lost or stolen.

For more information, please refer to **[BYOD POLICY OR OTHER RELATED POLICY].**

## Types Of Employee Monitoring Conducted and Their Purpose

### Video Surveillance

**Video surveillance** **equipment** is used on premises to ensure that employees, patrons, and organization-owned assets are kept secure from theft, vandalism, and other forms of misconduct. Should unlawful activity be discovered, the recordings captured by video surveillance equipment will be used to the fullest extent of the law—including the possibility of disclosure to authorized third parties.

Video surveillance equipment will not be used in areas where employees have a reasonable expectation of privacy, such as bathrooms, changing rooms, and other private areas. Where video surveillance equipment is used the equipment will be made clearly visible and there will be notices indicating the presence of the equipment.

### Computer Monitoring

**[ORGANIZATION]** monitors the network and computer activity of employees to ensure that organization-owned IT resources are used in accordance with our acceptable use policy (AUP), information security policy, and other policies where relevant.

Computer activity data may also be used to evaluate employee performance, detect malicious or high-risk activities, monitor network performance, and prevent security incidents from occurring.

#### CurrentWare Employee Computer Monitoring Software

**[ORGANIZATION]** computer systems are monitored and managed with security and computer monitoring software provided by CurrentWare Inc. As per [CurrentWare’s Terms of Service](https://www.currentware.com/terms-of-service/) **they will not have access to employee computer activity data** unless it is explicitly provided by **[ORGANIZATION]** for the purpose of troubleshooting the software.

### Telephone Monitoring

All organization-owned mobile and landline phones may be monitored to ensure appropriate usage and compliance with **[ORGANIZATION]’s** policies surrounding the use of telephony in the workplace. If a personal mobile device is used for work purposes, phone calls will not be monitored unless they are made through organization-provided mobile applications that are provided for the purpose of making work-related calls.

### Email Monitoring

All email communications that are sent through organization-owned networks, equipment, or user accounts are subject to monitoring. This may include personal email accounts when those accounts are accessed through organization-owned IT assets.

When sending personal emails using organization-owned systems employees must tag personal messages accordingly to indicate to authorized personnel that they must not be reviewed under the normal course of business.

### Prohibited Forms of Surveillance

To provide **[ORGANIZATION]** employees with a reasonable degree of privacy on organization-owned assets, the following forms of surveillance are strictly prohibited unless there are exceptional circumstances and a legitimate business reason to do so.

* Keylogging (recording individual keystrokes)
* Video monitoring in private spaces such as bathrooms
* Covert surveillance, such as monitoring computer activity without due notice
* Covert recording or streaming of webcam feeds

Should dire circumstances require that any of the aforementioned prohibited forms of surveillance be conducted, the surveillance will be done in accordance with the privacy requirements of **[PRIVACY LEGISLATION].**

## Employee Data Collection & Processing Practices

The following measures have been put in place by **[ORGANIZATION]** to ensure that workplace monitoring data, personal information, and other forms of sensitive data are adequately protected and explicitly used for their intended purpose.

### Applicable Data Privacy Laws

1. Describe your legal basis for processing the data
2. Describe your statutory obligations as per relevant data protection and privacy laws (GDPR, CCPA, PIPEDA, etc)

### Data Retention

To ensure that all personal information is only kept for as long as it is necessary to do so, all data that is captured as a result of workplace monitoring will be stored digitally on **[DATA STORAGE LOCATIONS]** up to a period of no greater than **[RETENTION PERIOD]**. Personal information will only be stored for a greater period of time under exceptional circumstances or as required by law.

### Categories of Data Collected

**The employee monitoring measures put in place capture the following data:**

* Timestamps of computer power states: Startup, shutdown, and sleep events
* Logons on organization computers, virtual machines, and other desktops
* Logs of peripheral devices used on a given endpoint, such as storage devices (USB, DVD/CD, Tape, SD Card, etc), wireless devices, communication ports, imaging devices, and mobile phones.
* File operations to portable storage devices (files copied, created, renamed, and/or deleted to/from these devices)
* Internet usage data including URLs/domains, pre-defined website content category, web page headers, search engine queries, timestamps, bandwidth consumption, and browsing time
* Application usage, including software downloads and time spent using each software
* Screenshots of activities on organization-owned workstations
* IP addresses and system information of client computers

### Purpose Limitation

The personal information that is collected through workplace monitoring shall only be used for the purpose for which it was collected. The purpose of data collection is outlined in this policy as well as **[OTHER RELEVANT POLICIES].**

**[ORGANIZATION]** will only use personal data for a new purpose if the new purpose is either compatible with the original purpose, an employee provides informed consent, or the organization has a clear obligation or function set out in law.

## Employee Data Security & Privacy Measures

### Data Security Practices

**[ORGANIZATION]** recognizes that employee computer activity data and other data collected through workplace monitoring may be sensitive in nature. For this reason, any personal information that is collected through workplace monitoring will be treated as personally identifiable information (PII) and secured according to the standards set out in **[INFORMATION SECURITY POLICY]** and **[PRIVACY/SECURITY LEGISLATION].**

### Data Breach Notifications

In the event that personal information is disclosed or made available to an unauthorized third party **[ORGANIZATION]** will follow the incident response plan dictated by **[INFORMATION SECURITY POLICY]** and **[PRIVACY/SECURITY LEGISLATION].**

### Who Has Access to Employee Data

Employee data is made available to a limited number of authorized representatives or third parties associated with **[ORGANIZATION].** All persons with access to employee information are required to comply with the confidentiality and security requirements dictated by **[INFORMATION SECURITY POLICY]** and **[PRIVACY/SECURITY LEGISLATION].**

In addition, all access to workplace monitoring data is restricted to an as-needed basis. Employee data will not be made available to managers unless the employee is their direct report and the data is required for a legitimate business reason.

#### Disclosure of Workplace Monitoring Data to Third Parties

Workplace monitoring data is only disclosed to third parties as is required by law or as needed to troubleshoot the workplace monitoring systems used by **[ORGANIZATION]** to monitor employees in the workplace**.** All third parties that are provided with access to workplace monitoring data are subject to equivalent confidentiality and security requirements to ensure that employee data is not misused or disclosed without authorization.

## Comments, Questions, or Concerns?

To ensure that workplace monitoring is done fairly and transparently, the organization has appointed internal representatives for our employees. If an employee does not feel comfortable disclosing their concerns internally they may also contact an external privacy officer or another third party representative.

**If you have any questions about this Workplace Monitoring Policy or concerns about how your personal information is managed, please contact one of the below entities.**

### Internal Contacts

* **[INTERNAL CONTACTS]**

### External Contacts

* **[EXTERNAL CONTACTS]**

## Policy Acknowledgement

**Please read the workplace monitoring policy carefully to ensure that you understand the policy and your responsibilities before signing this document.**

By signing this workplace monitoring policy I indicate that I have read and been informed about the content, requirements, and expectations of the policy. I acknowledge that I have received a copy of the workplace monitoring policy for my records and I agree to abide by the policy guidelines as a condition of my employment and my continuing employment at **[ORGANIZATION].**

I understand that if I have questions, at any time, regarding the workplace monitoring policy, I will consult the contacts that I have been provided.

| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| --- | --- | --- |
| **Employee Signature** | **Employee Printed Name** | **Date** |
|  |  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Witness Signature** | **Witness Printed Name** | **Date** |

# 

# About CurrentWare

**At CurrentWare, our mission is to help businesses stay productive and secure.** We achieve this through our commitment to providing user-friendly software solutions with high-quality customer service.

## Our Commitment to Data Privacy

**When you use CurrentWare products the data you collect remains solely in your control.** CurrentWare’s solutions are installed and managed by your organization. Your employee’s data cannot be accessed by CurrentWare. For more information please refer to our [Terms of Service.](https://currentware.com/terms-of-service)

## What CurrentWare’s Software Can Track

This section outlines the categories of data that CurrentWare’s computer monitoring software is capable of collecting when monitoring employees in the workplace. The data that is specifically captured by each solution depends on what tracking methods are enabled during deployment.

The CurrentWare Suite also includes an **Auto Delete Scheduler** to periodically cull URL, bandwidth, application, and peripheral device usage data. In addition to reducing storage requirements for the CurrentWare database that is managed by your organization, this is a valuable feature for automatically maintaining compliance with the data retention requirements of your organization.

*The information contained here is for reference purposes only and is current as of June 2021.* For the most up-to-date information on CurrentWare products, please refer to our [Release Notes](https://www.currentware.com/support/release-notes/) or contact your CurrentWare Account Executive.

### 

### [BrowseControl](https://www.currentware.com/browsecontrol/)

**Web Filtering Software**

* Logs of websites that have been blocked (optional feature for troubleshooting)

### [BrowseReporter](https://www.currentware.com/browsereporter/)

**Employee Computer Monitoring Software**

* Websites visited including URL, content category, timestamp, and browsing time
* Application usage tracking
* Bandwidth usage, including the source URL
* Remote screen capture, including screenshots
* Search engine queries
* IP address of client computer (disabled by default)

### [AccessPatrol](https://www.currentware.com/accesspatrol/)

**Device Control & Data Loss Prevention Software**

* Logs of inserted portable storage devices (USB, DVD/CD, Tape, SD Card, etc), scanners, webcams, printers, and mobile phones. | [Learn More](https://www.currentware.com/support/which-devices-can-i-control/)
* Logs of allowed vs denied peripheral devices
* File operations to portable storage devices (files copied, created, renamed, and/or deleted to/from these devices)

### [enPowerManager](https://www.currentware.com/enpowermanager/)

**Remote PC Power Management Software**

* Timestamps of computer power states: Startup, shutdown, and sleep events
* Timestamped logon and logoff events
* Duration of logons

**Disclaimer**

The contents of this policy are intended to convey general information only and not to provide legal advice or opinions. The contents should not be construed as legal advice. CurrentWare advises consultation with legal counsel and/or an attorney for advice and legal opinion on specific legal issues.

CurrentWare.com | 1-888-912-9619 | [info@currentware.com](mailto:info@currentware.com)

**Contact us today and sign up for a FREE 14-Day trial!**