

Workplace Surveillance Policy

V02 04/03/2021

SECTION 1 - PURPOSE AND CONTEXT

The purpose of this policy is to ensure that Pax Australia [Pax] complies with the requirements of the Workplace Surveillance Act 2005. The Act requires that employees be formally notified of any actions by Pax that would fall within the definition of 'surveillance'.

The Act deals with surveillance of employees by means of cameras, computers or tracking devices and requires that employees are notified as to the nature of that surveillance. The notice provided to employees must indicate:

The kind of surveillance to be carried out (camera, computer or tracking)

How the surveillance will be carried out

When the surveillance will start

Whether the surveillance will be continuous or intermittent

Whether the surveillance will be for a specified time or ongoing

Any surveillance type activity that is undertaken by Pax must be in accordance with the Act and specifically the notice provided to employees. Any surveillance outside the parameters of the notice is considered to be covert surveillance and must be authorised by a Magistrate.

SECTION 2 - DEFINITIONS

Under the Workplace Surveillance Act 2005, surveillance of an employee means surveillance of an employee by any of the following means:

camera surveillance, which is surveillance by means of a camera that monitors or records visual images of activities on premises or in any other place;

computer surveillance, which is surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of a computer or any IP based Smart Device or Smart Technology (including, but not limited to, the sending and receipt of emails and the accessing of Internet websites); a Smart device is an electronic device generally connected to other devices or networks via wireless protocols.

tracking surveillance, which is surveillance by means of an electronic device the primary purpose of which is to monitor or record geographical location or movement (such as a Global Positioning System tracking device).

SECTION 3 - POLICY STATEMENT

Pax is committed to meeting all statutory obligations under the Workplace Surveillance Act 2005.

Section 4 - Procedures of this policy details instances of activity by Pax that are covered by the surveillance provisions, being: a) camera surveillance; b) computer surveillance; and c) tracking surveillance.

Pax will also comply with the legal requirements of the Act where surveillance is prohibited. These are contained in Part 3 of the Act (sections 15 to 18) and cover:

a prohibition on surveillance in any change room, toilet facility, shower or other bathing facility at the workplace;

a prohibition on surveillance when the employee is not at work except in cases of computer surveillance where the employee is using equipment and/or resources supplied by Pax or connected to Pax network in

any way. i.e. If staff connect to Pax network via a private computer, or other network capable devices (including all IP based Smart Technology or MAC defined equipment), such surveillance shall be restricted to any traffic through Pax network only;

a prohibition on blocking the delivery of emails unless notice (prevented delivery notice) has been given to the employee or where the incoming communication is perceived to be spam or a threat to the security of Pax systems or contains potentially menacing, harassing or offensive material; and

a prohibition on preventing delivery of an email or access to a website merely because it has been sent by or on behalf of an industrial organisation of employees or an officer of such an organisation or contains information about industrial matters; and

the website or email contains information relating to industrial matters [within the meaning of the Industrial Relations Act 1996 (NSW)].

SECTION 4 - PROCEDURES

Individual staff are prohibited from undertaking surveillance in their workplace.

Where it is necessary to undertake new or additional workplace surveillance it will be in accordance with this policy and approved by the CEO, Site Manager and Human Resources Manager.

Responsibility for retrieval of 'video footage' acquired during the surveillance process upon an approved request lies with either Site Manager or HR Department.

When reviewing or retrieving any such 'video footage' this may be done in company of the appropriate Senior Manager for their input, reference or direction.

In absence of the Site Manager or HR personnel being available when a review/retrieval is required, with concurrence of the CEO or Operations Manager suitably trained Senior Managers may effect such requirement.

Any of the CEO, Site Manager or Human Resources Manager can authorise a person to analyse Computer activity or Computer Surveillance records obtained in accordance with this Policy, unless there is reasonable cause to suspect misconduct or serious misconduct.

Part A - Notification

Pax will provide written notification to staff of surveillance activities that occur within the business. Pax will also periodically remind staff of the surveillance activities and will refer staff to this policy.

Human Resources/Payroll will provide written notification of surveillance activities at Pax to all new employees before they commence. Such notification will also refer to this policy.

This Policy will be emailed to all employees who have or use a Pax email account. It will be handed to those employees who do not have Pax email accounts. It will be published on the Pax web site.

Part B - Camera Surveillance

Security & Safety Cameras

Pax operates surveillance cameras in and around our premises, both within and outside of buildings. This is for the purpose of ensuring safety and security of all employees and visitors to our premises and facilities. Camera footage may be accessed and used as evidence where an act (e.g. assault of a person, damage to facilities or infrastructure, unsafe working practice) has occurred that warrants investigation by Pax. Such records may also be required by law to be provided to other parties such as a court or to the police. As such extracts of Surveillance footage may be retained by the company for purpose of underpinning any circumstance that may warrant either defending or prosecuting in any legal action – security, safety or industrial relations based.

Cameras are not installed for purpose of reviewing incidents within company parking areas where people allege their vehicle has been damaged.

Please Do Not Request Access Of This Type, You Will Be Refused

This is not why these cameras are installed.

Pax does not employ any individual who has sole function of reviewing issues such as this as a component of their core function.

We do not, unless required for business, safety or security need review recordings. This is defined by legislation.

'Generic' employees are not authorised to review any footage taken.

Unless there is (or has been) a safety breach, a criminal act, an act that damages the facilities of the business, the integrity of the business or its business partners there is no access to footage within our system whatsoever.

Notices that Pax premises are monitored by cameras are located at all entrances to Pax and on noticeboards within the business. Security cameras are located in and around facilities requiring monitoring for the safety or security and individuals or property and are not disguised or secreted.

Security cameras are in place and functional (since 2015).

Camera security monitoring is continuous and ongoing

Portable Device Cameras

Cameras in mobile telephones, computers or tablets supplied by Pax are not to be used to record images of any persons without their knowledge or consent.

Part C - Computer Surveillance

General Use of Pax Technology [IT] Systems and Facilities

The policy applies to all employees, contractors, consultants and visitors who are given access to the computer systems and network facilities of Pax.

Use of Pax computers, our network and any associated systems are governed by the conditions under which an employee or any guest user has access provided to the IT facilities, services and systems.

Accordingly, the IT Manager, authorised staff of the IT department, or other authorised personnel may access Pax computers, computer logs and other system records, databases and backups to ensure the security, confidentiality, availability and integrity of all Pax IT systems.

Pax may use computer surveillance records for a documented and agreed purpose (such as assessing workload or operational factors).

Compliance and Breaches

Pax may commence applicable disciplinary procedures if a person to whom this policy applies breaches this policy (or any of its related procedures).

From time to time Pax may investigate alleged breaches of the law or Pax policies by employees or guests using its IT systems and facilities and this can involve accessing the employee's computer and electronic records. For employee's, such investigations may involve misconduct or serious misconduct and are managed in accordance with the provisions of the relevant employment agreement.

Surveillance purposes may also include, but are not limited to, employee compliance with work tasks, tracking of Pax property (against theft for example), assisting employees in utilising Pax network resources

while offsite, compliance with TGA Data Audit regulations, compliance with Pax policies and operational standards.

Computer surveillance may prevent, or cause to be prevented:
delivery of an email sent to or by an IT user
access to an internet website
access to software applications

Pax monitors employee use of Pax computers and IT systems in the following areas:

Any device connected to the Pax network, regardless of who owns the device.

Pertains to both wired and wireless connected devices.

Pax retains logs, backups and archives of computing activities, which may be audited. Such records are the property of Pax, are subject to State and Federal laws and may be used as evidence.

Monitoring may include, but is not limited to: storage volumes, download volumes, browsing/download history, access point to network, email use and content, web browser, screen, print output, device log on and log off times, microphone &/or camera use, environmental monitoring - including temperature, network configuration, network devices, IP based telephone logs. In addition any personal devices connected to the Pax system including but not limited to mobile phones, tablets, smart watches, and personal computers. Particular attention will be paid to potential breaches of the law (including intellectual property/copyright law) and suspected malicious code or viruses.

Any communication platform, existing or future, that uses network facilities.

What is ALWAYS collected during surveillance processes:

Employee emails, employee web browsing history, employee data storage, log on - log off times, files accessed on Pax network, print jobs sent to printers;

Login credentials when authenticating at the access point (user names, guest wifi token code);

DNS queries – specifically hostname resolutions to IP addresses;

IP reservations to MAC address (DHCP leases);

From employee devices – including private equipment - connected to the Pax network – employee emails, employee web browsing history, device unique address (MAC address), connection dates and times;

TGA Critical Devices – details of files created, accessed, changed or deleted.

Domain name component of HTTPS sites visited

What MAY BE collected during surveillance processes:

When offsite: temperature, battery status, geolocation, network configuration, network devices, programs accessed;

Also, employee performance issues (employee being notified) – screenshots;

When a device is lost or stolen – screenshots, webcam footage, microphone recordings, geolocation, network configuration, network devices.

What is NOT collected by Pax during surveillance processes:

Login credentials for websites - user names or passwords;

Browsing history of encrypted websites (https), neither intercepted nor collected.

Computer surveillance is intermittent but ongoing. It is in place as at the date of approval and promulgation of this policy.

Pax will conduct ongoing and intermittent computer surveillance for the purposes of:

protecting its assets, property and finances from suspected unlawful activity or activities which are in breach of Pax policy or Rules

its business and operational requirements

protecting its reputation

compliance with legislative requirements

meeting the expectations of its stakeholders and the general public
protecting the reputation and proprietary information of its Customers

Email and Internet

Email of all employees is not routinely read or monitored, but copies are retained for reasons of business security and integrity. However, any email sent or received from Pax issued equipment – from either internal or external location, and any email transmitted via the Pax network is deemed to be a record of Pax and these should be managed accordingly and will be accessible in that context. An email may also be the subject of a right to information request (under GIPA) or an application under privacy legislation.

Pax may access and monitor staff use of the Pax email and internet systems in the following ways:
Pax monitors email server performance and retains logs, backups and archives of emails sent and received through the Pax server(s). Even where the user has deleted an email, Pax may still retain archived and/or backup copies of the email. Only staff authorised by the CEO and IT Manager may examine such records. Pax retains logs, backups and archives of all internet access and network usage. These records may be audited, are subject to State and Federal laws and may be used as evidence.

While individual usage is not routinely monitored, unusual or high volume activities may warrant more detailed examination.

For the purposes of producing the email in response to a legal requirement or other lawful investigation.

For the purpose of determining, as part of an investigation by Pax whether there has been unacceptable use of email.

For the purpose of determining whether there has been a breach of any Pax policy in the use by an employee of Pax resources to access the internet.

For the purpose of investigating allegations of misconduct or to provide materials to external investigative authorities lawfully investigating possible criminal conduct.

Specific provisions related to access to email messages held on Pax servers are contained in the Email Policy.

Email and Internet surveillance is intermittent but ongoing. It is in place as at the date of approval and promulgation of this policy.

Part D - Tracking Surveillance

A tracking device means any electronic device capable of being used to determine or monitor the geographical location of a person or an object.

The purpose of such tracking devices is to maintain safety and security and not to monitor the location of staff.

Currently, for purpose of safety and security within the business operations, Pax does utilise a 'LiveLife Mobile Alarm' (mobility alarm). This is used for the purpose of monitoring safety and security of personnel when working alone.

This unit when used has both GPS and 'fall detection' capability.

The GPS function is 'enabled by the user' in event of a Safety issue and when enabled will specify the location of the person wearing the pendant to within 1 metre.

SECTION 5 - GUIDELINES

Devices in relation to which Pax monitors staff use include workstations, laptops – business supplied and private owned if connected to Pax network, servers, mobile devices including mobile phones, tablets, IP phones, smart watches, or other smart technology capable devices, email and network services, printers, network connected devices, and connections to internet services supplied by Pax (including fixed, Wi-Fi and 3G/4G/5G).

The term Pax network includes all contracted service providers and services we engage with that are hosted or accessed over the Internet. These services include, but are not limited to, any cloud based application or data repository utilised by Pax such as:

Email (Exchange Online, Mailguard)

Document storage (SharePoint, OneDrive)

Messaging (Skype for Business, Teams)

IP phone / SIP trunk provider

'Computer': by definition for purpose of this policy includes a device or part thereof that connects to the Pax network such as personal computer, mobile phone, desktop phone, mobile scanner, tablet computer, printer, server, network switch, wristwatch, company vehicle, measurement instrument, programmed logic controller.



Paul Curryer
Chief Executive Officer



Wes Pembroke
Site Manager