Monitoring Policy

What this policy covers

This policy applies to employees, workers and contractors. This policy sets out the Company's approach to monitoring and log monitoring and provides information relating to the types of monitoring used and the Company's obligations in relation to such monitoring and in introducing additional monitoring. Logging and monitoring are also essential information security controls to monitor for anomalous behaviours and potential information security incidents used to identify, prevent and respond to operational problems, security incidents, policy violations and fraudulent activity.

The Company's responsibilities

You should be aware that the Company may carry out monitoring of employees, workers and contractors. Monitoring may be necessary either to allow the Company to perform its contract with you or for the Company's own legitimate interests. The Company's reasons for monitoring include:

- security and the prevention and detection of crime
- ensuring appropriate use of the Company's telecommunications and computer systems
- ensuring compliance with regulatory requirements
- monitoring attendance, work and behaviour

Types of monitoring

The monitoring carried out may include (not limited to):

- monitoring of premises using CCTV cameras (both video and audio)
- monitoring e-mails and analysing e-mail traffic
- monitoring websites visited by staff using Company systems
- recording telephone calls and checking call logs
- monitoring systems for detecting security incidents or potential incidents
- logging, including but not limited to creation, access, modification and/or deletion activities
- monitoring the use of Company vehicles via vehicle-tracking systems
- entry and exit systems, including the use of biometric data such as fingerprints
- monitoring, including recording, of digital meeting systems used by staff
- tracking via mobile devices, computers, laptops or endpoint devices
- outbound and inbound network, system and application traffic
- access to systems, servers, networking equipment, monitoring systems, critical applications
- critical or admin level and network configuration fields
- logs from security tools and activities (i.e. antivirus, web filters, firewalls, data leakage, etc)
- unusual or abnormal systems behaviours and events (i.e., keystroke logins, deviations in use of standard protocols)
- unplanned termination of processes and applications,
- unusual user and system behaviour or unauthorised scanning of business applications

The Company may use information gathered through monitoring as the basis for disciplinary action. If disciplinary action results from information gathered through monitoring, you will be allowed to see or hear the relevant information before the disciplinary meeting.

The Company will ensure data collected through monitoring is processed in accordance with the Company's Data Protection Policy and data protection legislation and, in particular, it will be kept secure and access will be limited to authorised individuals. Monitoring may be used for any past events, in real-time or in period intervals, subject to organisational needs and capacities. Abnormal events will be communicated to the relevant parties as and when required to improve auditing, security evaluations, vulnerability and monitoring.

Covert monitoring

If the Company has reason to believe that certain employees, workers or contractors are engaged in criminal activity, the Company may use covert monitoring to investigate that suspicion.

In such instances, any monitoring will take place under the guidance of the police and will be carried out in accordance with Data Protection legislation.

Logging monitoring

Logs are one of the primary tools used by system administrators and management to detect and investigate attempted and successful unauthorized activity and to troubleshoot problems. Access to Interr's network, systems and communications shall be logged and monitored to also identify potential misuse of systems or information. Logging activities shall include regular monitoring of system access to prevent attempts at unauthorized access and confirm access control systems are effective. Log servers and any related log documents shall be kept secure and only made available to personnel authorized or their designee. These logs shall be kept as long as necessary or required for functional use or appropriate state regulation or law.

Information security monitoring is a proactive and ongoing process that involves the systematic observation, collection, analysis, and response to security events in order to protect an organization's information assets. Monitoring helps to detect and respond to security incidents, vulnerabilities, and policy violations.

Interr's information systems (servers, workstations, firewalls, routers, switches, communications equipment, etc.) shall be monitored and logged to (not limited to):

- Ensure use is authorized
- Manage, administer, and troubleshoot systems
- Protect against unauthorised access
- Verify security procedures and access
- Verify system and operational security
- Comply with Interr's policies and procedures
- Detect and prevent criminal or illegal activities
- Individual user access to systems and sensitive information
- All actions taken by any individual with administrative privileges
- Access to audit trails
- Invalid logical access attempts and failures
- Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with administrative privileges
- Initialization, stopping, or pausing of the audit logs
- Creation and deletion of system level objects

The logging of any monitoring data, events information, etc will managed in line with the Information Security Incident and Event Reporting Policy.

Additional monitoring

The Company reserves the right to introduce additional monitoring. Before doing so, the Company will:

- identify the purpose for which the monitoring is to be introduced
- ensure that the type and extent of monitoring is limited to what is necessary to achieve that purpose
- where appropriate, consult with affected staff in advance of introducing the monitoring
- weigh up the benefits that the monitoring is expected to achieve against the impact it may have on staff

The Company will ensure that you are aware of when, why and how monitoring is to take place and the standards they are expected to achieve.

Policy Review and Assessment

This policy may be amended by Interr at any time to take into account changes in legislation and best practice. This policy was last reviewed and agreed by the Board and seeks to be reviewed and updated annually. Any queries arising regarding this policy should be addressed to Mick Tabori.

Mick Tabori - CEO
January 2024