**Audit Logging and Monitoring Policy**

**Template**

This is an example policy. Please ensure you update this policy template so that it’s suitable for your organisation.

## Purpose

1. To address the regulatory requirements for safeguarding the confidentiality, integrity, and availability of information assets through auditing, logging, and monitoring activities.
2. To verify compliance with access controls and administrative and other safeguards developed and implemented to prevent or limit inappropriate access to data.
3. To ensure that routine and random audits are utilised as oversight tools for recording and examining access to information. For example, who accessed what data and when.

## Scope

This policy applies to all parties who access or use our information assets, regardless of physical location.

Information technology (IT) resources include all owned, licensed, leased, or managed hardware and software, and use of our network through a physical or wireless connection. This is regardless of the ownership of the computing device connected to the network.

This policy applies to:

* IT administered centrally
* personally-owned computing devices connected by wire or wirelessly to our network
* off-site computing devices that connect remotely to our network

## Policy

This policy aims to ensure that appropriate safeguards are in place and effective, <organisation> shall audit, log, and monitor access and events to detect, report, and guard against:

* network vulnerabilities and intrusions
* performance problems and flaws in applications
* security violations
* data loss
* unauthorized access to confidential data – including attorney-client privileged information
* breaches in confidentiality and security of confidential data
* degradation or loss of information integrity – such as improper alteration or destruction of confidential data

We’re committed to conducting business in compliance with all applicable laws, regulations and our own policies.

The following events may be audited:

* normal system events – such as start-up, shutdown, login attempts, errors, security policy changes, software installations
* information changes (create, read, update, delete) that include confidential data
* unauthorized access to confidential data for non-permitted purposes
* system management activities – including execution of privileged functions
* information exchanges containing confidential data
* activities relating to administration account(s)

## Audit Record Retention:

Audit records shall be retained and archived for a minimum of 7 years.

## Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the <role> and the <organisation>.

Policy exceptions must describe:

* the nature of the exception
* a reasonable explanation for why the policy exception is required
* any risks created by the policy exception
* evidence of approval by all appropriate parties

Review of this policy: this will be reviewed annually by the <role>.

Next review date: <date month year>