Artificial Intelligence Security Policy

Version Control

Version number	Date	Description of changes
V1.0	15 October 2025	Policy launch

Contents

ETL Artificial Intelligence Security Policy

1. Overview

1.1. It is the policy of ETL Systems Ltd to conduct all its business in compliance with our **Data Protection and Security requirements**. This policy defines these requirements in relation to use of Artificial Intelligence.

1.2. This policy sets user responsibilities in relation to AI tools and aims to ensure:

1.2.1. Data protection and information management processes are followed
1.2.2. User accountability for AI usage
1.2.3. Accuracy of information generated by AI tools
1.2.4. Transparency when using AI tools

2. Purpose

2.1. This policy establishes user responsibilities when using AI tools for ETL business. The policy aims to ensure that AI tools are used securely by outlining acceptable use of AI, the need to check accuracy of results, the need for transparency and user accountability for AI generated content. This policy also addresses the data protection responsibilities of users when using AI tools.

3. Who the policy applies to

3.1. The scope of this policy applies to:

3.1.1. All ETL employees (permanent and temporary), contractors, suppliers and third parties who use ETL systems' equipment and/or software licenced by ETL systems, referred to as "users" throughout this policy.

3.1.2. All AI tools

4. Definitions

Artificial Intelligence (AI):
A computer programme which "learns" from data and may perform tasks usually carried out by humans.
AI tool
Any computer software that uses artificial intelligence in its processing
Approved AI tools
AI tools that reside on ETL Systems' infrastructure and that have been approved by the Executive Leadership Team (ELT)
Online AI tools
AI tools which are accessed on the internet through a web browser
AI output
Any content that is generated by an AI tool

5. Policy Statements

5.1. Approved AI tools and online AI tools that can be accessed on ETL Systems' devices may be used where there is a business requirement to do so.

5.2. Where there is a business need to use an AI tool, users must ensure that approval has been granted by the Executive Leadership Team – see approval process.

5.3. Users must not upload information or data to any AI tool unless explicit approval has been granted by the Executive Leadership Team – see approval process.

5.4. Uses must avoid the sharing of any IP-related data and any IP-related discussions when using any AI tool.

5.5. Where there is a significant change to the use case of an approved AI tool, this change must be approved by the Executive Leadership Team – see approval process.

5.6. Users must ensure to the best of their ability that the data they provide to AI tools is accurate.

5.7. Users must check the accuracy, reliability, and credibility of AI output, to verify to the best of their ability that it does not contain any misinformation, or bias.

5.8. ETL Systems' **IT, Data Protection and Security Policies** apply when using AI tools.

5.9. Online AI tools may initially be blocked. Where users have a business need to access a blocked online AI tool a request can be submitted to the ELT – see approval process

6. Accountabilities and Responsibilities

6.1. The IT Manager is the accountable owner of the ETL Systems' AI Security Policy and is responsible for its maintenance and review.

6.2. Line managers must ensure that employees are aware of their responsibilities in relation to and when using AI tools.

6.3. It is the responsibility of all users to ensure that breach of this policy or misuse of AI tools is reported either to their line manager and/or in accordance with the **Security Incident Management Policy**.

6.4. It is the line manager's responsibility to take appropriate action where non-compliance to this policy is identified, in accordance with ETL's Disciplinary Policy.

7. Compliance

7.1. All ETL employees (permanent and temporary), contractors, suppliers and third parties who use ETL systems' equipment and/or software licenced by ETL systems, must be aware of and comply with ETL Systems' security policies and standards, including this AI Security

Policy.

7.2. If an individual is aware of an activity that breaches ETL Systems' security policy or standards, they should notify their Line Manager and/or report it in accordance with the **Security Incident Management Policy**.

7.3. Failure to report a security incident, potential or otherwise, could result in disciplinary action and, in the most severe circumstances, result in dismissal. A security incident is the attempted or actual unauthorised access, use, disclosure, modification, loss or destruction of an ETL Systems' asset (or a supplier or customer asset) in violation of security policy. Security incidents must be reported as soon as possible. Users must report security incidents, using the **Security Incident Management Policy**.

7.4. The IT Manager will regularly assess for compliance with this policy and may need to inspect systems, information and documentation to facilitate this. All ETL employees (permanent and temporary), contractors, suppliers and third parties who use ETL Systems' equipment and / or software licenced by ETL Systems will be required to support this activity.

8. Our procedures

8.1. We have performed a risk assessment through which we have:

8.1.1. identified our AI Tools;

8.1.2. considered our existing policies and procedures which overlap with this area of compliance including:

- Data Protection Policy
- Electronic Communication Policy
- Mobile Device Management Policy
- Security Incident Management Policy

and
produced this guidance for all staff

8.2. We have adopted a risk-based approach to compliance, as there are instances when AI can be helpful when used in a controlled and measured way.

8.3. Users should be familiar with all our related policies and procedures, including ETL's Data Protection Policy, Electronic Communication Policy, Mobile Device Management Policy, and Security Incident Management Policy.

9. Reporting concerns

9.1. It is essential that you properly raise any concerns you have in relation to a breach of this policy by any user, either by reporting to your Line Manager or following the **Security Incident Management Policy**.

10. Further information

If you require any further information, or you have any questions or concerns regarding the ETL Artificial Intelligence Security Policy, please contact Kevin Baldwin (IT Manager).

11. Monitoring and review

This policy will be reviewed periodically by the Company and updated in accordance with ETL's security requirements.