AI Security & Compliance Policy Framework

[COMPANY NAME]

LOGO

1. AI ACCOUNTABILITY & RESPONSIBILITY

Every AI tool or system used within the organisation must have a designated owner responsible for its security, compliance, and ethical usage. However, as an individual user, you are also accountable for ensuring responsible AI interaction and safeguarding company data. If you are uncertain about any aspect of AI use, seek guidance from your manager before proceeding.

2. SECURITY PRINCIPLES FOR AI USAGE

AI systems must be used in a way that aligns with our company's security policies and data protection obligations. The following principles apply to all users:

2.1 Protection of Confidential & Sensitive Data

- Do not upload, share, or process confidential, proprietary, or legally protected data (e.g., personal identifiable information, customer records, or employee details) without explicit approval.
- AI-generated content must be reviewed to ensure compliance before being shared externally.

2.2 Access Management & Authentication

- AI tools requiring login credentials must be accessed only by authorised users. Sharing credentials or unauthorised delegation of access is strictly prohibited.
- Multi-factor authentication (MFA) should be enabled where applicable to strengthen security.

2.3 Approved & Trusted AI Solutions

- Only AI tools approved through the company's risk assessment and approval process may be used. Using unauthorised AI services could expose the organisation to security vulnerabilities.
- A list of approved AI applications will be maintained and updated regularly.

2.4 Compliance with Security & IT Policies

- AI usage must adhere to all existing company security protocols, including password hygiene, software updates, and secure data disposal practices.
- Employees must follow relevant compliance regulations and industry standards when using AI-powered tools.

3. AI RISK CLASSIFICATION & USAGE LEVELS

AI applications are categorised based on their risk level, data sensitivity, and operational impact.

3.1 Low-Risk AI Applications

Definition: AI tools hosted internally and used for non-sensitive internal tasks.

- Employees may use these tools for non-sensitive tasks without additional approval.
- No customer, employee, or business-sensitive data should be shared with AI applications, even if they are hosted internally.

3.2 Moderate-Risk AI Applications

Definition: Externally hosted AI systems used for internal business functions.

- Employees may use these tools with caution and must never input customer or sensitive data.
- AI-generated content should be reviewed and sanitised before integration into company workflows.
- Any external AI deployment (e.g., chatbots, automated customer service) requires prior approval from IT and compliance teams.

3.3 High-Risk AI Applications

Definition: AI tools used for mission-critical operations or sensitive data processing.

- High-risk AI systems require strict oversight from IT, cybersecurity, and compliance teams.
- Use of AI in decision-making processes affecting customers, employees, or financials must undergo rigorous testing, monitoring, and approval.