2TWENTY4 CONSULTING
DATA PROTECTION SERVICES

AI Policy Template

A template policy to outline internal standards and requirements for organisations considering AI.

September 2023

Policy statement

Our organisation recognizes that the use of AI/ML tools can pose risks to our clients, employees, internal operations and organisational reputation. Therefore, we are committed to protecting the confidentiality, integrity, and availability of all organisational and client data. This policy requires all parties identified in the scope statement to use AI/ML tools in a manner consistent with our security and ethical best practices.

Introduction

The purpose of this policy is to establish guidelines and best practices for the responsible and ethical use of generative Artificial Intelligence (AI) within [Company Name]. It ensures that our employees are using AI systems and platforms in a manner that aligns with the company's values, adheres to legal and regulatory standards, meets our internal information security and data protection standards and applies appropriate care to organisation, employee and client data.

Scope

This policy applies to all technologies defined as AI or Machine Learning (ML). This particularly applies where a desired output will not require human intervention.

This policy applies to all employees, contractors, and third-party individuals who have access to generative AI technologies or are involved in using generative AI tools or platforms on behalf of our organisation.

Use

Generative AI/ML tools MUST only be used for business purposes approved by the organisation.

These purposes may include: [list relevant examples]

- contract drafting,
- legal advice,
- research
- knowledge management
- marketing/pitch creation

1 Pre-engagement Considerations

1 .1 Before the commencement of use of an AI/ML tool or platform, the project team MUST make themselves familiar with our internal Information Security and Data Protection Policies.

1.2 Before the commencement of use of an AI/ML tool or platform, any proposed AI project MUST be communicated to the DPO and Chief Information Security Officer (CISO).

1.3 Before the commencement of use of an AI/ML tool or platform, a Data Protection Impact Assessment (DPIA) MUST be completed.

2 Technical Considerations

2.1 If an AI/ML project needs to include personal data, the project sponsor MUST consider anonymising the data.

2.2 The project team MUST evaluate the security of any AI/ML tool before using it. This includes reviewing the tool's security features, terms of service, and data protection policy.

2.3 Wherever possible data both processed and outputted MUST be encrypted at rest and in transit.

2.4 Where AI/ML technology is used, the latest updates, patches, and security fixes MUST be applied in a timely manner.

2.5 Where possible a DLP (Data Loss Prevention) solution should be implemented and used.

3 Procedural Considerations

3.1 The project team MUST NOT process or share any data that is confidential, personal, or protected by regulation without prior approval from the appropriate department.

3.2 The project team MUST NOT give access to AI/ML tools outside the organisation without prior approval from the appropriate department or manager.

3.3 The project team MUST NOT give access to AI/ML outputs or results outside the organisation without prior approval from the appropriate department or manager.

3.4 An AI/ML project MUST have baked in checkpoints for DPO and InfoSec confirmation that is aligned with the internal Data Protection and Information Security policies.

3.5 Any broadening of scope (including additional or extended data sets) MUST be communicated to DPO and CISO.

3.6 An AI/ML project MUST be fully tested before used to provide customer services or outputs.

3.7 Any outputs from an AI/ML project MUST be analysed for personal data.

3.8 Any outputs from an AI/ML project MUST be assessed for bias. Outputs MUST be fair, inclusive, and not discriminate against any individuals or groups.

3.9 A live AI solution/service MUST be risk assessed on at least a quarterly basis.

4 Compliance with Laws and Regulations

4.1 All users of generative AI must comply with applicable laws, regulations, policies and guidelines governing intellectual property, data protection, client confidentiality and any other relevant areas.

4.2 Unauthorized use of copyrighted material or creation of content that infringes on the intellectual property of others is strictly prohibited.

5 Audit logs

5.1 Appropriate logging and auditing mechanisms MUST be in place to capture activities related to generative AI/ML usage.

5.2 Logs MUST be regularly reviewed to detect and respond to any suspicious or unauthorised activities.

6 Incident Reporting

6.1 Any suspected or confirmed security incidents related to generative AI/ML usage MUST be reported immediately to the DPO and CISO.

7 Training and Awareness

7.1 Users of AI/ML tools MUST receive training on the responsible and secure use of generative AI. This training should cover topics such as ethical considerations, potential risks, security best practices, and compliance requirements.

7.2 Regular awareness campaigns and communications should be conducted to all employees stating the importance of cybersecurity, responsible AI usage, and adherence to this policy.

8 Non-Compliance

8.1 Non-Compliance with this policy may result in disciplinary action, up to and including termination of employment or contract.

9 Policy Review

This policy will be reviewed periodically and updated as necessary to address emerging risks, technological advancements and any applicable regulatory changes.

REVIEW DATE	NAME	ROLE

It is our view that an AI Policy is a fundamental requirement for any organisation that takes data confidentiality and data protection seriously.

Additional recommended policies are;

- **Data Protection Policy**
- **Information Security Policy**
- **Acceptable Usage Policy**
- **Retention Policy**
- **Business continuity Policy**
- **Remote Working Policy**

2twenty4 offer a fixed price policy review service for GDPR and ISO 27001 compliance.

Contact us at info@2twenty4consulting.com