RIDGELINE CYBER DEFENCE

AI Security Documentation Suite

Governance documentation for organisations adopting AI technologies. Mapped to NIST AI RMF 1.0, OWASP Top 10 for LLM Applications 2025, and NIST CSF 2.0.

DOCUMENTS	FRAMEWORKS	FORMAT
30+	NIST AI RMF 1.0, OWASP LLM Top 10, CSF 2.0	Word (.docx) + Excel (.xlsx)

PRODUCT PREVIEW

This document provides a preview of the product contents, structure, and sample documentation quality. Visit ridgelinecyber.com to purchase the full toolkit.

WHAT'S INCLUDED

The AI Security Documentation Suite contains the following documents, templates, and tools:

AI Governance Policies

- AI Acceptable Use Policy
- AI Risk Management Policy
- AI Data Governance Policy
- AI Ethics and Responsible Use Policy
- Shadow AI Prevention and Detection Policy
- AI Vendor and Third-Party Assessment Policy

AI Risk Management

- AI Risk Assessment Framework (aligned to NIST AI RMF Map/Measure/Manage/Govern)
- AI Risk Register Template (Excel)
- AI Threat Modelling Guide (OWASP LLM Top 10 2025 mapped)
- AI Impact Assessment Template
- AI Model Inventory and Lifecycle Tracker

AI Security Controls

- Prompt Injection Prevention Controls (LLM01:2025)
- Sensitive Information Disclosure Controls (LLM02:2025)
- AI Supply Chain Security Controls (LLM03:2025)
- Data and Model Poisoning Prevention (LLM04:2025)
- Output Handling and Validation Controls (LLM05:2025)
- Excessive Agency Prevention Controls (LLM06:2025)

Implementation Tools

- AI Security Readiness Checklist
- AI Vendor Assessment Questionnaire
- AI Incident Response Playbook Addendum
- AI Security Awareness Training Materials
- AI Governance Metrics Dashboard (Excel)
- OWASP LLM Top 10 2025 Cross-Mapping Workbook

AI Acceptable Use Policy

Document ID: AI-POL-001 | Version: 1.0 | Classification: Internal | Status: Template

1. Purpose

This policy establishes the requirements and boundaries for the acceptable use of Artificial Intelligence (AI) technologies, including Large Language Models (LLMs), generative AI services, machine learning platforms, and AI-powered tools, across [Organisation Name]. It ensures that AI adoption supports organisational objectives while managing associated risks to confidentiality, integrity, availability, and ethical standards.

2. Scope

This policy applies to all employees, contractors, and third parties who access or use AI technologies in connection with organisational activities. It covers commercially available AI services (e.g., ChatGPT, Claude, Copilot, Gemini), internally developed or hosted AI models, AI features embedded in existing enterprise software, AI-powered automation and decision-support tools, and any processing of organisational data through AI systems.

3. Approved and Prohibited Uses

3.1 Approved Uses: Personnel may use organisation-approved AI tools for content drafting and editing assistance, code generation and review (subject to security review procedures), data analysis and summarisation of non-sensitive information, research and information gathering from publicly available sources, and process automation within approved workflows. 3.2 Prohibited Uses: The following uses of AI technologies are strictly prohibited: submitting classified, restricted, or personally identifiable information to external AI services without explicit authorisation, using AI outputs as final decision-making authority for actions affecting individuals, generating content that impersonates individuals or creates deceptive materials, bypassing security controls or using AI to circumvent established policies, and using AI tools not approved through the organisation's software approval process.

4. Data Protection Requirements

4.1 Personnel must not input data classified as Confidential or above into any external AI service unless the service has been formally assessed, approved, and contractually bound to appropriate data protection terms. 4.2 Outputs from AI systems that will be used in organisational documents, communications, or decisions must be reviewed for accuracy, bias, and appropriateness by a qualified individual before use. 4.3 All AI-related data processing must comply with the organisation's Data Classification and Protection Policy and applicable data protection legislation.

This is a preview excerpt. The full document continues with additional sections including detailed implementation requirements, roles and responsibilities, compliance measures, exceptions process, and review procedures.

FRAMEWORK CROSS-MAPPING EXAMPLE

Every document in the toolkit includes framework traceability. Below is an example of how our documentation maps to multiple compliance frameworks simultaneously.

NIST CSF 2.0	ISO 27001:2022	CIS Controls v8	RidgeLine Document
GV.PO-01	A.5.1	NIST AI RMF Govern 1.1	AI Acceptable Use Policy
GV.RM-01	Clause 6.1	NIST AI RMF Map 1.1	AI Risk Management Policy
PR.DS-01	A.8.24	OWASP LLM02 (Sensitive Info)	AI Data Governance Policy
ID.RA-01	A.8.8	OWASP LLM01 (Prompt Injection)	AI Threat Modelling Guide
PR.PS-05	A.8.19	OWASP LLM06 (Excessive Agency)	Shadow AI Prevention Policy
GV.SC-07	A.5.21	OWASP LLM03 (Supply Chain)	AI Vendor Assessment

Ready to close your governance gaps?

The full AI Security Documentation Suite includes every document shown in this preview — plus all supporting standards, procedures, forms, templates, and cross-mapping workbooks.

Starting from $149

ridgelinecyber.com/ai-security-suite/

contact@ridgelinecyber.com

14-day money-back guarantee | Instant download | Customise and deploy in days

This is a customisable template product only. It is not legal advice. Organisations should seek qualified professional advice for their specific circumstances and jurisdiction.