

Field	Value
Document ID	GOV-SEC-AI-001
Version	1.0
Effective Date	December 2024
Document Owner	Chief Information Security Officer
Classification	Internal Use
Review Cycle	Annual

Table of Contents

Security Controls for AI Systems.....1

1. Purpose and Objectives..... 1

1.1 Primary Objectives..... 1

1.2 Business Alignment..... 1

2. Scope and Applicability..... 1

2.1 In-Scope Systems and Components..... 1

2.2 Security Control Domains..... 2

2.3 Exclusions and Dependencies..... 2

3. Governance Structure and Accountability.....2

3.1 Roles and Responsibilities Matrix..... 2

3.2 Decision Authority Matrix..... 3

3.3 Governance Bodies and Committees..... 4

4. Security Control Framework..... 4

4.1 Secrets Management Controls (SEC-AI-001)..... 4

4.2 Data Egress Prevention Controls (SEC-AI-002)..... 6

4.3 Cryptographic Key Management Controls (SEC-AI-003).....8

4.4 System Isolation and Network Segmentation Controls (SEC-AI-004)..... 9

4.5 Model Hardening and Adversarial Protection Controls (SEC-AI-005)..... 11

4.6 Identity and Access Management Controls (SEC-AI-006)..... 13

4.7 Monitoring and Incident Response Controls (SEC-AI-007)..... 14

5. Threat Model and Risk Assessment Framework..... 16

5.1 AI Threat Landscape Analysis..... 16

5.2 Risk Treatment Strategies and Implementation..... 19

5.3 Business Continuity and Disaster Recovery for AI Systems..... 19

6. Compliance and Regulatory Alignment.....20

6.1 Standards and Framework Mapping.....20

6.2 Regulatory Compliance Requirements.....22

6.3 Audit and Assessment Procedures..... 23

7. Implementation Guidelines and Best Practices..... 23

7.1 Phased Implementation Approach..... 23

7.2 Technical Implementation Guidance..... 25

7.3 Operational Procedures and Playbooks..... 25

8. Metrics, Monitoring, and Continuous Improvement.....28

8.1 Key Performance Indicators and Success Metrics..... 28

8.2 Monitoring and Alerting Framework.....29

8.3 Continuous Improvement Framework..... 31

9. Training and Awareness Programs..... 32

9.1 Role-Based Training Curriculum..... 32

9.2 Security Culture Development.....33

10. Document Maintenance and Governance..... 33

10.1 Change Management Process..... 33

10.2 Review and Update Triggers.....34

10.3 Training and Communication..... 34

Security Controls for AI Systems

1. Purpose and Objectives

This document establishes comprehensive security controls for artificial intelligence systems within the organization's Information Security Management System (ISMS). The framework ensures robust protection of AI models, training data, inference data, prompts, tools, and supporting infrastructure while maintaining the confidentiality, integrity, and availability of AI-enabled services.

1.1 Primary Objectives

- Integrate AI-specific security requirements into existing ISO 27001:2013 ISMS framework
- Establish baseline security controls addressing unique AI threats and vulnerabilities
- Ensure compliance with NIST AI Risk Management Framework GOVERN-1.1 and MANAGE-2.3 functions
- Provide actionable implementation guidance for AI security control deployment
- Enable continuous monitoring and improvement of AI security posture

1.2 Business Alignment

This framework directly supports organizational risk management objectives by addressing the unique security challenges posed by AI systems, including model theft, adversarial attacks, data poisoning, prompt injection, and unauthorized access to proprietary algorithms. Controls integrate seamlessly with existing security governance structures while addressing regulatory compliance requirements under emerging AI legislation.

2. Scope and Applicability

2.1 In-Scope Systems and Components

System Category	Specific Components	Control Applicability
-----------------	---------------------	-----------------------