

Field	Value
Document ID	GOV-IRP-001
Version	2.0
Effective Date	December 2024
Document Owner	Chief Information Security Officer
Classification	Confidential - Internal Use
Review Cycle	Annual with quarterly updates

Table of Contents

AI Incident Response Runbook..... 1

1. Executive Summary..... 1

1.1 Key Objectives..... 1

1.2 Business Value Proposition..... 1

2. Document Purpose and Authority..... 2

2.1 Primary Objectives..... 2

2.2 Regulatory Framework Alignment..... 2

2.3 Document Authority and Approval..... 3

3. Scope and Applicability..... 3

3.1 AI Systems Coverage..... 3

3.2 Incident Categories in Scope..... 3

3.3 Geographic and Jurisdictional Scope..... 4

3.4 Exclusions..... 5

4. AI Incident Classification Framework..... 5

4.1 Comprehensive Incident Taxonomy..... 5

4.2 Severity Assessment Matrix..... 6

4.3 Impact Assessment Criteria..... 8

4.4 AI-Specific Risk Factors..... 9

5. Incident Response Organization and Governance..... 10

5.1 Comprehensive RACI Matrix..... 10

5.2 Incident Response Team Structure..... 11

5.3 Decision-Making Authority Matrix..... 13

5.4 On-Call Rotation and Escalation..... 14

5.5 Command and Control Structure..... 15

6. Incident Detection and Monitoring Framework..... 16

6.1 Automated Detection Systems..... 16

6.2 Human-Initiated Detection..... 17

6.3 Threat Intelligence and Early Warning..... 19

6.4 Monitoring Infrastructure and Architecture..... 20

7. Incident Response Procedures..... 22

7.1 Initial Response Workflow..... 22

7.2 Containment Strategies by Incident Type..... 24

7.3 Investigation Procedures..... 28

7.4 Recovery and Restoration Procedures.....	30
7.5 Special Procedures for High-Risk AI Systems.....	32
8. Communication and Notification Framework.....	33
8.1 Internal Communication Protocols.....	33
8.2 External Communication Requirements.....	38
8.3 Crisis Communication Procedures.....	43
9. Post-Incident Activities and Organizational Learning.....	44
9.1 Post-Incident Analysis Framework.....	44
9.2 Comprehensive Post-Mortem Process.....	47
9.3 Corrective Action Management.....	48
9.4 Organizational Learning and Knowledge Management.....	51
10. Regulatory Compliance and Standards Alignment.....	55
10.1 EU AI Act Compliance Framework.....	55
10.2 GDPR Integration for AI Incidents.....	57
10.3 ISO/IEC Standards Compliance.....	59
10.4 SOC 2 Control Integration.....	61
11. Technology Infrastructure and Tools.....	64
11.1 Incident Management Platform Architecture.....	64
11.2 AI-Specific Detection and Analysis Tools.....	66
11.3 Communication and Collaboration Systems.....	67
11.4 Metrics and Analytics Infrastructure.....	69

AI Incident Response Runbook

1. Executive Summary

This AI Incident Response Runbook establishes comprehensive procedures for detecting, responding to, and managing incidents related to artificial intelligence systems that pose risks to safety, privacy, fairness, security, or regulatory compliance. The runbook ensures rapid response capabilities, stakeholder protection, and systematic incident management across all AI operations within the organization.

The framework addresses critical business requirements including regulatory compliance under the EU AI Act Article 62, ISO/IEC 23053:2022 framework for AI risk management, NIST AI Risk Management Framework (AI RMF 1.0) GOVERN-3.1 and MANAGE-4.1, and SOC 2 Type II control objectives CC7.1 through CC7.4.

This document serves as the authoritative operational guide for incident response teams, AI system owners, legal counsel, communications teams, and executive leadership involved in managing AI-related incidents from initial detection through post-incident analysis and organizational learning.