ISO/IEC 42001:2023 Documentation Kit – Artificial Intelligence Management System (AIMS)

Level 1 – Manual and Policies	
Manual	
1.	ISO/IEC 42001:2023 Manual
Policies	
1.	Artificial Intelligence Policy
2.	Acceptable Use of Generative AI Tools
3.	Training Policy
4.	AI Tool Usage Policy
5.	AI Incident Recording and Reporting Policy
6.	Change Control
7.	Data Protection Policy
8.	HR Security Policy
9.	Backup Policy
Level 2 - Procedures	
1.	Management Review Procedure
2.	Documented Information Control Procedure
3.	Corrective Action Procedure
4.	Control of Records Procedure
5.	Internal Audit Procedure
6.	Risk Management Procedure
7.	Human Resources and Training Procedure
8.	Customer Relationship Procedure
9.	AI Incident Management Procedure
10.	Change Management Procedure
11.	AI System Impact Assessment Procedure
12.	Data Management Procedure
13.	Data Quality Procedure
14.	Scope Documentation for Implementation Procedure
15.	AI Life Cycle Development Procedure
16.	Monitoring and Measurement of Processes Procedure
17.	Managing Security Threats and Vulnerabilities Procedure
18.	Supplier and Contractor Management Procedure

19.	Information Transfer Procedure
20.	Employee Screening Procedure
21.	Software Development Life Cycle (SDLC) Procedure
Level 3 – SOPs	
1.	Responsible Design and Development of AI System
2.	Management of Removable Media
3.	Handling of Virus Attacks
4.	Artificial Intelligence Incident Management
5.	Group Internet and E-mail Usage
6.	Climate Change Mitigation and Adaptation
7.	Data Management
8.	Virtual Work Guidance
9.	Roles and Responsibilities for Virtual work
10.	Strategy for Virtual Work
11.	List of Criteria for Remote Work
12.	Information for Interested Parties of AI Systems
13.	AI Governance Framework
14.	Human-AI Collaboration
Level 4 – Formats & Templates	
Formats	
1.	Master List and Distribution List of Documents
2.	Change Note
3.	Corrective Action Report
4.	Master List of Records
5.	Objectives Monitoring Sheet
6.	Audit Plan / Schedule
7.	Internal Audit Non-Conformity Report
8.	ISO 42001 Clause-Wise Audit Review Report
9.	Continual Improvement Plan
10.	Change Request / Control Form
11.	Communication Report
12.	Management Review Meeting
13.	List of Licenses / Certificates

14.	Climate Change Preparedness Checklist
15.	Continual Improvement Monitoring Log
16.	List of Opportunities
17.	Need and Expectations of Interested Parties
18.	Instrument History Card
19.	Contractor Assessment Form
20.	Customer Property Monitoring Register
21.	Visitor Entry Register
22.	Employee Leaving / Transfer / Termination Checklist
23.	Employment Confidentiality and Non-Competition Agreement
24.	Job Description and Specification
25.	Manpower Requirement Form
26.	Performance Appraisal Form
27.	Gate Pass
28.	Supplier Confidentiality and Non-Competition Agreement
29.	Training Calendar
30.	Employee-Wise Training and Competence Record Sheet
31.	Induction Training Report
32.	Training Report
33.	Multi Skill Analysis
34.	Purchase Order
35.	Indent and Incoming Inspection Record
36.	Approved Supplier List
37.	Supplier Registration Form
38.	Annual Purchase Order
39.	Supplier Evaluation / Rating
40.	Order Form / Order Confirmation
41.	Contract Review Checklist / Summary of Contract
42.	Customer Complaint Report
43.	Customer Feedback Form
44.	Service Level Agreement
45.	Software Project Plan and Review Approval Register
46.	Minutes of Meeting

ISO/IEC 42001:2023 Manual

Contents

DOCUMENT NO:	
REVISION NO:	
DATE OF REVISION:	
PREPARED BY:	
REVIEWED BY:	
APPROVED BY:	
SIGNATURE:	

7 Support

7.1 Resources

Organization Name ensures that adequate resources are allocated to support the effective implementation and maintenance of its AIMS. This includes providing necessary financial resources, technological infrastructure, and human resources. Our resource planning addresses the requirements for developing, deploying, and managing AI systems, including hardware, software, and expertise. We continuously assess and adjust resource allocation to align with evolving needs and to ensure that our AI systems remain robust, secure, and compliant with industry standards.

Top management ensures that adequate resources are provided for:

- Establishing, implementing, operating, and maintaining the AIMS;
- Developing and using AI systems and components to enhance customer satisfaction and meet requirements;
- Managing and performing AIMS activities effectively.

7.2 Competence

At Organization Name, we prioritize the development and maintenance of competence among employees involved in AI system management. We identify specific competence requirements related to AI technologies, data management, ethical considerations, and regulatory compliance.

To meet these requirements, we provide targeted training and development opportunities. This includes internal and external training programs, workshops, and certifications to ensure that our staff receives the necessary skills and knowledge to effectively contribute to the AIMS. Competence is regularly reviewed and updated based on changes in technology and regulatory requirements.

7.3 Awareness

Organization Name actively raises awareness about the importance of AIMS and its impact on the organization and its stakeholders. We ensure that employees at all levels understand their roles and responsibilities concerning AI systems and the broader implications of AI ethics, security, and compliance.

AI Incident Management Procedure

Contents

DOCUMENT NO:	
REVISION NO:	
DATE OF REVISION:	
PREPARED BY:	
REVIEWED BY:	
APPROVED BY:	
SIGNATURE:	

1 Purpose

The purpose of this *AI Incident Management Procedure* is to establish a systematic approach for identifying, managing, and resolving incidents related to Organization Name's AI products and services. The procedure aims to ensure prompt response, effective resolution, and minimal impact on operations, aligning with the requirements of ISO/IEC 42001:2023. This includes maintaining product integrity, ensuring service continuity, and enhancing customer trust.

2 Scope

This procedure applies to all incidents involving Organization Name's products and services, including but not limited to:

- Failures or malfunctions of AI algorithms or systems
- Data breaches or security incidents affecting AI systems
- Compliance issues or ethical concerns related to AI
- Performance issues or unintended outcomes from AI services
- Customer complaints or issues impacting AI products and services

3 Responsibility

3.1 **Incident Response Manager**: Responsible for overseeing the entire incident management process, including detection, assessment, response, resolution, and post-incident review. Ensures that incidents are handled according to ISO/IEC 42001:2023 standards and that effective communication and coordination are maintained throughout the process.

3.2 **Incident Response Coordinator**: Leads the incident response efforts, manages the investigation, and ensures that incidents are resolved effectively. The Incident Response Coordinator is responsible for communication with stakeholders and documentation of the incident lifecycle.

3.3 **AI Security Specialist**: Focuses on incidents related to the security of AI systems, such as breaches or vulnerabilities. Works closely with the Incident Response Manager to address security-specific issues and implement measures to prevent future incidents.

3.4 **Technical Support Team**: Provides technical expertise and assistance in diagnosing and resolving incidents affecting AI products and services. Responsible for implementing corrective actions and ensuring that systems are restored to normal operation.

3.5 **Compliance Officer**: Ensures that incident management practices comply with legal and regulatory requirements. Monitors incidents for potential compliance issues and collaborates with the Incident Response Manager to address any regulatory implications.

4 Description of Activity

4.1 Objectives

The objectives of the incident management process are to:

- Ensure that all issues are properly documented and recorded.
- Assign the correct priority level to each reported problem.
- Identify recurring problems and escalate them as necessary.
- Oversee the resolution of all outstanding issues and restore services effectively.
- Identify and escalate issues to management that have not been resolved within the specified criteria.
- Review closed problems and confirm that their resolutions are effective.

4.2 Key Success Factors

- Assign problems to individuals or teams with the appropriate expertise. If a problem exceeds the knowledge, skills, or responsibilities of the assigned person or group, it should be reassigned accordingly. Problems may also be handed over to a coordinator for formal resolution and closure.
- All problems are logged with details of occurrence and resolution dates, facilitating the tracking of recurring issues and enabling reference to previous actions.
- Ensure each incident is escalated to the appropriate managers to allocate resources effectively and ensure timely communication.

4.3 Incident Response Process

The incident response process is divided into four stages:

- Invocation
- Assessment, Mitigation, and Escalation
- Resolution
- Post-Mortem

Internal Audit Procedure

Contents

DOCUMENT NO:	
REVISION NO:	
DATE OF REVISION:	
PREPARED BY:	
REVIEWED BY:	
APPROVED BY:	
SIGNATURE:	

1 Purpose

The purpose of this *Internal Audit Procedure* is to establish a systematic process for conducting internal audits of Organization Name's Artificial Intelligence Management System (AIMS). The procedure aims to evaluate the effectiveness of AIMS, ensure compliance with ISO/IEC 42001:2023, identify areas for improvement, and enhance overall organizational performance.

2 Scope

This procedure applies to all components of the AI Management System within Organization Name, including processes, controls, and documentation related to AI governance, implementation, and operation. It covers all internal audits conducted across departments and functions involved in AI management, ensuring comprehensive evaluation of the system's effectiveness and compliance.

3 Responsibility

3.1 **Internal Audit Team**: Responsible for planning, conducting, and reporting on internal audits. This team should be independent of the activities being audited to maintain objectivity.

3.2 **Audit Manager**: Oversees the internal audit process, ensuring compliance with this procedure, and addressing any issues identified.

3.3 **Department Heads**: Support the audit process by providing access to records, facilities, and personnel as required. They are also responsible for implementing corrective actions based on audit findings.

3.4 **AI Manager**: Provides input on audit criteria related to AI systems and ensures that audit findings related to AI processes are addressed. Supports the Internal Audit Manager in coordinating audits involving AI-related activities.

4 Description of Activity

4.1 Audit Schedule

4.1.1 The AI Manager prepares and approves the annual AIMS internal audit schedule, which encompasses all aspects of the AI management system. The schedule is determined based on the status and significance of activities, as well as findings from previous audits.

4.1.2 Regular audits are conducted, with the interval between audits for any specific system element or department not exceeding six months.

4.2 Planning and Scheduling of Audits

4.2.1 The AI Manager plans AIMS internal audits according to the annual AIMS internal audit schedule and provides the audit plan or program to the relevant personnel. Following the execution of the audit, the actual audit program is recorded in the audit plan. The AI Manager ensures that the auditor assigned is independent of the area being audited. The reference to the audit plan is included in the annual AIMS internal audit schedule. The audit criteria and scope are detailed in the audit plan or program.

4.3 Frequency

4.3.1 AIMS internal audits are scheduled based on the status and significance of the activity being audited. Typically, each function or element is audited at least once every six months. However, audits may be conducted more frequently during the initial establishment of the system or when:

a. AIMS results are not being met in specific areas or activities;
b. Previous internal audit reports (e.g., IANCRs) remain unresolved; or
c. There are substantial changes in key personnel, processes, techniques, or technology.

4.4 Audit Plan

4.4.1 Audit plans for different functional areas may be staggered to accommodate the availability of qualified and trained auditors or for other reasons. A copy of the audit plan is distributed to the auditor, audited personnel, and other relevant parties. Any changes to the audit plan are communicated by the auditor to the audited parties.

4.5 Selection of Auditors

The criteria for selecting auditors are as follows:

4.5.1 Auditors must have completed training in AIMS auditing in accordance with ISO 42001:2023 standards.

4.5.2 Auditors must not be employed in the same section or area being audited.

AI Tool Usage Policy

Contents

DOCUMENT NO:	
REVISION NO:	
DATE OF REVISION:	
PREPARED BY:	
REVIEWED BY:	
APPROVED BY:	
SIGNATURE:	

AI Tool Usage Policy

1 Purpose

The purpose of this *AI Tool Usage Policy* is to establish clear guidelines and procedures for the responsible and effective use of AI tools at Organization Name. This policy ensures that AI tools are used in a manner that complies with ISO/IEC 42001:2023 standards, promoting ethical practices, data security, and regulatory compliance.

2 Scope

This policy applies to all employees, contractors, and third parties who use AI tools within Organization Name. It covers the use of all AI tools, including but not limited to machine learning platforms, data analytics tools, automated decision-making systems, and natural language processing applications.

3 Responsibility

3.1 **Management**: Responsible for overseeing the implementation of this policy, allocating resources for AI tool management, and ensuring that all AI tools are used in accordance with the policy guidelines.

3.2 **AI Governance Team**: Responsible for establishing procedures for AI tool selection, risk assessment, and quality assurance. They also monitor the performance of AI tools and ensure that they align with the company's ethical and compliance standards.

3.3 **Department Heads**: Responsible for ensuring that AI tools used within their respective departments comply with this policy and that their teams adhere to the guidelines set forth.

3.4 **IT Department**: Responsible for the technical evaluation, deployment, and maintenance of AI tools, ensuring they meet security and performance standards.

4 AI Tool Usage Policy

4.1 Ethical and Responsible Use

AI tools must be used in a manner that aligns with Organization Name's ethical standards and values. Users are required to ensure that AI tools do not perpetuate biases, engage in discriminatory practices, or produce misleading or harmful outcomes. All AI-generated outputs should be transparent and understandable, with clear disclosure of their origins and limitations.

4.2 Compliance with Legal and Regulatory Requirements

The use of AI tools must comply with all relevant laws, regulations, and industry standards. This includes adhering to data protection regulations, intellectual property laws, and other legal frameworks applicable to the use of AI technologies. Users are responsible for ensuring that their use of AI tools is in compliance with these requirements.

4.3 Tool Selection and Evaluation

Before any AI tool is adopted or implemented, a thorough evaluation process must be conducted to assess its suitability for the intended use. This includes evaluating the tool's functionality, performance, and alignment with ethical and regulatory standards. The selection process should involve input from the AI Governance Committee, IT Department, and relevant departmental stakeholders to ensure that the chosen tool meets the company's requirements and standards.

4.4 Implementation and Integration

AI tools must be implemented following a structured approach that includes planning, testing, and integration into existing systems. The IT Department will oversee the technical aspects of implementation, ensuring that tools are integrated smoothly and that any potential issues are addressed promptly. Department heads are responsible for coordinating with the IT Department to ensure that tools are effectively integrated into departmental workflows.

4.5 Data Management and Security

AI tools must be managed in a way that ensures the security and privacy of data. Personal and sensitive data processed by AI tools must be handled in accordance with Organization Name's data protection policies. This includes implementing appropriate security measures to safeguard data against unauthorized access, breaches, or misuse.

4.6 Risk Management

Before deploying AI tools, a thorough risk assessment must be conducted to identify potential risks and impacts. This includes evaluating risks related to accuracy, security, and compliance. Risk management strategies must be implemented to address identified risks and mitigate potential adverse effects

SOP for Human-AI Collaboration

Contents

DOCUMENT NO:	
REVISION NO:	
DATE OF REVISION:	
PREPARED BY:	
REVIEWED BY:	
APPROVED BY:	
SIGNATURE:	

1 Objective

The objective of this Standard Operating Procedure (SOP) is to establish clear guidelines and processes for the effective collaboration between human employees and Artificial Intelligence (AI) systems within Organization Name, in alignment with the principles and requirements outlined in ISO/IEC 42001:2023 (Artificial Intelligence Management System). This SOP aims to ensure that AI systems enhance human capabilities, promote seamless interactions, foster mutual understanding between AI and human agents, and ensure ethical and responsible use of AI technologies.

Specific Objectives:

- Promote the integration of AI systems into business processes that enhance human decision-making, creativity, and productivity.
- Ensure that AI systems work in synergy with human employees to improve efficiency and operational outcomes.
- Establish clear roles, responsibilities, and processes for the collaboration between humans and AI.
- Mitigate risks arising from AI-human interaction, including bias, discrimination, and decision-making errors.

2 Scope

This SOP applies to all areas of Organization Name where AI systems and human employees interact, including but not limited to:

- **AI-Assisted Decision Making**: Where AI systems provide recommendations or decision-support for human decision-makers.
- **AI-Augmented Workforce**: AI systems that assist or enhance human performance in tasks such as data analysis, process automation, and customer service.
- **Human-AI Interaction**: The direct interaction between employees and AI interfaces or systems in everyday operations.
- **Collaboration Tools**: Use of AI-powered tools (e.g., chatbots, virtual assistants) that employees utilize to improve work efficiency and quality.
- **Training and Support**: Ongoing training and development to ensure that employees understand and effectively collaborate with AI systems

3 Responsibility

3.1 **AI Governance Committee**: Responsible for overseeing the overall framework for human-AI collaboration within Organization Name. They ensure that AI systems align with company policies, business goals, and regulatory standards. The committee also monitors the ethical implications of human-AI interactions, making sure that the collaboration supports fairness, transparency, and accountability. They provide strategic guidance and ensure that the integration of AI within business processes is both effective and compliant with ISO/IEC 42001:2023.

3.2 **AI Project Teams**: Responsible for the development and deployment of AI systems that facilitate human-AI collaboration. They design AI tools and models that support and enhance human decision-making and productivity. These teams ensure that AI systems are transparent, interpretable, and adaptable to human needs. They also provide necessary documentation and training to employees on how to effectively collaborate with AI systems, ensuring smooth integration into daily workflows.

3.3 **Human Resources (HR) and Training Teams**: Ensure that employees are properly equipped to collaborate with AI systems. They design and implement training programs that teach employees how to effectively use AI tools and understand their role in human-AI collaboration. Additionally, HR ensures that ongoing support is available to help employees maximize the benefits of AI while keeping them informed about best practices, ethical considerations, and new developments in AI technologies.

3.4 **AI Ethics Officer**: Ensuring that human-AI collaboration adheres to ethical guidelines. This role involves monitoring AI systems to ensure they operate fairly, transparently, and without bias. The Ethics Officer works to minimize any negative impact of AI on employees, ensuring that the collaboration is ethical and responsible. They also advise on best practices for maintaining trust and accountability in human-AI interactions.

3.5 **Employees**: Responsible for effectively collaborating with AI systems as part of their everyday tasks. They are expected to engage with AI tools, provide feedback, and follow ethical guidelines related to AI usage. Employees should ensure that AI-generated insights are used responsibly and that they maintain human oversight where necessary. They also help identify any issues or challenges arising from human-AI collaboration, contributing to the continuous improvement of AI systems.

4 Description of Activity

4.1 Human-AI Collaborative Design and Development

Ensure that AI systems are developed with the intent of complementing and enhancing human capabilities.

- Design AI systems with a focus on user-friendliness and transparency, ensuring they are interpretable and adaptable to human needs.
- Integrate human input in the design phase to understand user expectations, challenges, and work processes.
- Develop AI systems that provide clear, actionable insights, ensuring humans can easily interpret and use the information provided.

4.2 AI-Augmented Decision Making

Enhance human decision-making by providing AI-generated insights, recommendations, or support.

- Implement AI systems that provide data-driven recommendations, predictive analytics, or decision-support tools to assist human employees in complex decision-making.
- Establish feedback loops where human input is used to refine AI recommendations, ensuring continuous improvement and adaptation.
- Develop clear guidelines for human oversight of AI-driven decisions, ensuring final decisions remain under human control and accountability.

4.3 Training and Skill Development

Equip employees with the skills and knowledge necessary for effective collaboration with AI systems.

- Develop and deliver training programs focused on enhancing employees' understanding of AI systems, their capabilities, and limitations.
- Provide scenario-based training to help employees understand how to effectively use AI tools in their day-to-day tasks.
- Offer continuous learning opportunities to keep employees updated on new AI tools and collaboration techniques.

INTERNAL AUDIT NON–CONFORMITY REPORT			
NC report no		Date	
Department / area		Document reference	
Auditor		ISO 42001 clause no	
Audit criteria		Control #	
Description of nonconformity			
In-charge with action date			
Responsible person		Planned date	
Actual date		Completion date	
Audit information			
Auditee name		Auditor name	
Root cause of nonconformity			
Action taken to resolve the non–conformities			
Corrective action taken			
Review of action taken			
Status	☐ Closed	☐ Open	Date
Review of the effectiveness of action taken (next audit)			
Effectiveness checked by		Date	