

# INFORMATION SECURITY POLICY

## 1. Purpose

This Information Security Policy establishes the framework for protecting the confidentiality, integrity, and availability of information assets within FledgeWorks. It demonstrates management's commitment to information security and provides direction for the implementation and maintenance of the Information Security Management System (ISMS).

## 2. Scope

This policy applies to all information assets, systems, and processes within the scope of the organization's ISMS. It covers all employees, contractors, consultants, temporary staff, and other workers including all personnel affiliated with third parties who access, use, or handle the organization's information assets.

## 3. Information Security Objectives

FledgeWorks is a cloud-based, comprehensive, user-friendly and affordable HR solution aimed at providing enterprise-level services for companies of all sizes. FledgeWorks is designed to provide businesses with all the tools they need to manage their HR functions from recruitment and onboarding to performance, talent management and employee engagement.

We are committed to providing our clients with exceptional customer service and support. Our team is always on hand to provide assistance when needed.

One of our core objectives is to be recognized for strong and well-architected information security in our processes. This will be achieved through:

- ✓ **Continuous improvement of the ISMS according to ISO 27001:2022** – We are committed to the continuous improvement of our Information Security Management System (ISMS) based on the principles of ISO 27001:2022;
- ✓ **Employee Well-being and Professional Development** – We strive to ensure a healthy working environment and promote the professional development of our employees to maintain a culture of security awareness;
- ✓ **Compliance with Legal and Regulatory Requirements** – We will adhere to all relevant legal, regulatory, and contractual requirements, including those outlined by ISO 27001:2022;
- ✓ **Confidentiality** – We will protect the confidentiality of information in all business processes, ensuring that sensitive data is not disclosed to unauthorized individuals or entities;
- ✓ **Incident Management** – We adopt a proactive approach to minimize the impact of security incidents, ensuring that recovery time is minimized, and the consequences of downtime are reduced;
- ✓ **Threat Prevention and Risk Mitigation** – We are dedicated to identifying, preventing, and eliminating existing and potential threats to the security of FledgeWorks business;

FledgeWorks' approach to information security is founded on the following principles:

- **Confidentiality:** Information must be protected against unauthorized disclosure. This includes ensuring that only authorized personnel have access to sensitive information.
- **Integrity:** Information must be protected against unauthorized modification. The authenticity, accuracy, non-repudiation, and completeness of information must be maintained.
- **Availability:** Information and systems must be accessible and usable when needed, and protection must be in place to prevent unauthorized destruction or loss.

## 4. Leadership Commitment

# INFORMATION SECURITY POLICY

Top management demonstrates leadership and commitment to the ISMS by:

- Taking accountability for the effectiveness of the ISMS
- Ensuring the information security policy and objectives are established and compatible with the strategic direction of the organization
- Ensuring the integration of the ISMS requirements into the organization's processes
- Ensuring that the resources needed for the ISMS are available
- Communicating the importance of effective information security management
- Directing and supporting persons to contribute to the effectiveness of the ISMS
- Promoting continual improvement
- Supporting other relevant management roles to demonstrate their leadership

## 5. Roles and Responsibilities

### 5.1. Top Management

- Approves the Information Security Policy
- Provides resources for the implementation and maintenance of the ISMS
- Reviews the performance of the ISMS at planned intervals

### 5.2. Information Security Manager/Officer

- Develops and maintains the ISMS
- Coordinates information security activities
- Reports on the performance of the ISMS to top management
- Promotes information security awareness

### 5.3. Department Managers

- Implement information security controls within their areas of responsibility
- Ensure staff compliance with information security policies and procedures

### 5.4. All Staff

- Comply with information security policies and procedures
- Report information security incidents and weaknesses
- Participate in information security awareness training

## 6. Risk Management

The organization shall:

- Establish and maintain a documented risk assessment methodology
- Conduct regular risk assessments to identify, analyze, and evaluate information security risks
- Implement risk treatment plans to address identified risks
- Accept, avoid, transfer, or mitigate risks based on defined risk acceptance criteria
- Maintain a Statement of Applicability documenting the applicability of controls

## 7. Information Security Controls

The organization shall implement appropriate controls to address information security risks, including but not limited to:

- Access control
- Physical and environmental security
- Operational security
- Communications security
- System acquisition, development, and maintenance
- Supplier relationships
- Information security incident management
- Business continuity management

## INFORMATION SECURITY POLICY

- Compliance

### 8. Awareness and Training

The organization shall:

- Ensure that all personnel are aware of their information security responsibilities
- Provide appropriate information security awareness training
- Maintain records of training, skills, experience, and qualifications

### 9. Performance Evaluation

The organization shall:

- Monitor, measure, analyse, and evaluate the performance of the ISMS
- Conduct internal audits at planned intervals
- Perform management reviews of the ISMS

### 10. Improvement

The organization shall:

- Identify and address nonconformities through appropriate corrective actions
- Continuously improve the suitability, adequacy, and effectiveness of the ISMS

### 11. Policy Review

This Information Security Policy shall be reviewed at planned intervals or when significant changes occur to ensure its continued suitability, adequacy, and effectiveness.

### 12. Policy Approval

This Information Security Policy is approved by top management and is effective from the date of approval.

Approved by: CEO

Date: 01.07.2025

Version: 1.0