ISMS Implementation According to ISO/IEC 27001:2022

ISMS Policy

CLASSIFICATION: ***Public***

ISMS Policy

Contents

1. Purpose

The purpose of this policy is to ensure that appropriate controls and countermeasures are in place to protect corporate and client data, as well as **JPMC**'s information technology systems, services, and equipment. The policy aims to safeguard **JPMC**'s information assets from all threats—whether internal or external, deliberate or accidental—by maintaining the confidentiality, integrity, and availability of data and supporting compliance with industry regulations and best practices.

2. Scope

The policy applies to all information created or received by **JPMC** and covers all employees, contractors, and third-party partners. This policy forms the foundation of **JPMC**'s Information Security Management System (ISMS), incorporating related policies and procedures based on the ISO/IEC 27001 standard, using a risk-based approach to embed appropriate levels of information security controls and countermeasures

3. Policy Statement

JPMC is committed to ensuring the confidentiality, integrity, and availability of its information assets by:

- **Access Control:**
  - Protecting information assets from unauthorized access and potential threats.
  - Enforcing the principles of need-to-know and least privilege for access to information.
- **Compliance**:
  - Complying with all applicable regulatory and legislative requirements.
- **Training and Competence:**
  - Maintaining a high level of competence among staff by providing regular information security training and awareness programs.
- **ISMS Framework:**
  - Adopting ISO/IEC 27001 as a framework for implementing and maintaining a formal ISMS to protect the confidentiality, integrity, and availability of information.
- **Alignment and Risk Management:**
  - Ensuring information security aligns with **JPMC**'s strategic direction and business objectives.
  - Managing information security risks based on **JPMC**'s Risk Management Methodology.
- **Continuous Improvement**:
  - Committing to the continuous improvement of the ISMS by measuring performance, reviewing outcomes, and suggesting necessary actions for enhanced effectiveness.
- **Incident Management:**
  - Addressing and resolving security incidents and suspected vulnerabilities based on their nature to minimize impact and prevent recurrence.

4. Responsibilities

- **Managers**:
  - All managers are directly responsible for implementing this ISMS Policy and ensuring that their staff adhere to it.
- **IT and Security Teams**:
  - The IT and security teams are responsible for providing the necessary guidance and technical support for the effective implementation and maintenance of the ISMS.
- **All Employees**:
  - All employees are responsible for supporting the organization's information security framework by adhering to the ISMS Policy, as well as all supporting policies, standards, and procedures.
  - Participation in training and awareness programs is required to maintain compliance with information security requirements.
  - Any violations of the ISMS Policy or related standards will result in corrective actions and disciplinary measures, based on the severity of the violation.
- **Third Parties:**
  - Third parties are required to comply with the ISMS Policy and all supporting policies, standards, and procedures.
  - Violations by third parties will be addressed with appropriate corrective actions, including potential contract termination, based on the severity of the violation.