Information Governance Policy

DISTRIBUTION

This Information Governance Policy is communicated to all employees. A copy is available at the Head Office, held in the sites folder, and published on the internal company shared drive. All employees are encouraged to read it and communicate any queries to a Director.

REVISION HISTORY

Issue Number	Review Date	Changes	Signed
01	07/06/2022	Original version (draft)	MD
01	07/06/2022	Signed off	MD
02	07/06/2023	Review	MD

Information Governance Policy

Purpose:
The purpose of this Information Governance Policy is to establish guidelines for the responsible and secure management of information within ZAM FM LTD in the security industry.

Scope:
This policy applies to all employees, contractors, and third-party entities handling information on behalf of ZAM FM LTD.

Definitions:
Sensitive Information: Refers to any information that, if compromised, could harm the security, integrity, or reputation of ZAM FM LTD.
Security Personnel: All employees, contractors, or individuals engaged in security-related functions.

Responsibilities:
Security Personnel are responsible for ensuring the confidentiality, integrity, and availability of sensitive information.
The Information Governance Officer is appointed to oversee and enforce compliance with this policy.

Information Classification:
Information will be classified based on its criticality to security operations.
Classification levels include Public, Internal Use, Confidential, and Top Secret.

Data Handling and Transmission:
Security Personnel must follow established protocols for the secure handling, storage, and transmission of sensitive information.
Encryption measures must be applied to all confidential and top-secret information during transmission.

Data Privacy and Protection:
ZAM FM LTD adheres to all relevant data protection laws and regulations applicable to the security industry.
Personal information collected during security operations will be handled with the utmost care and in compliance with privacy laws.

Information Security:
Security measures, including access controls, surveillance, and cybersecurity protocols, will be implemented to protect information assets.
Regular security training will be provided to ensure awareness and adherence to security measures.

Information Governance Policy

Record Management:
Recordkeeping related to security operations must follow established procedures, including proper documentation and storage.
Records will be retained based on industry regulations and legal requirements.

Compliance and Auditing:
Regular internal audits will be conducted to assess compliance with this policy.
External audits may be conducted to ensure adherence to industry standards and regulations.

Incident Response:
Procedures for reporting and responding to information security incidents are outlined in the Incident Response Plan.
Security Personnel must report any breaches or incidents promptly.

Training and Awareness:
Security awareness training programs will be conducted regularly to keep personnel informed of the latest security threats and best practices.
All personnel must undergo security training upon onboarding.

This policy is a foundational document, and it should be supported by detailed procedures, guidelines, and staff training to ensure effective implementation.

Managing Director
Danish
Dated: 07/06/2023