Retention Policy

This Retention Policy outlines the guidelines and procedures for the retention and disposal of records and information for WL Risk Management Ltd. It is designed to ensure compliance with legal and regulatory requirements, as well as to protect the company's sensitive information.

Purpose

The purpose of this policy is to establish a consistent and systematic approach to the retention and disposal of records and information within the security company. This will help to ensure the proper management of information, reduce the risk of data breaches, and maintain the integrity and confidentiality of the company's information.

Scope

This policy applies to all employees, clients, sub contractors or workers, and third-party vendors who handle or have access to company records and information. This includes both physical and electronic records, such as paper documents, digital files, emails, and any other form of information.

Retention Periods

The retention periods for records and information within the security company are determined based on the legal and regulatory requirements, as well as business needs. The following are the general retention periods for different types of records:

- Employee records: 6 years (+ 1 year) after termination of employment.
- Financial records: 6 years (+ 1yr) after the end of the fiscal year.
- Contracts and agreements: 6 years (+ 1yr) after expiration or termination
- Incident reports and security logs: 3 years
- Training records: 3 years
- Client information: 3 years after the end of the business relationship

Under GDPR Article 5 (1) (e) WL Risk Management will comply sensibly and not retain information for longer than necessary.

Storage and Disposal

All records and information must be stored securely and protected from unauthorized access. Physical records should be kept in locked cabinets or rooms, and digital records should be stored on secure servers with access controls in place.
At the end of the retention period, records and information should be disposed of in a secure manner, such as shredding or digital erasure. Any disposal must be documented and approved by the appropriate personnel.

Exceptions

In some cases, certain records or information may need to be retained for longer periods due to legal or regulatory requirements. In such cases, the retention period will be extended as necessary and documented accordingly.

According to GDPR Article 5 (1) (b)*…further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes,* allows for longer retention periods.

Training and Awareness

All employees, subcontractors, workers, and third-party vendors must be trained on this Retention Policy and its procedures. Regular training and awareness programs will be conducted to ensure compliance and understanding of the policy.

Non-Compliance

Non-compliance with this Retention Policy may result in disciplinary action, up to and including termination of employment. Any intentional destruction or alteration of records or information is strictly prohibited and will result in immediate termination and possible legal action.

Review and Revision

This Retention Policy will be reviewed annually and updated as needed to ensure compliance with changing laws and regulations. Any revisions or updates will be communicated to all employees, contractors, and third-party vendors.

This Retention Policy is essential for the proper management and protection of the security company's records and information. By following these guidelines, we can ensure compliance, prevent data breaches, and maintain the integrity and confidentiality of our information.