Internal Data Protection & Security Policy

Document Owner: Compliance Team
Effective Date: 01 Jan 2025
Review Cycle: Periodic
Applies To: All employees, contractors, and third parties

1. Purpose

This policy defines the organisation’s approach to protecting personal data and managing security-related incidents in accordance with applicable regulatory and business requirements.

2. Scope

This policy applies to all personal data and information assets processed, stored, or transmitted by the organisation.

3. Data Retention

Personal data should not be retained longer than necessary to fulfil business or legal requirements.
Retention practices shall consider operational needs and applicable regulatory obligations.

4. Access Control

Access to systems and information assets shall be limited to authorised personnel only.
Access privileges should be aligned with job responsibilities.

5. Information Deletion

Information that is no longer required for business purposes should be removed from systems in a timely manner.

6. Incident Management

Any suspected or confirmed security or data incidents should be reported to management as soon as reasonably practicable.
Appropriate action shall be taken to contain and remediate such incidents.

7. Awareness

Employees are expected to be aware of their responsibilities when handling personal data and information assets.

8. Policy Review

This policy shall be reviewed periodically to ensure ongoing relevance.