Company IT Policy

Governance

Document Control

The IT policy document will be reviewed and updated annually. All revisions must be documented, and previous versions archived.

Approvals

All policy amendments require approval from the IT Governance Board prior to implementation.

Change Management

- Changes to IT systems must follow a standardized process to minimize risks.
- A risk assessment must be completed for each proposed change.

Organizational Structure and Strategy

The IT department aligns with the company's strategic goals, supporting efficiency and innovation while managing operational costs.

Cost and Performance Reporting

Regular reporting of IT costs and performance metrics will be conducted to assess alignment with business objectives.

Service Level Management

- Service levels for IT support and operations are defined, measured, and reviewed periodically to ensure quality standards are met.

Legal and Regulatory Compliance

All IT operations must adhere to applicable laws and regulations, including data protection and privacy requirements.

Asset and Operations Management

- IT assets must be recorded, tracked, and managed effectively.
- Operational procedures must ensure business continuity and reliable IT services.

Third-Party Services

All contracts with external service providers will include clauses ensuring compliance with the company's IT policies.

Development Methodology

Software development will follow Agile methodologies for adaptability and efficiency.

Access Controls

- Access to IT systems is restricted to authorized personnel only.
- Periodic reviews of access rights are conducted to ensure compliance.

Network and Computer Security

Robust security measures are implemented to protect against unauthorized access and threats.

End-User Computing

- End-users must adhere to the Acceptable Use Policy at all times.
- Training will be provided to ensure users understand security protocols.

Email and Malware Policies

Email systems are monitored for compliance with security standards, and anti-malware solutions are deployed across all IT assets.

Business Continuity and Disaster Recovery

A comprehensive plan is in place to ensure business operations continue with minimal disruption in the event of a disaster.

Audit Procedures

Regular audits of IT systems and processes are conducted to ensure adherence to policies and identify areas for improvement.

Website Governance

The corporate website is maintained to reflect accurate, up-to-date information and adhere to company branding and security guidelines.

Signatures

Formal approval of this IT policy is required from the following designated authorities:

- Chief Information Officer
- Executive Board Member