Sri Lanka Institute of Information Technology

ISMS Document Pack

Group Number - 59

IE3102 - Enterprise Standards for Information Security

Group Details:

	Student ID	Student Name	Email	Contact Number
1	IT23415140	U.L.K.H. Liyanage	it23415140@my.sliit.lk	0773092825
2	IT23159730	W.H.M.S.R. Bandara	it23159730@my.sliit.lk	0763366659
3	IT23269484	T.H. Ranasinghe	it23269484@my.sliit.lk	0762090122
4	IT23187214	N.K.B.H. Rathnayake	it23187214@my.sliit.lk	0719106526
5	IT23171138	D.P.D.K. Perera	it23171138@my.sliit.lk	0710426973

1. Executive Summary

Dynamic Biz IT Solutions is a medium-sized IT services provider managing sensitive client data, intellectual property, and financial information. As the company grows, ensuring the confidentiality, integrity, and availability of its information assets is vital to maintaining customer trust, regulatory compliance, and business resilience.

This ISMS Documentation Pack has been prepared to guide Dynamic Biz in aligning with the **ISO/IEC 27001:2022 standard**. It consists of:

- **Scope Statement**: Defines the ISMS boundaries, including systems, processes, and information assets.
- **Information Security Policy**: Establishes the organization's commitment to protecting information and creating a security-aware culture.
- **Statement of Applicability (SoA)**: Maps ISO/IEC 27001 Annex A controls to Dynamic Biz's current practices, highlighting both strengths and areas requiring attention.
- **Risk Treatment Plan**: Provides strategies to mitigate key risks such as phishing, unauthorized access, and policy non-compliance.

By adopting this ISMS framework, Dynamic Biz will not only strengthen its security posture but also demonstrate accountability to clients and regulators. It creates a foundation for continuous improvement, employee awareness, and long-term competitive advantage.

2. Scope Statement

Dynamic Biz IT Solutions is a medium-sized IT services company with around 300 employees. The organization specializes in software development, customer support, and managed IT services. Since the company handles sensitive information such as client records, intellectual property, and financial data, the scope of its Information Security Management System (ISMS) has been carefully defined to include all core areas that impact information confidentiality, integrity, and availability.

In-Scope:

- **Applications & Services:** The web-based security awareness and policy management platform, client-facing portals, and internal collaboration tools.
- **IT Infrastructure:** On-premise servers, employee laptops, cloud-hosted applications, and networking devices.
- **Business Processes:** Policy management, software development lifecycle (SDLC), customer support, and accounting operations.
- **Information Assets:** Client data, source code repositories, training content, financial information, HR records, and internal communications.
- **Departments Covered:** Development, Security, Customer Care, Marketing, Design & Content, and accounting teams.

Out of Scope:

- Physical security measures of office premises, beyond server room access control.
- Third-party vendor environments, except where service-level agreements (SLAs) explicitly define security obligations.

This scope ensures the ISMS focuses on assets and processes critical to service delivery and regulatory compliance, while excluding areas not directly under Dynamic Biz's control.

3. Information Security Policy

Purpose

The purpose of this policy is to protect the information assets of Dynamic Biz IT Solutions from internal and external threats, whether deliberate or accidental. The policy provides a framework for setting security objectives, managing risks, and ensuring ongoing compliance with **ISO/IEC 27001:2022**.

Commitment from Management

Top management is committed to safeguarding information by:

- Prioritizing confidentiality, integrity, and availability (CIA triad).
- Meeting all contractual, regulatory, and legal obligations such as GDPR and Sri Lanka's PDPA.
- Providing adequate resources for security initiatives and training.
- Building a **security aware culture** where employees understand and accept their responsibilities.
- Continually improving the ISMS through periodic reviews, internal audits, and corrective actions.

Key Principles

1. **Access Control:** All information systems shall be protected by role-based access, MFA, and the principle of least privilege.
2. **Training & Awareness:** Every employee must undergo annual security awareness training tailored to their role.
3. **Data Protection:** Critical information shall be encrypted both in transit (TLS 1.2+) and at rest (AES-256).
4. **Incident Response:** All employees must immediately report incidents. A formal response plan is in place to manage breaches effectively.
5. **Vendor Security:** Third parties must comply with agreed security requirements before handling company data.

Responsibilities

- **Top Management:** Set strategy, approve policies, allocate resources.
- **Security Coordinator:** Manage ISMS, monitor compliance, handle incidents.
- **Employees:** Follow policies, maintain security hygiene, report issues promptly.

4. Expanded Statement of Applicability (SoA)

The following table lists a broader set of Annex A controls, indicating whether they are implemented, partially implemented, or not applicable to Dynamic Biz IT Solutions. Each control is mapped to the organization's practices and justifications.

Control ID	Control Title	Status	Justification
A.5.1	Information Security Policies	Implemented	ISMS policy documented, approved by management, and communicated to staff.
A.5.3	Information Security Roles & Responsibilities	Implemented	Security Coordinator role established; roles defined in policy.
A.5.34	Awareness, Education, and Training	Implemented	Role-based awareness platform deployed with tracking of participation.
A.6.1	Organization of Information Security	Implemented	Clear roles defined, reporting lines established, responsibilities documented.
A.6.3	Contact with Authorities	Partially Implemented	Incident response team has authority contacts, but not yet tested in simulation.
A.7.2	Screening	Implemented	Pre-employment background checks performed before hiring.
A.7.3	Terms and Conditions of Employment	Implemented	Employee contracts include confidentiality and acceptable use clauses.
A.8.1	Asset Management	Implemented	IT maintains asset register for servers, devices, and cloud resources.
A.8.23	Web Filtering & Phishing Défense	Implemented	Anti-phishing tools and email filtering implemented.
A.8.24	Data Protection (Encryption)	Implemented	AES-256 encryption at rest, TLS 1.2+ for in transit data.
A.8.28	Data Loss Prevention	Partially Implemented	Endpoint monitoring planned; basic access restrictions already in place.
A.9.1	Access Control Policy	Implemented	Role-based access (RBAC) and MFA in place across core systems.

A.9.2	User Access Management	Implemented	User provisioning and reviews performed by IT/security coordinator.
A.9.4	System & Application Access Control	Implemented	Session timeouts, password policies, MFA enforced.
A.10.1	Cryptographic Controls	Implemented	Data encryption at rest and in transit, secure key management practices.
A.12.6	Technical Vulnerability Management	Partially Implemented	Vulnerability scanning active, patch cycle still being formalized.
A.12.8	Logging & Monitoring	Implemented	Centralized logging in place; logs reviewed monthly.
A.13.1	Network Security Management	Implemented	Firewalls, IDS/IPS, and segmentation deployed.
A.14.2	Secure Development Practices	Implemented	Developers trained in secure coding, repository access controlled.
A.15.1	Supplier Security	Partially Implemented	Vendor contracts include security clauses, but vendor audits not yet regular.
A.16.1	Information Security Incident Management	Implemented	Incident reporting process documented and tested.
A.17.1	Business Continuity & Disaster Recovery	Not Applicable	Covered by third party DR vendor under SLA.
A.18.1	Compliance with Legal & Regulatory Requirements	Implemented	GDPR and PDPA requirements reviewed; policy updated accordingly.

5. Risk Treatment Plan

The initial risk assessment identified several critical risks requiring treatment. The following table summarizes the proposed strategies:

Risk ID	Asset	Threat	Vulnerability	Risk Level	Treatment Strategy	ISO Control
R1	Client Data	Phishing Attack	Human error	High	Deploy email filtering, conduct role-specific phishing simulations, enforce reporting.	A.5.34, A.8.23
R2	Source Code Repo	Unauthorized Access	Weak credentials	High	Enforce MFA, password policy, and access reviews.	A.9.2
R3	Financial Records	Data Breach	No encryption at rest	Medium	Encrypt with AES-256, monitor access logs.	A.8.24
R4	Web Application	DoS Attack	No WAF in place	Medium	Implement Web Application Firewall (WAF), monitoring, and alerts.	A.8.16
R5	Employee Devices	Insider Misuse	Lack of DLP	Medium	Deploy Data Loss Prevention tools, enforce RBAC.	A.8.28
R6	Training Platform	Policy Non-Compliance	Employees skipping modules	Low	Track participation via LMS, link completion to performance KPIs.	A.6.3

Treatment Approach

- **Avoidance:** Prevent risks where possible (e.g., WAF to block DoS).
- **Mitigation:** Reduce likelihood/impact with technical controls (e.g., encryption, MFA).
- **Transfer:** Outsource DR to third-party vendor under SLA.
- **Acceptance:** Low-level risks will be accepted with monitoring.

6. Conclusion

The ISMS Documentation Pack equips **Dynamic Biz IT Solutions** with a solid framework to align with **ISO/IEC 27001:2022**. By defining scope, publishing and Information Security Policy, expanding the Statement of Applicability, and creating a Risk Treatment Plan, the company now has both direction and actionable steps for strengthening its security posture.

This framework addresses major risks such as phishing, insider misuse, and system vulnerabilities, while also embedding a culture of accountability through awareness training and clear role-based responsibilities. The expanded SoA highlights areas of strength (access control, asset management, awareness) and gaps needing attention (vendor management, patching, business continuity).

Implementing this ISMS will deliver key business benefits: increased client trust, reduced likelihood of breaches, stronger compliance, and greater resilience. To sustain progress, Dynamic Biz should focus on continuous improvement, regular audits, and measuring key security metrics.

In short, this ISMS Pack is both a practical roadmap and a cultural shift, positioning Dynamic Biz for ISO 27001 certification and long-term competitive advantage.