Information Security Policy

DOCUMENT CLASSIFICATION	Public
DOCUMENT REF	ISMS-DOC-05-4
VERSION	2.0
DATED	7 Dec 2025
DOCUMENT AUTHOR	Eng.Taghreed Antar
DOCUMENT OWNER	Cyber Security & Information Security Unit

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
0.1	15 Oct 2023	SMT Team	Create the Document
0.2	7 Dec 2023	Taghreed Antar	Update the Document
1.0	3 Jan 2024	Rania Hiasat	Release the Document
1.0	15 Sep 2024	Dr.Ahmad Al-Omoosh	Approve the Document
1.1	1 Jan 2025	Taghreed Antar	Review the Document/Update Document Classification

Distribution

NAME	TITLE
DLS Team	Employees in scope

Approval

NAME	POSITION	SIGNATURE	DATE
Eng.Khaldoun Al-Khaldi	General Manager		7 Dec 2025
Rania Hiasat	Deputy General Manager for IT		7 Dec 2025

Contents

Figures

Tables

1 Introduction

This document defines the information security policy of DLS.

As a government service organization, DLS recognizes at senior levels the need to ensure its ability to perform its duties, protect the real estate property and information entrusted, and provide its services smoothly and without interruption for the benefit of its customers, and other stakeholders.

In order to provide such a level of continuous operation, DLS has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001. This standard defines the requirements for an ISMS based on internationally recognized best practice.

The operation of the ISMS has many benefits for the business, including:

- Maintain customer service levels and customer confidence.
- Protect sensitive data and assets.
- Improve risk management through reducing the impact of internal and external threats.
- Enhance operational effectiveness for processes by sustaining DLS activities and services.
- Continually improve the department's information security and reduce their costs.
- Compliance with legal and regulatory requirements.

DLS has decided to maintain full certification to ISO/IEC 27001 in order that the effective adoption of information security best practice may be validated by an independent third party, a Registered Certification Body (RCB).

This policy applies to all systems operated by DLS or third party contracted with DLS, also applies to processes that constitute the organization's information systems, and people including managers, employees, consultants, contractors, suppliers, vendors, temporary workers and other third parties who have access to DLS systems and facilities.

The following supporting documents are relevant to this information security policy and provide additional information about how it is applied:

- *Risk Assessment and Treatment Process*
- *Statement of Applicability*
- *Supplier Evaluation Form*
- *Risk Management Strategic Plan*
- *Code of professional conduct and work ethics*
- *Code of Professional Conduct and Non-Disclosure Agreement*

- *Acceptable Use Policy*
- *Password Construction Standards*
- *Password Protection Policy*
- *Email Policy*
- *Acceptable Encryption Policy*
- *Media Protection Policy*
- *Minimum Access Policy*
- *Access Control Policy*
- *Clean Desk Policy*
- *Anti-Virus & Anti-Malware Policy*
- *Router & Switch Policy*
- *Network Security Policy*
- *Configuration Management Policy*
- *Wireless Communication Standards*
- *Wireless Communication Policy*
- *Remote Access Policy*
- *Area & Facility Access Policy*
- *Technology Equipment Disposal Policy*
- *Equipment & Storage Security Policy*
- *Backup & Recovery Policy*
- *Disaster Recovery Plan Policy*
- *Auditing Policy*
- *Database Security Policy*
- *Information Logging Standards*
- *Protective Monitoring Policy*
- *Incident Response Policy*
- *Personnel Security Standard*
- *Security Awareness & Training Policy*

Details of the latest version number of each of these documents are available from the ISMS Documentation Log.

2 Information security policy

2.1 Information security requirements

A clear definition of the requirements for information security within DLS will be agreed and maintained with the internal business so that all ISMS activity is focused on the fulfilment of those requirements. Statutory, regulatory and contractual requirements will also be documented and input to the planning process. Specific requirements about the security of new or changed systems or services will be captured as part of the design stage of each project.

It is a fundamental principle of the DLS Information Security Management System that the controls implemented are driven by business needs and this will be regularly communicated to all staff through team meetings and briefing documents.

2.2 Framework for setting objectives

A regular cycle will be used for the setting of objectives for information security, to coincide with the budget planning cycle. This will ensure that adequate funding is obtained for the improvement activities identified. These objectives will be based upon a clear understanding of the business requirements, informed by the management review process during which the views of relevant interested parties may be obtained.

Information security objectives will be documented for an agreed time period, together with details of how they will be achieved. These will be evaluated and monitored as part of management reviews to ensure that they remain valid. If amendments are required, these will be managed through the change management process.

In accordance with ISO/IEC 27001 the reference controls detailed in Annex A of the standard will be adopted where appropriate by DLS. These will be reviewed on a regular basis in the light of the outcome from risk assessments and in line with information security risk treatment plans. For details of which Annex A controls have been implemented and which have been excluded please see the *Statement of Applicability*.

In addition, enhanced and additional controls from the following codes of practice will be adopted and implemented where appropriate:

- ISO/IEC 27002 – Code of practice for information security controls

The adoption of these codes of practice will provide additional assurance to our customers and help further with our compliance with international data protection legislation.

2.3 Continual improvement of the ISMS

DLS policy regarding continual improvement is to:

- Continually improve the effectiveness of the ISMS.
- Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001 and related standards.
- Achieve ISO/IEC 27001 certification and maintain it on an on-going basis.
- Increase the level of proactivity (and the stakeholder perception of proactivity) with regard to information security.
- Make information security processes and controls more measurable in order to provide a sound basis for informed decisions.
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data.
- Obtain ideas for improvement via regular meetings and other forms of communication with interested parties.
- Review ideas for improvement at regular management meetings in order to prioritize and assess timescales and benefits.

Ideas for improvements may be obtained from any source including employees, customers, suppliers, IT staff, compliance audit reports, cyber security assessments, risk assessments and service reports. Once identified they will be recorded and evaluated as part of management reviews.

2.4 Information security policy areas

DLS defines policy in a wide variety of information security-related areas which are classified into six core areas and described in detail in a comprehensive set of policy documentation that accompanies this overarching information security policy.

Core and subsidiary areas of Information security policy are shown in DLS Cyber Security Framework below:

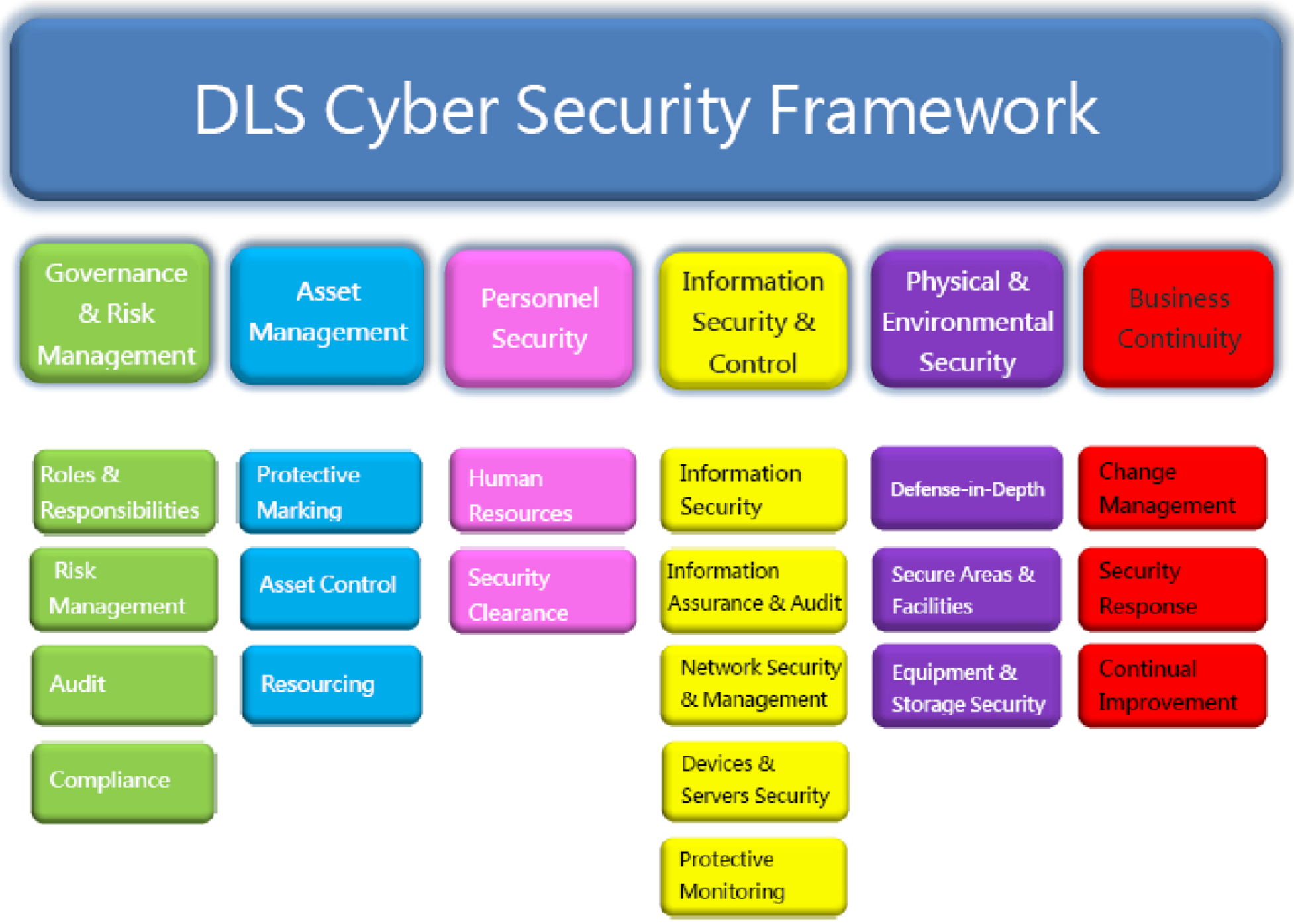

Figure 1 – DLS Cyber Security Framework

Each of these policies is defined and agreed by one or more people with competence in the relevant area and, once formally approved, is communicated to an appropriate audience, both within and external to, the organization.

The table below shows the individual policies within the documentation set and summarizes each policy's content and the target audience of interested parties.

POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
Acceptable Use Policy	Determine the acceptable/unacceptable use of all computer equipment and information systems in the DLS, proprietary information, email and communication activities, blogging and social media , employee commitment to organizational information security policies ,.	All employees
Password Construction Standards	Best practices for creating strong passwords.	All employees
Password Protection Policy	Establish the standard for creating strong passwords, changing them, protecting these passwords, and setting the frequency of changing them, application development precautions, and multi-factor authentication.	All employees
Email Policy	Specifies the acceptable and unacceptable use of e-mail and the restrictions on its use within the DLS.	All employees using email
Acceptable Encryption Policy	Determine a consistent approach to using encryption controls and algorithms to prevent unauthorized access to information, requirements, key generation, and key management.	Employees involved in setting up and managing the use of cryptographic technology and techniques
Media Protection Policy	General and specific principles for ensuring the secure storage, transmission and destruction of sensitive information contained in storage media (Media use, media access, media storage, media transfer, media marking, media inventory).	All employees
Minimum Access Policy	Minimum security standards required for devices connected to DLS network.	
Access Control Policy	Access control procedures , user access management, (user registration, privilege management ,password management ,access rights) ,user responsibilities , separation of duties, OS access control (logon procedure ,identification, authentication, using utility programs, limitation of access and connectivity, source code) ,application access control ,network access control , shared folders , remote access, mobile computing, and monitoring system access and use .	Employees involved in setting up and managing access control
Clean Desk Policy	Minimum requirements for maintaining a "clean	All employees

POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
	office" – so that sensitive/confidential information shown on screens, printed out and held on removable media is maintained.	
Anti-Virus & Anti-Malware Policy	Preventing the infection of computers in the DLS, networks and technological systems with computer viruses and other malicious programs, technical reviews and malware incident management.	Employees responsible for protecting the organization's infrastructure from malware
Router & Switch Policy	Baseline configurations, perimeter devices standard services and configurations.	Employees responsible for designing, implementing and managing networks e.g network admin.
Network Security Policy	Protecting network infrastructure, vulnerability scans, penetration testing, IDS/IPS, Protecting Network / Internet Perimeter, firewalls, routers, DMZs, third-Party Network Services.	Employees responsible for designing, implementing and managing networks e.g network admin.
Configuration Management Policy	General rules for secure configuration of hardware, software, services and networks, network asset inventory, configuration control, vulnerability management.	All DLS employees who are directly responsible for the configuration, management, oversight, and daily operations of DLS hardware, software and applicable documentation
Wireless Communication Standards	Standard configurations for wireless infrastructure devices, isolated and home wireless devices.	Employees responsible for designing, implementing and managing networks e.g network admin.
Wireless Communication Policy	General requirements for wireless infrastructure devices, isolated wireless devices requirements, home wireless devices requirements.	Employees responsible for designing, implementing and managing networks e.g network admin.
Remote Access Policy	Rules and requirements for remote access connection necessary to connect to the DLS network from any host and used to do work on behalf of DLS.	All employees, contractors, consultants, temporary, and other workers at DLS with a DLS-owned or personally-owned computer used to connect to the DLS

POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
		network
Area & Facility Access Policy	Define security parameters, physical access controls, public area controls, limited security area controls, high security area controls ,visitor access control, monitoring, securing offices and facilities.,	All employees, contractors, consultants, temporary, and other workers.
Technology Equipment Disposal Policy	Guidelines for the disposal of technological equipment and components owned by DLS to ensure the secure destruction of data stores.	All DLS employees and IT team who are responsible for disposal
Equipment & Storage Security Policy	Equipment siting and protection, maintenance, Secure Disposal or Re-Use, cabling security, environmental threats, electrical power, emergency power shutoff, shutdown procedures, alarm systems, emergency lighting, fire protection, temperature control, telecommunications.	DLS Asset owners and ICT team and administrators
Backup & Recovery Policy	Responsibilities and accountability, defining important data, backup types, backup procedure, backup frequency and retention, backup storage, backup media, backup documentation, restore policy.	DLS employees who are responsible of providing backup and restoration services to any DLS equipment such as IT administrators
Disaster Recovery Plan Policy	General rules in business continuity ,BCP plan, disaster recovery plan DR, requirements, asset register, criticality of service List ,data study, business impact analysis BIA, risk assessment, DR plan development, DR plan components, DR plan testing, review and update.	DLS Management staff , IT team responsible for configuring, maintaining, and monitoring information systems on DLS
Auditing Policy	Audit program and procedure, scope , criteria, reporting , documentation.	Cyber security employees and IT administrator
Database Security Policy	Physical DB security, use firewall, protect oracle listener, IP addresses(valid node checking), encryption, harden OS ,restrict OS access, DB installation, DB user management, privilege management , DBA responsibilities, system and application development, auditing and monitoring, change control, backup and recovery.	All those involved in DB operations at DLS including end user(external, internal) , system administrator, system operator , system and application developers , DB administrator, DB operators and contractors .
Information Logging Standards	General requirements, elements of the log, events to be logged, storage and retention, log review and analysis, log access.	Cyber security employees, IT and network administrators.

POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
Protective Monitoring Policy	Process monitoring, levels of protective monitoring, networks, IDS/IPS, firewalls, data traffic, user activities, log analysis and management, monitoring controls.	Cyber security employees, IT and network administrators.
Incident Response Policy	Roles and responsibilities, IR Plan, IR team, communication channels, escalating, reporting incidents and vulnerabilities, assessment and classification, incident response procedure and phases, training and awareness.	Cyber security employees, IT and network administrators.
Personnel Security Standard	Security Audit, terms and conditions of recruitment, management responsibilities, Disciplinary process, termination.	All employees , HR employees
Security Awareness & Training Policy	Security awareness training, role-based training, training records.	All employees , cyber security team, HR employees

Table 1: Set of policy documents

2.5 Application of information security policy

The policy statements made in this document and in the set of supporting policies listed in Table 1 have been reviewed and approved by the top management of DLS and must be complied with. Violation of these policies or failure to comply with by an employee may result in disciplinary action, up to and including termination of employment, according to the laws of the Civil Service Bureau related to the type of violation.

Questions regarding any DLS policy should be addressed in the first instance to the employee's immediate line manager.