DXC Luxoft Information Security Policy

PO-10-3-01-0-LUX(ENG)

Version 3.2

Table of contents

Document control

Document name	DXC Luxoft Information Security Policy	
Document type	Policy	
Document reference	PO-10-3-01-0-LUX-(ENG)	
Document approval	Suresh Gumma | Deputy CISO	06.08.2025
	Joanna Ayton | Senior Manager, Information Security	

1. Purpose

The purpose of this policy is to establish and maintain an Information Security Management System (ISMS) in accordance with ISO 27001 standards throughout DXC Luxoft (here and after referred to as a “Company”). It aims to implement administrative, technical, and physical security measures to minimize security risks, protect information assets, and ensure confidentiality, integrity, and availability of data.

2. Applicability

This policy applies to:

- All DXC Luxoft, customer, supplier, employee, and other third party confidential, proprietary, financial, personal, or other sensitive information stored, processed, or received using DXC Luxoft Information systems. The term “Information” applies regardless of whether the Information exists in digital, audio, electronic, or other form.
- Any employee of DXC Luxoft, any business partner, customer, supplier, sub-contractor, will either assist DXC Luxoft in delivering services, represent DXC Luxoft’ s interests to a customer or third party, or provide DXC Luxoft with a service.

3. Policy statement

DXC Luxoft’s management shall ensure:

- An Information Security Management System (ISMS) that incorporates a systematic approach to information security management is established, maintained, and continually improved.
- ISMS objectives are identified and based on a set of key performance indicators (KPIs). An effective operational security framework is implemented and maintained to achieve ISMS objectives. The achievement of ISMS objectives is assessed and reported to the Company’s management on an annual basis.
- The confidentiality, availability, and integrity of the DXC Luxoft customers’, suppliers’, employees’, and other third parties’ non-public information are assured. All reasonable administrative, technical, and physical security measures are implemented and maintained to protect non-public information against unauthorized access, disclosure, leakage, and/or loss.
- Information security risks are assessed at least annually, remediated, and maintained at acceptable levels.
- DXC Luxoft maintains continuous monitoring of its systems and will respond appropriately to potential cybersecurity events. Those events are treated with priority and managed in accordance with the DXC Luxoft incident response plan and relevant DXC Luxoft client agreements.
- The regulatory, legislative, and contractual requirements are met.
- DXC Luxoft is in conformance with and certified to the ISO 27001:2022 security standard.
- This Information Security Policy is reviewed and approved by DXC Luxoft’ s management on an annual basis.
- This Policy and its related standards represent a minimum set of information security requirements and serve as a framework to govern information security at DXC Luxoft.

4. Exception and variances

Exceptions or variances to this Information Security Policy must be sought and secured in writing from the ISMS owner.

5. Compliance

All DXC Luxoft employees and Third Parties (including contractors) should follow DXC Luxoft Information Security Policies, Rules and Guidelines. The failure to comply with the Information Security rules may result in disciplinary actions.