

I. Purpose

DXI Logistics LLC is committed to protecting the confidentiality, integrity and availability of all the information it produces, receives, manages and stores. This policy protects DXI's information assets against internal, external, deliberate or accidental threats, and supports compliance with the UAE Personal Data Protection Law (Federal Decree-Law No. 45 of 2021) and the UAE Federal Decree-Law No. 34 of 2021 on Combatting Rumours and Cybercrimes.

II. Scope

This policy applies to all employees, contractors and third parties who use DXI information, systems or devices, and to all information held by DXI in any form, including personal data relating to customers, agents, suppliers and employees.

III. Our commitments

DXI will:

- Classify information according to its sensitivity and handle confidential information securely.
- Treat all information, including third-party and personal data, as confidential and maintain its integrity.
- Comply with all applicable legal, regulatory and contractual requirements.
- Protect business continuity through backups and recovery arrangements.
- Make information available to authorised staff with minimum disruption.
- Raise staff awareness of information security through training.
- Control access to prevent unauthorised use of our systems.

IV. Access control

- Access to e-mail, cloud storage, the ERP/accounting system and other business systems is protected by individual user accounts, strong passwords and, where available, multi-factor authentication.
- Access rights are granted on a need-to-know basis according to each employee's role.
- When an employee leaves, all access is revoked on or before the last working day; mailbox and file contents are retained under management control for business and legal purposes for a defined period, then deleted.
- When an employee changes role, access is updated to match the new role.
- Passwords must never be shared, and must be changed immediately if compromise is suspected.

V. Devices, network and backup

- Business data is stored in managed cloud services with regular, tested backups.
- Firewalls, anti-malware protection and automatic operating-system and software updates are maintained on all company devices.
- Removable media may only be used where authorised by management.
- Mobile devices used to access company e-mail must be protected by a passcode.

VI. Incidents and data breaches

All actual or suspected information security incidents, including phishing, lost devices and data breaches, must be reported immediately to management and the IT function, which will contain, investigate and record them. Where personal data is affected, DXI will notify the UAE Data Office and affected individuals where required by law.

VII. CCTV

CCTV operates at DXI's premises for security purposes, in line with the requirements of Dubai's Security Industry Regulatory Agency (SIRA). Recordings are retained for the required period and may be viewed only by authorised personnel (management, Operations Manager, HR and security personnel).

VIII. Maintaining compliance

- The IT function maintains the information security procedures and supporting documents.
- Managers implement this policy within their teams and report weaknesses to management.
- Training is provided at induction and periodically thereafter.
- Breaches of this policy may result in disciplinary action, up to and including termination of employment.

This policy is approved by top management and is reviewed annually.

Approved by:

Jerry Nazzal
Group President

This policy is effective from Oct. 2026 and will be reviewed by Oct. 2027, or earlier if required by changes in UAE law or DXI operations.