DHL Express Turkey Information Security Policy

DHL Express Turkey Information Security Policy defines the basic requirements of the Information Security measures that must be implemented in DPDHL. The basic principle behind Information Security within DPDHL is to meet or exceed ISO - Information Security Management Standard (ISO 27002: 2013) control requirements, as well as being fully compliant with legal obligations and local regulations. In this way; we ensure business continuity, minimize the risks and damages that may arise and maximize the return on investment and business opportunities by protecting all DPDHL Group information -which could be digital, hardcopy or oral- from threats.

Information Security is applied with the scope of:

Confidentiality: Ensuring that information is accessible to those with authorized access.
Integrity: Safeguarding the accuracy and completeness of information, and processing methods, and ensuring that a transaction cannot be disputed.
Availability: Ensuring that authorized users have access to information and associated assets, when required.

- Ensure a high level of confidentiality and accessibility for all data processed in systems.
- Provide data integrity and confidentiality to meet the requirements of all DPDHL departments and subsidiaries.
- Ensure availability of DPDHL information systems.
- Ensure the proper conduct of Information Security for DPDHL business operations.
- Protect information assets against all kinds of threats from inside or outside, intentionally or unintentionally, to ensure access to information through business processes as necessary, and to perform continuous improvement.
- Increasing awareness of all employees by providing Information Security Awareness and Data Protection trainings.
- Prepare, maintain and test business continuity plans.
- Periodically assessing the existing risks in terms of Information Security and make action plans where necessary.
- Prevent any conflicts of interest with the contracts.
- Comply with DPDHL Group Information Security standards.
- Process the personal data of our customers, employees and providers in accordance with the local data protection law.