T Ü R K Ç E

Bilgi Güvenliği Politikası

TS EN ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemin ana teması;**DHL Freight Taşımacılık ve Lojistik Hizmetleri A.Ş**. bilgi sistemlerinde; insan, altyapı, yazılım, donanım, müşteri bilgileri, kuruluş bilgileri, üçüncü şahıslara ait bilgiler ve finansal kaynaklar içerisinde bilgi güvenliği yönetiminin sağlandığını göstermek, risk yönetimini güvence altına almak, bilgi güvenliği yönetimi süreç performansını ölçmek ve bilgi güvenliği ile ilgili konularda üçüncü taraflarla olan ilişkilerin düzenlenmesini sağlamaktır.
Bu doğrultuda **BGYS Politikamızın** amacı;

- İçeriden veya dışarıdan, bilerek ya da bilmeyerek meydana gelebilecek her türlü tehdide karşı **DHL Freight Taşımacılık ve Lojistik Hizmetleri A.Ş.** bilgi varlıklarını korumak, bilgiye erişebilirliği iş süreçlerinin gerektirdiği şekilde sağlamak, yasal mevzuat gereksinimlerini karşılamak, sürekli iyileştirmeye yönelik çalışmalar yapmak,

- Yürütülen tüm faaliyetlerde Bilgi Güvenliği Yönetim Sisteminin üç temel öğesinin sürekliliğini sağlamak:

  Gizlilik: Önem taşıyan bilgilere yetkisiz erişimlerin önlenmesi,

  Bütünlük: Bilginin doğruluk ve tamlığının sağlandığının gösterilmesi,

  Erişebilirlik: Yetkisi olanların gerektiği hallerde bilgiye ulaşılabilirliğinin gösterilmesi,

- Sadece elektronik ortamda tutulan verilerin değil; yazılı, basılı, sözlü ve benzeri ortamda bulunan tüm verilerin güvenliği ile ilgilenmek,

- Bilgi Güvenliği Yönetimi eğitimlerini tüm personele vererek bilinçlenmeyi sağlamak.

E N G L I S H

Information Security Policy

The main theme of the TS EN ISO 27001:2022 Information Security Management System is to demonstrate that information security management is provided within the information systems of **DHL Freight Taşımacılık ve Lojistik Hizmetleri A.Ş**.; people, infrastructure, software, hardware, customer information, organisational information, third party information and financial resources, to ensure risk management, to measure information security management process performance and to regulate relations with third parties on information security issues.In this direction, the purpose of our **ISMS Policy** is;

- To protect the information assets of **DHL Freight Taşımacılık ve Lojistik Hizmetleri A.Ş.** against all kinds of threats that may arise from inside or outside, intentionally or unintentionally, to ensure accessibility to information as required by business processes, to meet the requirements of legal regulations, to work towards continuous improvement,

- To ensure the continuity of the three basic elements of the Information Security Management System in all activities carried out:

  Confidentiality: Preventing unauthorised access to important information,

  Integrity: Demonstration that the accuracy and completeness of the information is ensured,

  Accessibility: Demonstrating that authorised persons can access information when necessary,

- To deal with the security of not only the data kept electronically, but also all data in written, printed, verbal and similar media,

- To increase awareness raising by providing Information Security Management Awareness trainings to all employees.

- Bilgi Güvenliğindeki gerçekte var olan veya şüphe uyandıran tüm açıklıkların, BGYS Ekibine bildirilmesini ve BGYS Ekibi tarafından soruşturulmasını sağlamak.
- Bilgi güvenliği yönetimine yönelik sorumlulukların tanımlanmış rollere atanmasını sağlamak amacıyla, her personelin bilgi güvenliği görev ve sorumlulukları belirlemek ve dokümante etmek, bu roller ve sorumluluklar, bilgi güvenliği yönetim sistemimizin etkin bir şekilde işlemesini ve sürekli iyileştirilmesini desteklemek.
- İş süreklilik planları hazırlamak, sürdürmek ve test etmek.
- Bilgi Güvenliği konusunda periyodik olarak değerlendirmeler yaparak mevcut riskleri tespit etmek. Risk değerlendirmesi sonucunda, aksiyon planlarını gözden geçirmek ve takibini yapmak.
- Sözleşmelerden doğabilecek her türlü anlaşmazlık ve çıkar çatışmasını engellemek.
- Bilgiye erişilebilirlik ve bilgi sistemleri için iş gereksinimlerini karşılamak.
- DHL Grup Bilgi Güvenliği standartlarına uymak.
- Kişisel Verileri Koruma Kanuna uygun olarak hukuki, organizasyonel ve teknik tedbirleri almak.
- Bilgi güvenliği politikamızı iklim değişikliği konusundaki hassasiyetimizi göz önünde bulundurarak, karbon ayak izimizi azaltmayı, sürdürülebilir BT çözümlerini teşvik etmeyi ve operasyonlarımızın çevresel sürdürülebilirlik ilkelerine uygun olmasını sağlamayı taahhüt ederiz.

- To ensure that all actual or suspected gaps in Information Security are reported to the ISMS Team and investigated by the ISMS Team.
- To determine and document the information security duties and responsibilities of each personnel in order to ensure that responsibilities for information security management are assigned to defined roles, these roles and responsibilities support the effective operation and continuous improvement of our information security management system.
- To prepare, maintain and test business continuity plans.
- To identify existing risks by making periodic assessments on Information Security. To review and follow up action plans as a result of risk assessment.
- To prevent any disputes and conflicts of interest that may arise from contracts.
- Meet business requirements for information accessibility and information systems.
- Comply with DHL Group Information Security standards.
- To take legal, organisational and technical measures in accordance with the Personal Data Protection Lav (KVKK).
- We are committed to reducing our carbon footprint, promoting sustainable IT solutions and ensuring that our operations comply with the principles of environmental sustainability, taking into account our sensitivity to climate change in our information security policy.

Ahmet Murat Kavrar
Managing Director
DHL Freight Türkiye