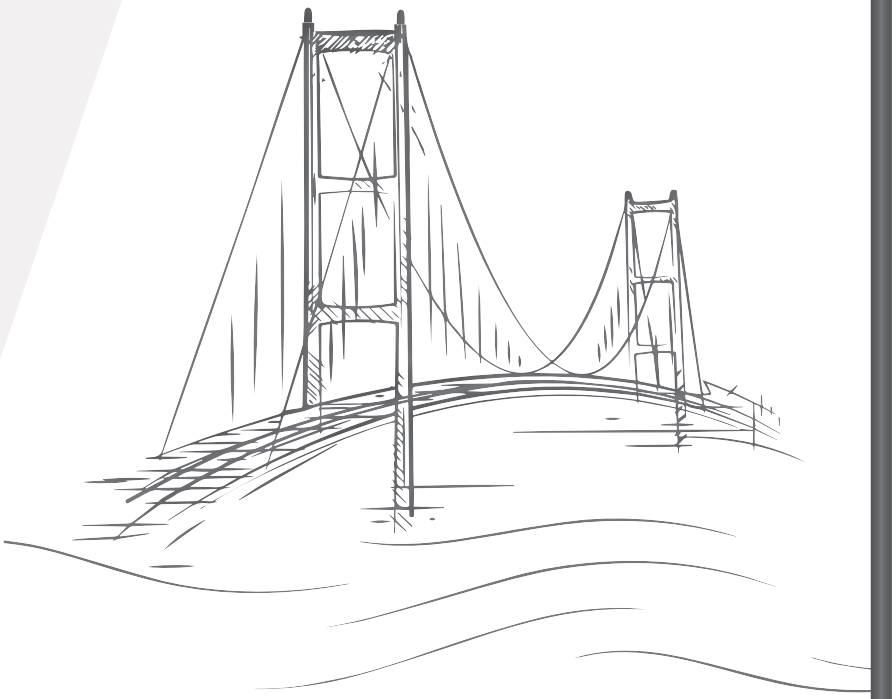
ÇANAKKALE MOTORWAY AND BRIDGE

INFORMATION SECURITY POLICY

ÇANAKKALE OTOYOL VE KÖPRÜSÜ

BİLGİ GÜVENLİĞİ POLİTİKASI



1915 ÇANAKKALE

INFORMATION SECURITY AND PERSONAL DATA MANAGEMENT SYSTEM

Çanakkale Motorway and Bridge Construction Investment and Operation Inc.; In alignment with the Information Security Management System (ISMS) Standard, we hereby commit to ensuring secure access to the information assets of all individuals whose data we process, and pledge to uphold the following principles:

1. To effectively manage information assets by identifying their security values, requirements, and associated risks, and implementing appropriate controls within the framework of the Information Security Management System.
2. To define a comprehensive methodology for identifying information assets, their values, security needs, vulnerabilities, threats, and the frequency of such threats.
3. To establish a framework for assessing the potential impacts of threats on the confidentiality, integrity, and availability of information assets.
4. To outline the procedures and principles for risk treatment.
5. To continuously monitor risks by evaluating technological developments and expectations within the defined service scope.
6. To ensure full compliance with applicable national and international regulations, legal and statutory requirements, contractual obligations, and information security expectations arising from corporate responsibilities toward internal and external stakeholders.
7. To reduce the impact of information security threats on service continuity and maintain uninterrupted operations.
8. To uphold the capability to promptly respond to potential information security incidents and minimize their effects.

BİLGİ GÜVENLİĞİ VE KİŞİSEL VERİ YÖNETİM SİSTEMİ

Çanakkale Otoyol ve Köprüsü İnşaat Yatırım ve İşletme A.Ş.; Bilgi Güvenliği Yönetim Sistemi Standardı doğrultusunda, verisini işlediğimiz kişilerin bilgi varlıklarına güvenli bir şekilde erişimini sağlamak üzere aşağıdaki hususları taahhüt eder:

1. Bilgi Güvenliği Yönetim Sistemi doğrultusunda; Bilgi varlıklarını yönetmek, varlıkların güvenlik değerlerini, ihtiyaçlarını ve risklerini belirlemek, güvenlik risklerine yönelik kontrolleri geliştirmek ve uygulamak.
2. Bilgi varlıkları, değerleri, güvenlik ihtiyaçları, zafiyetleri, varlıklara yönelik tehditlerin, tehditlerin sıklıklarının saptanması için yöntemlerin belirleyeceği çerçeveyi tanımlamak.
3. Tehditlerin varlıklar üzerindeki gizlilik, bütünlük, erişilebilirlik etkilerini değerlendirmeye yönelik bir çerçeveyi tanımlamak.
4. Risklerin işlenmesi için çalışma esaslarını ortaya koymak.
5. Hizmet verilen kapsam bağlamında teknolojik beklentileri gözden geçirerek riskleri sürekli takip etmek .
6. Tabi olduğu ulusal veya uluslararası düzenlemelerden, yasal ve ilgili mevzuat gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülüklerini karşılamaktan, iç ve dış paydaşlara yönelik şirket sorumluluklarından kaynaklanan bilgi güvenliği gereksinimlerini sağlamak.
7. Hizmet sürekliliğine yönelik bilgi güvenliği tehditlerinin etkisini azaltmak ve sürekliliğe katkıda bulunmak.
8. Gerçekleşebilecek bilgi güvenliği olaylarına hızla müdahale edebilecek ve olayın etkisini en aza indirecek yetkinliğe sahip olmak.

9. To maintain and enhance the level of information security over time through a cost-effective control infrastructure.

10. To provide regular training that promotes awareness and understanding of information security among all personnel, and to repeat these programs at defined intervals.

11. To continually improve the Information Security Management System by evaluating implementation results, audit findings, and corrective actions.

12. To operate the Information Security Management System in an integrated manner with other management systems implemented within the organization.

13. To protect and enhance the corporate reputation by mitigating risks and preventing adverse impacts arising from information security threats.

9. Maliyet etkin bir kontrol altyapısı ile bilgi güvenliği seviyesini zaman içinde korumak ve iyileştirmek.

10. Tüm personele Bilgi Güvenliği konularında farkındalık, bilgilendirme ve bilinçlendirme eğitimleri vermek. Bu eğitim belirli periyotlarda tekrarlamak.

11. Bilgi Güvenliği Yönetim Sistemi Standardı kapsamındaki uygulama, denetim, düzeltici faaliyet sonuçlarını göz önünde bulundurarak, sistemi sürekli iyileştirmek.

12. Bilgi Güvenliği Yönetim Sistemi Standardını firma bünyesindeki diğer yönetim sistemleriyle birlikte bütünleşik olarak yürütmek.

13. Firma itibarını geliştirmek, bilgi güvenliği temelli olumsuz etkilerden korumak.