

Bir Bakışta PCI Security Standards Council

PCI Security Standards Council (PCI SSC), kart sahibi verilerini korumak için güvenlik standartlarının sürekli geliştirilmesi, iyileştirilmesi, saklanması, yayımlanması ve uygulanmasına yönelik küresel bir forumdur. Görevimiz, eğitim, farkındalık ve paydaşlar tarafından etkin uygulamayı teşvik eden standartlar geliştirerek ve bunlara ilişkin hizmetleri destekleyerek küresel boyutta kart sahibi veri güvenliğini arttırmaktır. Bunu, karar verme sürecimize rehberlik edecek ve her girişimin misyonumuzla uyumlu olmasını ve küresel ödemeler sektörünün ihtiyaçlarını desteklemesini sağlayacak stratejik bir çerçeve ile başarıyoruz .

PCI SSC; American Express, Discover, JCB International, Mastercard, UnionPay ve Visa Inc. temsilcilerinden oluşan, karar verici bir [Yürütme Kurulu](#) tarafından yönetilmektedir. PCI Standartlarına uyumluluğun kontrolü ve uyumsuzluk cezalarının belirlenmesi, PCI SSC tarafından değil; her bir ödeme markasının kendisi tarafından gerçekleştirilir. Bu belge; paydaşların, kart sahibi verilerinin güvenliğini artırma amacı doğrultusunda PCI SSC'nin Stratejik Çerçeveyi nasıl kullandığını açıklamaktadır.

ÖDEME GÜVENLİĞİ NEDEN ÖNEMLİDİR?

- Kart sahibi verilerinin güvenliği herkesi etkiler
- Kart sahibi verilerinin ihlali ya da çalınması, büyük çapta finansal kayıplara yol açabilir
- Kart sahibi verilerinin gizliliğinin ihlal edilmesi ödeme ekosisteminin tamamını olumsuz şekilde etkileyebilir
- PCI Standartlarının uygulanması, kart sahibi verilerinin güvenliğini arttıracak ve dolandırıcılığın engellenmesine katkı sağlayacaktır

PCI SSC'nin Görevini Tanımlayan Dört Stratejik Temel

Stratejik Çerçeve, PCI SSC'ye kart sahibi verilerinin güvenliğine ilişkin görevini tanımlayan dört temel faaliyeti sunar. Temel faaliyetler içinde şunlar bulunur:



PCI Standartlarının geliştirilmesi süreçleri ve standartların paydaşların desteğiyle uygulanması için **sektör katılımını ve bilgisini arttırmak**. Bu, standartların ve kaynakların sektörün ihtiyaçlarını ve zorluklarını yansıtması ve ele almasını sağlar.



Güvenliği sağlamak için çeşitli ortamları, teknolojileri ve metodolojileri destekleyen **güvenlik standartlarını ve doğrulama programlarını geliştirmek**. Bu, güvenli ticareti destekleyen ve mümkün kılan standartları ve kaynakları ve bu standartları karşılamak için farklı yaklaşımları kullanma esnekliğini sağlar.



Daha geniş kapsamlı ödeme kabulünü desteklemek için PCI Standartlarının ve kaynaklarının geliştirilmesiyle **yeni ödeme kanallarını güvenli hâle getirmek**. Bu, yeni ve gelişmekte olan mobil ve nesnelerin interneti gibi kart ve kart temelli ödeme kanallarında güvenli şekilde ticareti mümkün kılar.



Gereksiz tekrarı azaltmak ve etkin uygulamayı desteklemek için PCI Standartlarının birbirleriyle olan **uyumluluğunu ve tutarlılığını arttırmak**.

PCI SSC Neler Yapar?

Teknik Güvenlik Standartları



- Farklı çapta 15 güvenlik standardını ve bunları destekleyen programları geliştirir ve sürdürür
- Sektör geri bildirimine ve ortaya çıkan tehditlere göre standartları ve programları sistematik olarak günceller
- Kart çıkaran kuruluşlar, üye iş yerleri, sağlayıcılar ve çözüm sağlayıcıları, kart kabul eden kuruluşlar ve işlemci kuruluşlar için ödeme güvenliğine dair çözümler sunar

Profesyoneller ve Ürünler için Doğrulama Kaynağı



- Sıkı güvenlik gereksinimlerini karşılayan ödeme güvenliği ürünlerini bulmaları için kuruluşlara faydalı kaynaklar sağlar
- PCI Standartlarına uyumluluğu doğrulayacak çeşitli denetçileri kalifiye eder ve listesini yayımlar
- Ödeme çözümlerini test eden ve onaylayan güvenlik değerlendirme laboratuvarları ağını tasdik eder ve bunların listesini yayımlar
- Veri ihlallerini soruşturan adli müfettişleri eğitir, onaylar ve listesini yayımlar

Güvenlik Eğitimi



- Çok çeşitli yüz yüze, bilgisayar tabanlı ve eğitmen liderliğinde çevrimiçi eğitim programı sunar
- PCI Uzmanları ve İç Denetçiler için Güvenlik Farkındalık Eğitimi ve yetkinliğini sağlar

Güvenlik İlkeleri



- Yaygın siber güvenlik tehditlerine dair eğitim ve rehberlik sağlaması açısından sektör bültenleri yayımlar
- Yeni ve gelişmekte olan teknolojiler için kapsamlı teknik kılavuzlar yayımlar

Paydaş Katılımı



- Yorumlar için İstek (RFC) süreci, Bölgesel Katılım Kurulu, Küresel Yönetim Değerlendirme Masası, Teknik Danışma Kurulu, Danışman Heyeti gibi katılım fırsatları sunar
- Paydaşlara, PCI Standartlarını ve Kılavuzlarını şekillendirebilecekleri Stratejik ve Özel Üyelik ile Katılımcı Organizasyon üyelik imkanlarını sunar
- Paydaşların aktif teknik girdi sağlayabilecekleri Çalışma Kolları ve Özel İlgi Grupları bulunur
- Kuzey Amerika, Avrupa, Asya Pasifik, Latin Amerika, Hindistan ve Afrika/Orta Doğuda yıllık Topluluk Buluşmaları ve Grup Toplantıları düzenler
- Devam eden web seminerleri ve çeşitli yayımlar ile paydaşların PCI Standartları ve ödeme güvenliğine ilişkin ortaya çıkan sorunlar hakkında güncel kalmasına yardımcı olur

PCI Standartlarına Kimler Uyar?

PCI Veri Güvenliği Standardı ve yürürlükteki diğer PCI Standartlarına uyumluluk, kart sahibi verilerini saklayan, işleyen veya ileten kuruluşlar için gerekli olabilir. PCI Standartları, ödeme işlemi kabul eden veya işleyen kuruluşların yanı sıra söz konusu işlemlerde kullanılan uygulamaların ve cihazların yazılım geliştiricilerine ve üreticilerine yönelik olarak da hazırlanmıştır.

Uyumluluğun Sorumlusu Kimdir?

PCI Standartlarına uyumluluk ve bunun uygulanması, PCI SSC'nin değil, ödeme markalarının ve kart kabul eden bankaların görevidir. PCI SSC'nin ödeme markası üyelerinin her biri, ilgili kart sahibi verilerinin korunması için kendi özel PCI uyumluluk programlarına sahiptir. Kuruluşlar, uyumluluk programları hakkında bilgi almak için doğrudan ödeme markalarıyla iletişime geçmelidirler.

Her ödeme markasının, kart sahibi verilerinin güvenliğini sağlamak amacıyla oluşturduğu kendi özel kuralları ve süreçleri mevcuttur. Bunlar, sırasıyla kart kabul eden bankalar tarafından uyarlanır ve uygulanır, buna karşılık kart kabul eden bankalar da müşterilerinin çeşitli PCI standartları uyarlamaları, uygulamaları ve uyumlulukları için üstlenmeleri gereken yaklaşımı ortaya koyan kendi kurallarını belirler.

Uyum. PCI Standartları uyum programları hakkında bilgi için bankanızla (kart kabul eden kuruluş) veya ödeme markasıyla doğrudan iletişime geçebilirsiniz. İletişim bilgileri [web sitemizdeki](#) 1142 no'lu SSS (Sıkça Sorulan Sorular) kısmında yer almaktadır.

PCI SSC, uyum değerlendirme raporlarının kopyalarını almaz ve uyumsuzluktan kaynaklı cezalara veya tazminatlara ilişkin herhangi bir dahli ya da bilgisi bulunmaz.

Adli Soruşturmalar. Onaylı PCI Adli Müfettişlerinin bir listesini [web sitemizde](#) bulabilirsiniz. PCI SSC, adli soruşturmaların herhangi bir aşamasına dahil değildir ve soruşturma kapsamına oluşturulan adli raporların kopyalarını almamaktadır. Veri ihlali durumunda kuruluşlar ayrıca yerel ve bölgesel yasal gereklilikleri takip etmelidir.

Değerlendirmeler. Bir PCI denetçisinin, PCI Onaylı bir Laboratuvarın veya bir PCI Adli Müfettişinin hizmetlerine ihtiyaç duyarsanız iletişim bilgilerini web sitemizde bulabilirsiniz. Ücretler ve masraflar kuruluş ve değerlendirmeyi gerçekleştiren firma arasında belirlenir. PCI SSC, sunulan hizmetlere ilişkin talep edilen ücret ve masrafları belirlemez veya bunlar üzerinde herhangi bir yetkisi yoktur.

PCI Standartları Hakkında Daha Fazla Bilgi

Tüm PCI Standartları ve belgeleri, eğitim ve yetkinlikler, kalifiye edilmiş denetçilerin listesi ve onaylı çözümler ve ürünler hakkında daha fazla bilgiyi [web sitemizde](#) bulabilirsiniz.