HP GÜVENLİK ÖNLEMLERİ ÖZETİ

HP, Müşteri verilerini korumak amacıyla kendi ve müşteri bilgilerinin (HP'nin Müşteri ve Veri İşleme Eklentisi'nde tanımlandığı Kişisel Veriler dahil) gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak üzere politikalar, uygulamalar, prosedürler ve kuruluş yapılarını içeren sağlam bir bilgi güvenliği denetimleri setine uyum sağlar. Aşağıda HP'nin şirket genelindeki teknik/kurumsal güvenlik tedbirlerine genel bir bakış edinebilirsiniz.

1. Güvenlik İlkesi

   HP; HP ve Müşteri verilerini korumak amacıyla genel olarak geçerli ilke, standart ve prosedürleri korur. HP'nin güvenlik ilkelerinin ayrıntıları, HP'nin veri ve sistemlerinin bütünlüğünü korumak amacıyla gizlidir. Bununla birlikte temel politikalarımızın özetleri aşağıda yer almaktadır.

2. Bilgi Güvenliği Kuruluşu

   HP Bilgi Güvenliği programı, kuruluşun bilgi güvenliği stratejisini ve denetimlerini yönlendirmek ve yönetmek üzere tasarlanmıştır. Bu sistem, HP'nin güvenlik ilkelerine ve denetimlerine kurumsal düzeyde uyumun yanı sıra müşterilerinin güvenlik gereksinimlerine de uyulmasını sağlar. Endüstri standardı siber güvenlik çerçeveleri, yasaları ve düzenlemeleri ile uyumlu olarak yapılandırılan Çerçeve, HP'nin gelişmiş tehdit yatay yapısına uyum sağlamak amacıyla yılda bir gözden geçirilir.

3. Siber Güvenlik Risk Yönetimi

   HP'nin siber güvenlik risk yönetimi programı, bilgi varlıklarının gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak üzere tasarlanmıştır. Bu program, siber güvenlik risklerini belirlemeye, değerlendirmeye, öncelik vermeye, tedavi etmeye, gidermeye, izlemeye ve raporlamaya yönelik tutarlı bir yaklaşım sunar. HP, Risk İştahı'nı bu iştahtan kaynaklanan değişim derecesi olarak kabul edilebilen kayıp maruziyet düzeyi ve Risk Toleransı olarak tanımlar. Riskler, tanımlanmış bir yöntem kullanılarak değerlendirilerek HP'nin bilgi güvenlik risklerini kabul edilebilir bir düzeye azaltmasını sağlar. Bu program, HP'nin Kurumsal Risk Yönetimi süreciyle uyumludur.

4. İK Güvenliği

   HP İnsan Kaynağı Güvenliği politikası, tesislere, bilgi sistemlerine ve diğer varlıklara erişim süreçleri oluşturarak, çalışanın yaşam döngüsü boyunca bilgi güvenliğini sağlar. Buna gizlilik ve açıklama dışı anlaşmalar aracılığıyla yazılı bildirim alma ile birlikte arka plan tarama işlemlerini yürütme de dahildir. HP çalışanı adaylarının ilgili yasa, yönetmelik ve etik değerlere uygun olarak arka plan doğrulama kontrollerini tamamlaması gerekir.

5. Varlık Yönetimi

   HP'nin, teknik bilgi varlıklarını tanımlamaya, önemli varlıkları kategorilere ayırmaya ve Kişisel Verileri içerenler de dahil olmak üzere her bilgi sınıflandırma türü için belgelenen işleme prosedürlerini tutmaya yönelik bir süreci vardır. Bu prosedürler depolama, iletim, iletişim, erişim, günlük kaydı, saklama, yıkım, bertaraf etme, olay yönetimi ve bildirim ihlalini kapsar. HP güvenlik ilkeleri ve standartları, medyanın güvenli bir şekilde bertaraf edilmesi görevini de karşılar.

6. Veri Güvenliği

   HP'nin Veri Güvenliği programı, verilerin gizliliğini, özgünlüğünü ve bütünlüğünü korumak için uygulanması gereken güvenlik uygulamalarını ve teknik kontrolleri özetler. Yasal gereksinimler, değer, kritiklik ve izinsiz ifşa veya değiştirme konusundaki hassasiyet, bilgilerin HP'nin Veri Güvenliği politikası altında nasıl sınıflandırıldığını belirleyen faktörlerden birkaçıdır. Bu ilke, veri işleme prosedürlerine ek olarak veri şifrelemeyi, silmeyi, toplamayı ve işlemeyi, saklamayı, yedeklemeyi ve veri kaybını önlemeyi ana hatlarıyla içerir.

7. Erişim Denetimi

   HP, mantıksal erişim kontrolü için en az ayrıcalık ilkesi kullanarak, benzersiz kullanıcı kimlikleri ve parolaları üzerinden kullanıcı erişimi sağlar. Parola ilkesi karmaşıklık, güç, geçerlilik ve parola geçmişi denetimlerini tanımlar. Erişim hakları personelin ayrılmasından sonra düzenli olarak gözden geçirilir ve iptal edilir. Katılım sırasında istemci sistemlerine erişim vermek ve iptal etmek için kullanıcı hesabı oluşturma ve silme üzerinde anlaşılan prosedürler uygulanır.

8. Şifreleme

   HP, bilgi varlıklarının gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için şifrelemeye yönelik bir dizi sağlam süreç tanımlamıştır. Onaylanan protokoller, kişisel veri içerenler de dahil olmak üzere belirli varlıklar için şifreleme gerektirir. Şifreleme programımız, verilere sadece yetkili tarafların erişebileceğini garanti ederek, bilgileri ve iletişimi güvenceye almak için matematiksel tekniklerin kullanılmasını gerektirir. HP bilgi güvenlik programının önemli bir bileşeni, verileri yetkisiz erişime ve yetkisiz erişime karşı korumaktır.

9. Fiziksel Güvenlik ve Çevre Güvenliği

   HP tesisleri; güvenlik görevlileri, elektronik erişim kontrolü ve kapalı devre televizyonlar (CCTV) dahil çeşitli fiziksel ve elektronik erişim kontrolleri kullanılarak güvenli hale getirilir. Tesisler ayrıca önemli hizmetleri desteklemek üzere UPS ve/veya dizel jeneratörler kullanılarak, sıcaklık kontrolü ve güç yedekleri dahil gerekli altyapı desteğiyle de donatılmıştır. Tüm HP personeli kayıtlı olup, uygun kimlik rozetlerini taşımaları gerekir.

10. İşlem Yönetimi

    HP; iş istasyonları, sunucular ve ağ ekipmanları dahil olmak üzere teknoloji altyapısı için minimum katılaştırma gereksinimleri kurmuştur. Bu aygıtlar, işletim sistemine ve uygulanan denetimlere göre değişen önceden sıkıştırılmış işletim sistemi görselleri kullanır. Ayrıca HP, 7/24 izlenen ve yönetilen Ağ Müdahale Algılama/Önleme Sistemleri (NIDS/NIPS) kurmuştur.

11. İletişim Güvenliği

    İletişim Güvenliği, şirket ağlarında bilginin korunmasını sağlar. Bu, ağ güvenlik bileşenlerinin (ör. güvenlik duvarlarının), ağların ayrıştırılmasından ve ayrıca web filtreleme ve e-posta kullanımı denetimlerinin yüklenmesinden ve yönetilmesinden oluşur. Ayrıca, yetkisiz erişim veya veri ihlalini tespit etmek ve önlemek için iletişim kanallarının izlenmesini ve yönetilmesini içerir.

12. Sistem Güvenliği

    HP'nin politikasında, yaşam döngüsü boyunca sistemler ve yazılımlar için güvenli bir geliştirme yöntemi zorunludur. Yazılım Geliştirme Yaşam Döngüsü başlatma, geliştirme/devralma, uygulama, işlemler ve elden çıkarma işlemlerini kapsar. Tüm sistem bileşenleri, genel güvenlik üzerindeki etkilerine göre değerlendirilir. HP, kullanıcı kimlik bilgisi doğrulama, dijital imzalar, şifreleme, güvenli iletişim protokolleri ve uygun ağ güvenlik alanında işlem ayrıntılarını depolama dahil, uygulama hizmeti işlemlerine yönelik denetimler oluşturmuştur. Düzenli iç güvenlik açığı taramaları da gerçekleştirilmiştir.

13. Üçüncü Taraflar ve Alt Yükleniciler

    HP, kapsamlı sözleşmeye bağlı güvenlik gerekliliklerine uygun alt yüklenicilerin seçilmesinin talep edildiği süreçlere sahiptir. Uygun tedarikçilerin HP veya müşteri verilerini işlemesi ya da HP ağına erişmesi için HP Siber Güvenlik, bir bilgi güvenlik programını fiziksel, teknik ve yönetimsel güvencelerle doğrulamak üzere bir risk değerlendirmesi yürütür. Bu değerlendirme, tedarikçinin HP bilgilerine erişebilmesi için gereklidir.

14. Bilgi Güvenliği Olay Yönetimi

    HP'nin amacı, kapsamı, rolleri, sorumlulukları, yönetim taahhüdünü, kuruluş koordinasyonunu, uygulama prosedürlerini ve uyum kontrollerini özetleyen kapsamlı bir Siber Olay Yönetim Süreci vardır. Bu süreç her sene gözden geçirilir ve güncelleştirilir. Olay anında müdahale ve kriz yönetimi eğitimi almış HP Siber Güvenlik personeli de dahil olmak üzere Siber Olay Müdahale Ekibi, süreç ve olaylarla ilgili düzenli olarak en iyi değerlendirmeleri yapar.

15. İş Sürekliliği Yönetimi

    HP'nin genel Süreklilik Operasyonu programı; iş birliğine dayalı, standartlaştırılmış ve belgelenen planlama süreçleriyle uçtan uca süreklilik sağlar. Şirket, yılda en az bir etkinliğin sağlanması, test edilmesi ve güncellenmesi amacıyla iş sürekliliği planlarını düzenli aralıklarla gerçekleştirir. Ayrıca, iş sürekliliği planında yer alan tüm personel uygun eğitimi alır.

16. Uyumluluk

    Uyumluluk, HP'nin etkin bir bilgi güvenlik programı için yasal, sözleşmeye dayalı ve kurum içi beklentileri karşılamaya olan yaklaşımını biçimlendirir. Düzenli bilgi güvenliği incelemeleri, protokollerin her iş grubunun işlemleriyle bütünleştirilmesini sağlar. İnceleme süreci, gereksinimler gelişmeye devam ettikçe belgeleri de mevcut yasal yükümlülükleri yansıtacak şekilde güncel tutar.

17. Ödeme Kartı Endüstrisi

    Payment Card Industry (PCI) çerçevesi, HP'nin PCI Uyumu'nu sağlama yaklaşımına yol gösterir, iş sorumluluklarını ve güvenlik denetimlerini PCI DSS ile uyumlu hale getirir. HP, güvenlik duvarları gibi ağ güvenlik denetimlerinin yüklenmesi ve bakımının yapılmasıyla bu denetimlerin PCI Uyum gereksinimlerini karşıladığından emin olur.

18. HP Ürün Güvenliği

    HP Ürün Güvenliği, HP ürünlerini güvence altına almak amacıyla kod imzalama, ürün güvenlik açıklarını yönetme, güvenlik bültenleri yayımlama ve ürün güvenlik sorunlarını raporlama gibi temel uygulamaları kapsar. Bu önlemler, HP ürünlerinin kullanıcılar için güvenli ve güvenilir kalmasını sağlar. Ürün güvenliği, müşteri güveninin korunmasına ve olası tehditlere karşı korunmasına yardımcı olduğundan HP'de son derece önemlidir.

19. HP Hizmet Güvenliği

    HP Hizmet Güvenliği, HP müşterilerine sunulan hizmetleri güvenceye almak üzere gerçekleştirilen temel uygulamaları kapsar. Bu ilke; HP altyapı özellikleri, üçüncü taraf barındırma hizmetleri, iş ortağı tarafından sunulanlar ve müşteri tarafından sunulan ortamlar dahil olmak üzere çeşitli hizmet güvenliği alanlarına yöneliktir. Bu önlemler, HP hizmetlerinin kullanıcılar için güvenli ve güvenilir kalmasını sağlar. HP, sağlam güvenlik uygulamaları uygulayıp ürün ve hizmetlerinin güvenliğini ve bütünlüğünü sağlayarak tüm kullanıcılar için güvenli ve güvenilir bir ortam sunar.