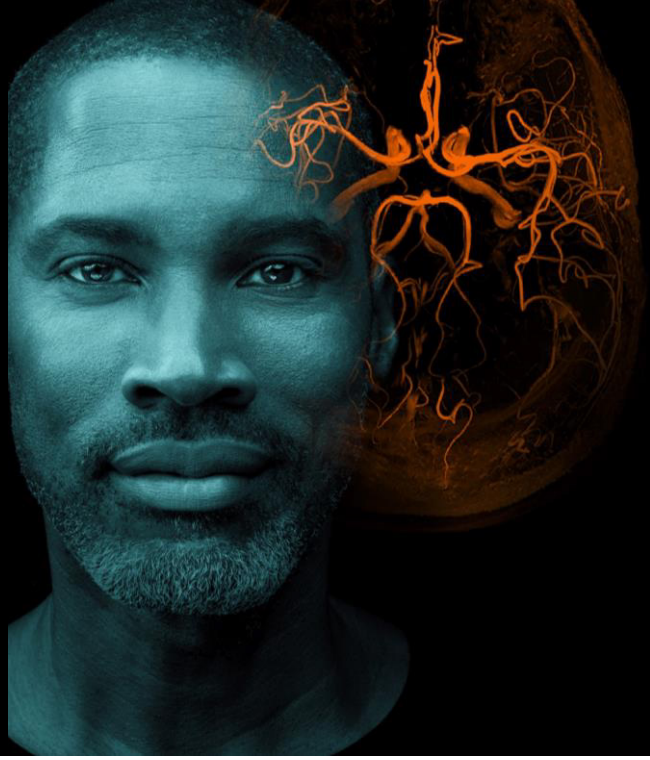
Siemens Healthineers Kurumsal Siber Güvenlik

Siber Güvenlik

Siber güvenliğimiz için rehberlik ve yetkilendirme



Bu politika, Siemens Healthineers'ın sorumluluğu altında bulunan veri işleme faaliyetleri dahil olmak üzere, Siemens Healthineers'ın bilgi sistemlerinin yönetimi, işletimi ve kullanımı süreçlerinde yer alan tüm çalışanları, yüklenicileri ve üçüncü taraf iş ortaklarını kapsamaktadır. Siber güvenlik hedefleri ve girişimleri, iş hedefleriyle ve risk toleransıyla uyumun sağlanması amacıyla, yönetim tarafından periyodik olarak gözden geçirilecektir.

Kurumsal Siber Güvenlik, Siemens Healthineers'ın varlıklarını siber tehditlere karşı korumak üzere kapsamlı bir çerçeve oluşturur.

Siber Güvenlik Taahhüdümüz

Şirketimizin Siber Güvenlik hedefleri doğrultusunda, siber riski azaltmak, siber dayanıklılığı artırmak ve pazar erişimini güçlendirmek üzere bilgi varlıklarımızın, sistemlerimizin ve dijital hizmetlerimizin (bulut hizmetleri dahil) gizliliğini, bütünlüğünü, erişilebilirliğini ve kimlik doğruluğunu korumayı taahhüt ediyoruz. Uygulamaya aldığımız Siber Güvenlik Yönetim Sistemi ve güçlü siber güvenlik pratiklerimiz aracılığıyla; Siber Güvenlik Yönetişimi, Süreçler, Yetkilendirme ve Teknoloji alanlarına odaklanarak çalışanlarımızı, müşterilerimizi ve tüm paydaşlarımızı ortaya çıkan tehditlere karşı korumayı amaçlıyoruz.

Ayrıca, siber güvenlik duruşumuzu endüstri standartlarına ve yasal düzenlemelere tam uyum sağlamak amacıyla sürekli olarak izliyor ve bağımsız olarak değerlendiriyoruz; çalışanlarımızın siber tehditleri etkili bir biçimde yönetebilmesi için gerekli bilgi ve becerilerle donatılmasını sağlamak üzere sürekli eğitim ve farkındalık programlarına yatırım yapıyoruz. Nihai hedefimiz, güçlü bir siber güvenlik kültürü oluşturarak paydaşlarımız arasında güven ve itimat inşa etmek ve aynı zamanda dayanıklı, güvenli bir dijital ortamı sürdürmektir.

Vizyonumuz ve Misyonumuz

Vizyon

Siber güvenlik şirketimizin temeline yerleşmiştir:
teknoloji, süreçler ve personel aracılığıyla bizi güvenilir bir iş ortağı konumuna getirir.

Misyon

Rehberlik ederiz
Mevcut yasalara ve siber güvenlik dayanıklılığına uyumu güvence altına alan standartlar ve kılavuzlar belirleyerek.

yetkilendiririz
İş birimleri ve ülkelerle etkileşime geçerek, düzenlemeleri uygulamalarını sağlamak ve bunları iş ve müşteri ihtiyaçlarına göre uyarlamak suretiyle.

ve koruma sağlarız
İş birimleri ve ülkelerin siber güvenliği uygulamalarına ve dayanıklılıklarını güçlendirmelerine destek olmak amacıyla hizmetler, teknoloji ve uzmanlık sunarak

Siber Güvenlik Hedeflerimiz

Vizyon

Siber güvenlik şirketimizin temeline yerleşmiştir:teknoloji, süreçler ve insanlar aracılığıyla – bizi güvenilir bir iş ortağı konumuna getirir.

Hedefler

1

Siber Riski Azaltmak
... şirketi korumak ve müşterilerimizi desteklemek için

Suç örgütleri, yeni teknolojilerden yararlanarak yeni hedefler belirlemekte ve saldırıları endüstriyel ölçekte başlatmaktadır; bunun için kurumların savunmasındaki en zayıf noktaları istismar ederler. Teknoloji, süreçler ve insan unsurları genelinde siber risk yönetiminin önemi temeldir.

2

Pazar Erişimini Desteklemek
... sertifikalı teknik ve kurumsal önlemlerle

Müşterilerimizi ve organizasyonumuzu korumak en yüksek önceliğimizdir; zira güvenlik, müşterilerimizin güvenini kazanmanın, operasyonlarımızı güvence altına almanın, hasta güvenliğini sağlamanın ve markayı korumanın temel unsurudur.

3

Siber Sağlığı Büyütmek
... dayanıklılık kültürünü geliştirerek şirket genelinde

Müşterilerimizin ve şirketimizin yararına olacak şekilde siber güvenlik yetkinliklerimizi güçlendirmek için dijital teknolojilerden yararlanıyor ve bunları sürekli olarak geliştiriyoruz; güçlü süreçler ve yetkin bireylerle bu süreci destekliyoruz.

Rehber İlkelerimiz

Siber Güvenliğe Bağlılık

Endüstri standartlarına, yasal gerekliliklere, sözleşmesel yükümlülüklere ve sektördeki en iyi uygulamalara tam olarak uygun, etkili güvenlik önlemlerini titizlikle uyguluyor ve sürekliliğini sağlıyoruz. Bu bütünleşik yaklaşım, operasyonlarımızın dayanıklılığını ve tüm hassas bilgilerin en üst düzeyde korunmasını güvence altına almaktadır.

Tüm Çalışanların Sorumluluğu

Siber Güvenlik hepimizin sorumluluğudur. Görevlerinden bağımsız olarak tüm çalışanlar, siber güvenlikle ilgili politikalara uymak, olayları bildirmek ve eğitim programlarına katılmakla yükümlüdür.

Güvenlik Önlemleri

Hizmetlerimizin güvenliğini artırmak en öncelikli hedeflerimizden biridir. Hizmetlerin geliştirilmesi, devreye alınması, işletilmesi ve destek süreçlerimiz, müşterilerimizi korumak ve yürürlükteki düzenlemelere uygunluğu sağlamak amacıyla tasarım aşamasında güvenlik ilkelerini temel almaktadır.

Güvenli Portföy

Hizmetlerimizin güvenliğini artırmak en öncelikli hedeflerimizden biridir. Hizmetlerin geliştirilmesi, devreye alınması, işletilmesi ve destek süreçlerimiz, müşterilerimizi korumak ve yürürlükteki düzenlemelere uygunluğu sağlamak amacıyla tasarım aşamasında güvenlik ilkelerini temel almaktadır.

Üçüncü Taraf Güvenliği

Üçüncü taraf iş ortaklarımızın, tedarikçilerimizin ve yüklenicilerimizin Siemens Healthineers'ın siber güvenlik politikalarına uymalarını zorunlu kılıyoruz, böylece sistemlerinin ve süreçlerinin güvenlik gereksinimlerimizi karşılamasını sağlıyoruz. Veri ve sistemlerimizi koruma konusundaki sorumluluklarını belirleyen sözleşmeler imzalıyoruz.

Sürekli İyileştirme

Siber güvenlik uygulamalarımızın sürekli olarak iyileştirilmesinde kararlıyız; bu doğrultuda yeni ortaya çıkan tehditler ve zafiyetler hakkında bilgi sahibi olmayı sürdürüyor, güvenlik duruşumuzu güçlendirmek amacıyla yeni teknolojileri ve çözümleri araştırıyoruz.

Kurumsal Siber Güvenlik Organizasyonu

Siemens Healthineers, Kurumsal Siber Güvenlik Yönetişim Yapısı ile hareket etmektedir. Bu yapı, Kurumsal Siber Güvenlik Sorumlusu (CCSO) tarafından yönetilmekte olup, küresel siber güvenlik stratejisinin oluşturulmasından, hedeflerin belirlenmesinden ve güvenlik süreçlerinde sürekli iyileştirmenin güvence altına alınmasından sorumludur. CCSO, gereklilikleri belirleme, uyumu değerlendirme, Siber Güvenlik Yönetim Sistemi oluşturma ve sürdürme yetkisine sahiptir. Kurumsal Siber Güvenlik birimi ayrıca farkındalık ve eğitim programlarını denetler, siber güvenlik hizmetlerinin ve araçlarının geliştirilmesini destekler ve Siber Güvenlik Topluluğu'na rehberlik eder. CCSO, düzenli olarak Yönetim Kurulu'na ve Risk Komitesi'ne rapor sunar.

İş birimi yöneticileri ve diğer sorumlu kişiler, siber güvenlikle ilgili rolleri atamak, yeterli kaynakları sağlamak, siber güvenlik gerekliliklerinin uygulanmasını desteklemek ve bunların etkinliğini izlemekle yükümlüdür.

Siber Güvenlik Kurulu (CSB), küresel stratejinin uygulanmasında CCSO'ya destek sağlar. Kurul, çeşitli yönetişim alanlarından temsilciler içerir ve siber güvenlik gerekliliklerinin ilgili düzenleme ve süreçlere entegre edilmesini sağlayarak kurum genelinde iş birliğini teşvik eder.

Siber güvenlik, Siemens Healthineers'ın tüm iş operasyonlarını kapsayan, hayati bir koruyucu kalkan görevi üstlenmektedir. Bu çerçevede, bilgi güvenliğinin sürdürülebilirliğini sağlamak için her bir çalışanımızın aktif sorumluluk alması esastır.

Politika Denetimi

Siemens Healthineers, bilgi koruma konusunda yüksek standartları sürdürmeyi taahhüt eder. Bu amacı desteklemek için, şirketin stratejik hedefleriyle uyumlu, iş ihtiyaçlarını, yasal ve düzenleyici gereklilikleri, sözleşmesel yükümlülükleri ve gelişen güvenlik tehditlerini karşılayacak şekilde tasarlanmış kapsamlı siber güvenlik politikaları uygulanmaktadır.

Aşağıda belirtilen politikalar, uluslararası ISO/IEC 27001 standardı temel alınarak oluşturulmuş; sektörce tanınan uygulama ve güvenlik çerçeveleriyle uyumlu şekilde Siemens Healthineers'ın bilgi varlıklarının, sistemlerinin, çözümlerinin ve hizmetlerinin korunmasına yönelik açık gereklilikler ortaya koymaktadır. Bu politikalar, Siemens Healthineers'ın bilgi varlıklarını yöneten, bunlara erişen veya bunları kullanan tüm çalışanlar ve iş ortakları için geçerlidir. Ayrıca, şirketin dijital operasyonlarını destekleyen altyapı ve hizmetler dahil olmak üzere tüm varlıkları ve işleme ortamlarını da kapsamaktadır.

Aşağıdaki liste, Siemens Healthineers'ın siber güvenliği kurmak, uygulamak, sürdürmek ve sürekli olarak iyileştirmek amacıyla oluşturduğu politikaları ortaya koymaktadır. Bu politika ve uygulamalar, temel bir standart olarak hizmet eder ve söz konusu standartların Siemens Healthineers'in iş operasyonları genelinde uygulanmasını kolaylaştırmayı amaçlamaktadır. Siemens Healthineers bünyesindeki politikalar bu şekilde sınırlı olmamak üzere aşağıdaki gibidir:

- Siber Güvenlik Direktifi
- Siber Güvenlik Yönetim Sistemi
- Erişim Yönetimi
- Varlık Yönetimi
- Bilgi Sınıflandırma ve İşleme
- Saha Dışı Çalışma
- İş Sürekliliği Yönetimi
- Bulut Güvenliği
- Şifreleme
- İnsan Kaynakları Güvenliği
- Olay Yönetimi
- Ağ Güvenliği
- Fiziksel ve Çevresel Güvenlik
- Portföy Güvenliği
- Siber Güvenlik ve Risk Yönetimi
- Tedarikçi Güvenliği

Siemens Healthineers, bazı politikalar ile ilgili bilgileri kamuya açık şekilde paylaşırken, koruma düzeyi gereksinimlerine bağlı olarak diğer bazı bilgileri şirket içinde tutmakta ve bu bilgileri dış paydaşlarla paylaşmamaktadır.