REHAU

BİLGİ GÜVENLİĞİ POLİTİKASI

IT/IS prosesinin önemli bir bileşeni, katma değerli zincirin sürekliliğini sağlamak için REHAU iş proseslerinin korunmasıdır. Denetim Kurulu ve Grup Yönetim Kurulu bilgi güvenliğini aktif bir şekilde geliştirmektedir ve tutarlı bir bilgi güvenliği politikası uygulamak için gerekli olan kaynakları sağlamaktadır.

Güvenlik hedefleri

- REHAU inovasyon ve teknoloji odaklı bir ortamda geliştirilen know-how ve fikri mülkiyeti gizliliğin ihlal edilmesine karşı korumakta ve güvence altına almaktadır.
- REHAU, üçüncü taraflardan alınan gizli bilgileri, gizlilik ihlaline karşı güvence altına almaktadır zira, güvenlik olayları ciddi imaj zedelenmesine yol açabilir.
- Yüksek kalite standartları sağlamak ve yasal gerekliliklere uymak için, REHAU temel ve yönetim proseslerindeki tüm bilgi sistemlerinin en yüksek doğruluk/bütünlüğünü sağlamaktadır.
- REHAU, proseslerin tam zamanında veya tam sırasında gerçekleştirilmesi için temel proseslerde gerekli olan bilgi sistemlerini korumaktadır. Sözleşme kapsamında cezaların uygulanması ve imaj zedelenmesine karşı koruma sağlamak amacı ile, tedarik zinciri yönetiminde kesintilerin meydana gelmesi önlenmektedir.
- REHAU tanımlanan maksimum yeniden başlama süresi içerisinde kesintilerin ve acil durumların ortadan kaldırılması için ve dolayısıyla finansal zararın en aza indirilmesi için IT/IS alanında arızaların ve kısıtlamaların çözümlenmesi için zamanında tedbirler almaktadır.
- REHAU çalışanlarının sorumluluk duygusuna sahip olmalarını sağlamaktadır. Sorumlulukların dikkatsiz bir şekilde ihmal edilmesi Şirkete zarar verebilir. Bu nedenle eğitim ve farkındalık arttırma faaliyetleri gerçekleştirilmektedir.

Güvenlik Proses

Güvenlik hedeflerine ulaşabilmek için ISO /IEC 27001'e göre bir Bilgi Güvenliği Yönetim Sistemi (BGYS) uygulanacaktır ve hem küresel hem de yerel düzeyde sorumluluklar tanımlanacaktır. Planlama, uygulama, izleme ve iyileştirme için spesifikasyonlar ITS005-WW "Bilgi Güvenliği Yönetimi" prosedüründe açıklanmıştır.

Bu prosesin temel unsurları aşağıda açıklanacaktır:

Risk yönetimi

BGYS bir risk odaklı yaklaşım uygulamaktadır. Bu amaçla, şirket risk yönetimine ilişkin arayüzde bulunan bilgi güvenliği risklerinin tanımlanması ve değerlendirilmesi için bir metot tanımlanmıştır. Ayrıca, risklerin nasıl ele alınacağı da tanımlanmıştır.

Buna riskin kabul edilmesi ve risk azaltma önlemlerinin tanımlanması ve onaylanması da dahildir. Kritik iş prosesleri veya destekleyici bilgi sistemleri ve IT alt yapısı için, tanımlanan metoda göre risk analizleri gerçekleştirilecektir. Tanımlanan riskler, belirlenen raporlama kanalları aracılığı ile duyurulacaktır. Riskin azaltılmasına ilişkin önlemler, bir eylem planında açıklandığı şekilde sorumlu departmanlar tarafından onaylanacak ve belirlenen süre içerisinde uygulanacaktır. Uygulama derecesi düzenli aralıklarla takip edilecektir.

Yayın Tarihi 11.12.2017 REV.01

İzleme

Tanımlanan güvenlik spesifikasyonlarının uygulama ve etkinlik derecesi ve uygulanan güvenlik önlemleri izlenecektir. Bu bir taraftan sistemlerin izlenmesi ve kayıt altına alınması ile kontrol gerçekleştirilmesini ve diğer taraftan denetimlerin planlanmasını ve düzenli olarak gerçekleştirilmesini kapsamaktadır. BGYS'nin değerlendirilmesi için bir temel unsur sistemi geliştirilecek ve uygulanacaktır. Elde edilen temel unsurlar düzenli aralıklarla ilgili raporlar aracılığı ile yönetime bildirilecektir.

İyileştirme

İzleme esnasında tespit edilen zayıf yönler ve iyileştirme potansiyeli açısından, uygun önlemler tanımlanacaktır ve tedbirlerin uygulanması için onay verilmek zorundadır.

Güvenlik organizasyonu

Grup Bilgi Güvenlik Müdürü, IT/IS toplantısının kılavuzluğu kapsamında bilgi güvenlik yönetim sisteminin içeriğinden ve geliştirilmesinden sorumludur. Bilgi güvenlik yönetim çerçevesini sürekli olarak iyileştirmekle, bunu gerçekleştirmek için gerekli olan görevleri koordine etmekle ve IT/IS toplantısı için karar alma evraklarını hazırlamakla görevlidir. Grup Bilgi Güvenlik Müdürü, her bir bölgede /ülke kümesinde bir Bilgi Güvenlik Müdürü tarafından desteklenmektedir. Bölge/Ülke Kümesindeki, Bilgi Güvenlik Müdürü, kendi bölgesinde bilgi güvenlik yönetim sisteminin uygulanması, sürdürülmesi ve iyileştirilmesinden sorumludur. Bilgi güvenlik yönetimi, SES (SES005-WW "Bilgi güvenliğine" bakınız) ve LEGAL (hukuk bölümü) arasında yakın işbirliği gerçekleştirilmesi, güvenlik hedeflerine ulaşılması için esastır.

Grup bünyesindeki tüm IT/IS kullanıcıları bilgi güvenliği politikasını ve bu politikadan doğan evrakları, özellikle de ITS317-WW "Kullanıcı Sorumluluğu" prosedürünü uygulamayı taahhüt ederler. Uyulmaması halinde yerel mevzuata göre iş yasası önlemleri uygulanabilir.

Güvenlik Prensipleri

Aşağıdaki genel bilgi güvenliği prensipleri; alt talimatları için spesifikasyon olarak ve çalışanlar için oryantasyon olarak kullanılmaktadır.

Mevcudiyetten önce güvenlik

Bilgi güvenliği, risklere karşı önlem alınması ve zararla mücadele edilmesi; sistemlerin, uygulamaların ve verilerin mevcudiyeti için talep üzerinde önceliğe sahiptir. Benzer şekilde, çalışma rahatlığı bilgi güvenliğine bağlıdır.

4-Göz Prensibi

İş açısından kritik işlemler birbirlerinden bağımsız olan iki yetkili tarafından onaylanacaktır.

En Aza İndirme Prensibi

Prosesler, sistemler ve uygulamaların tasarlanması, özellikle de verilere ve bilgilere erişim gerektiği ölçüde asgariye indirilecektir. Eğer organizasyonel veya teknik nedenlerle herhangi bir başka hak verilirse, bu haklar istismar edilmemelidir.

**BGYS: Bilgi Güvenliği Yönetim Sistemi*

Yayın Tarihi 11.12.2017 REV.01