ISO 27001 – Bilgi Güvenliği Yönetim Sistemleri

ISO 27001, işletmelerin bilgi güvenliğiyle ilgili kuralları belirleyen bir kılavuzdur. Bu kılavuz, şirketlerin hassas bilgilerini nasıl koruyacaklarını öğretir. Örneğin, güvenlik politikaları oluşturmak, riskleri değerlendirmek, sadece yetkili kişilerin bilgilere erişmesini sağlamak gibi konuları içerir. Ayrıca, veri sızıntılarını önlemek, güvenlik ihlallerini izlemek ve güvenlik problemlerini çözmek için ne yapılması gerektiğini anlatır. ISO 27001 sayesinde şirketler, bilgi güvenliği tehlikelerini azaltarak müşteri ve çalışanların bilgilerini güvende tutabilir, güven veren bir çalışma ortamı yaratabilirler.

- Kurumsal Firmalarda ne tür faaliyetler yapılmaktadır?

Kurumsal faaliyetler, bir organizasyonun iş yapısını ve süreçlerini kapsayan faaliyetlerdir. ISO 27001 standartı, organizasyonların bu faaliyetleri, bilgi güvenliği açısından incelemesini gerektirir. Bu inceleme, organizasyonun ne tür bilgi varlıklarıyla çalıştığını, bu bilgilerin nasıl işlendiğini, nerede depolandığını ve nasıl iletildiğini anlamayı hedefler.

Örneğin, bir finans şirketi için kurumsal faaliyetler, müşteri bilgilerini işlemek, finansal verileri saklamak, para transferlerini yönetmek gibi işlemleri içerebilir. Bir sağlık kuruluşu için ise hasta kayıtlarını işlemek, tıbbi raporları saklamak, hastalar arasında bilgi paylaşımını yönetmek gibi faaliyetler öne çıkabilir.

Bu analiz, organizasyonun hangi bilgilerin kritik olduğunu belirlemesine yardımcı olur. Buna göre, bu kritik bilgilerin nasıl korunacağına dair stratejiler ve önlemler geliştirilir. Organizasyon, bu analiz sonucunda bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak için gereken adımları atabilir. Bu sayede, olası güvenlik ihlalleri ve bilgi kayıplarının önüne geçilebilir, güvenli bir iş ortamı sağlanabilir.

- Ne tür önlemler alınmaktadır?

Organizasyonlar, bilgi güvenliğini sağlamak ve riskleri en aza indirmek için çeşitli önlemler alırlar. Bu önlemler, iş süreçlerinin ve risk değerlendirmelerinin sonuçlarına dayalı olarak şekillenir.

Erişim Kontrolleri: Sadece yetkili kişilerin belirli bilgilere veya sistemlere erişebilmesini sağlamak için erişim kontrolleri kullanılır. Kullanıcı yetki matrisleri oluşturularak, her kullanıcının erişim düzeyi belirlenir.

Şifreleme: Hassas verilerin korunması için veri şifreleme teknikleri kullanılır. Bu, verilerin izinsiz erişime karşı korunmasını sağlar.

Güvenlik Yazılımları: Virüs koruması, güvenlik duvarları ve kötü amaçlı yazılım tespiti gibi yazılımlar kullanılarak sistemler korunur.

Güvenlik Politikaları ve Prosedürleri: Organizasyonlar, güvenlik politikaları ve prosedürleri oluşturarak çalışanların ve kullanıcıların güvenlik kurallarına uyum sağlamasını sağlar.

İzleme ve Denetim: Sistemler ve ağlar sürekli olarak izlenir ve denetlenir. Bu sayede anormal aktiviteler veya güvenlik ihlalleri tespit edilebilir.

Fiziksel Güvenlik: Fiziksel erişim kontrolleri, güvenlik kameraları ve biyometrik giriş sistemleri gibi önlemlerle tesislerin fiziksel güvenliği sağlanır.

Çalışan Eğitimi: Çalışanlar, güvenlik politikaları, phishing gibi saldırılardan kaçınma ve güvenli parola kullanımı gibi konularda eğitilir.

Yedekleme ve Kurtarma: Verilerin düzenli olarak yedeklenmesi ve kurtarılabilirlik planlarının oluşturulması veri kaybı durumlarına karşı önlem sağlar.

Bu önlemler, organizasyonun yapısına ve ihtiyaçlarına göre özelleştirilir. İhtiyaçlar ve tehditler değiştikçe, bu önlemler güncellenir ve geliştirilir. Bu sayede organizasyonlar, bilgi varlıklarını koruyarak iş sürekliliğini ve güvenliği sağlamış olurlar.

- Firma çalışanları ile yapılan iş sözleşmesine nasıl maddeler eklenmelidir?

İş sözleşmeleri, çalışanların bilgi güvenliği politikalarına uyumunu sağlamak amacıyla önemli bir araçtır. Bu sözleşmelere eklenen hükümler, çalışanların güvenlik bilincini artırmak ve kurumun bilgi güvenliğine katkıda bulunmak için hayati önem taşır. Bu kapsamda, güvenlik eğitimleri, bilgi güvenliği sorumlulukları ve gizlilik taahhütleri gibi maddeler iş sözleşmelerine eklenmelidir. Böylece çalışanlar, bilgi güvenliği önlemlerine uyarak veri korumasını sağlar, bilgi sızıntılarını en aza indirir ve organizasyonun bütünlüğüne katkı sağlar.

- Firmanın diğer tedarikçi firmaları ile yapılan sözleşmesine nasıl maddeler eklenmelidir?

Tedarikçi sözleşmeleri, organizasyonların bilgi güvenliğini geniş bir ekosistemde sağlama sorumluluğunu yansıtır. Bu sözleşmelerde, tedarikçinin sunmuş olduğu ürün veya hizmetin yeterli bilgi güvenliği standartlarını sağlaması için gerekli maddeler yer almalıdır. Bu, veri koruma, yetki kontrolleri ve düzenli denetim gereksinimleri gibi temel konuları içerebilir. Bu önlemler, organizasyonların tedarik zincirinin güvenliğini koruyarak bilgi sızıntılarına karşı koruma sağlamasını ve müşteri bilgilerinin güvenliğini garanti altına almasını amaçlar.

- Yetki Kontrolleri

**Erişim Yetki Kontrolü:** Erişim kontrolleri, bilgi güvenliğinin temel taşlarından biridir ve organizasyonların verilerini korumak için kritik bir önlem sağlar. Bu kontroller, kullanıcıların sistemlerde ve uygulamalarda sadece ihtiyaç duydukları bilgilere ve yetkilere erişebilmelerini sağlamayı amaçlar. Bunun için yetki matrisleri, roller ve sorumlulukların belirlenmesi gibi yöntemler kullanılır.

Yetki matrisleri, farklı kullanıcıların hangi verilere veya işlevlere erişebileceğini tanımlar. Bu matrisler, iş pozisyonlarına veya rollerine göre ayrıcalıkları düzenlemek için kullanılır. Örneğin, bir müdürün finans verilerine erişimi olabilirken, temizlik personelinin böyle bir erişimi olmayabilir.

Roller, benzer yetkilere sahip kullanıcı gruplarını ifade eder. Bu, bir işlev veya departmandaki kişilere aynı tür erişimi sağlamak için kullanılır. Örneğin, bir IT ekibi tüm sistemlere erişebilirken, pazarlama ekibi sadece pazarlama araçlarına erişebilir.

Sorumluluklar, belirli verilere veya işlevlere erişimdeki görevleri ve kısıtlamaları ifade eder. Bu, veri girişi veya değişikliklerinde belirli bir denetime tabi olan kullanıcıları içerebilir.

**Local Admin Yetki Kontrolü:** Local admin yetki kontrolü, organizasyon içindeki bilgisayar veya ağ sistemlerinin yöneticileri tarafından kullanılan yüksek düzeydeki yetkileri kontrol etmeyi ifade eder. Bu, kötü amaçlı yazılım ve izinsiz değişikliklere karşı savunma sağlar.

**İnternet Erişim Yetki Kontrolü:** İnternet erişim yetki kontrolü, çalışanların interneti ne kadar ve hangi kaynaklara erişebileceklerini yönetmeyi amaçlar. Bu, güvenliği artırmak, veri kaybını önlemek ve iş verimliliğini yönetmek için kullanılır.

**İşe Giriş Çıkış Yapan Personel Kayıtları:** İşe giriş ve çıkış kayıtları, çalışanların iş süreçlerine erişimini kaydeder. Bu bilgiler, hassas verilere erişim yetkilerinin denetlenmesine yardımcı olur ve veri güvenliğini sağlar. Kayıtlar, güvenlik ihlallerini veya şüpheli faaliyetleri izlemek ve tespit etmek için kullanılabilir. Örneğin, bir çalışanın işten ayrılmasından sonra bilgilere erişmeye devam ettiği tespit edilirse, bu bir güvenlik ihlali olarak kabul edilebilir.

**Bölüm Değişikliği Yapan Personel İş Uygulama ve Portallarına Erişimi ve Yetkilendirme Kontrolü:** Bölüm değişikliği yapan personelin, iş uygulamalarına ve portal erişimine olan haklarının kontrolünü ifade eder. Bu, personelin yeni rol ve sorumluluklarına göre bilgi ve kaynaklara erişimini güncellemek ve gereksiz erişimi engellemek için kullanılır.

Bu kontroller, organizasyonların bilgi güvenliğini sağlamak ve veri güvenliği risklerini azaltmak için kullanılır. Her biri, organizasyonun güvenlik politika ve prosedürlerine uygun olarak yönetilir ve düzenli olarak gözden geçirilir.

-Uygulama ve Cihaz Güvenliği

Uygulama ve cihaz güvenliği, organizasyonların yazılım ve donanımları güvenli bir şekilde kullanmasını sağlar. Bu, potansiyel güvenlik açıklarının belirlenip düzeltilmesini, düzenli güvenlik güncellemeleri yapmayı ve cihazların güvenli bir şekilde yapılandırılmasını içerir.

Yazılımlar ve donanımlar, güvenlik açısından sürekli tehdit altında olduğundan, bu önlemler organizasyonların verilerini ve iş süreçlerini korumak için hayati önem taşır. Bu sayede siber saldırılara, veri kaybına ve iş kesintilerine karşı dirençli bir altyapı oluşturulur. Güncel ve güvenli uygulama ve cihaz kullanımı, organizasyonun güvenlik seviyesini artırırken güvenilir bir iş ortamı sağlar.

-Farkındalık Çalışmaları

Farkındalık çalışmaları, çalışanların güvenlik konularında bilinçlenmesini hedefler. Bu tür çalışmalar, eğitimler ve testler yoluyla gerçekleştirilir. Çalışanlara güvenlik tehditleri, phishing gibi saldırı türleri ve güçlü şifre kullanımı gibi konular öğretilir. Aynı zamanda farkındalık testleriyle çalışanların reaksiyonları ve güvenlik kurallarına uyumları değerlendirilir. Bu çalışmalar, çalışanların günlük iş akışlarında güvenlik önlemlerine dikkat etmelerini sağlar ve organizasyonun genel güvenlik seviyesini artırır.

-Risk Envanteri

Risk envanteri, organizasyonların olası güvenlik risklerini ve tehditleri belirlemelerini sağlar. Bu adım, risk analizi ve değerlendirmesiyle gerçekleşir. Olası güvenlik tehditleri tanımlanır, bu tehditlerin etkisi ve olasılığı değerlendirilir. Buna göre, risk düzeyleri belirlenir ve bu risklere karşı alınması gereken uygun önlemler tasarlanır. Bu süreç, organizasyonun güvenlik stratejisinin oluşturulmasında temel bir adımdır.

-Kullanıcı Yetki Matrisleri

Kullanıcı yetki matrisleri,önceki maddelerde de belirttiğim gibi organizasyonlarda her kullanıcının ne tür verilere ve işlevlere erişebileceğini belirler. Kullanıcılar sadece iş gereksinimlerine uygun olan bilgilere erişebilir. Bu önlem, bilgi güvenliği risklerini azaltmak ve içerideki tehditleri minimize etmek için kritik bir adımdır. Kullanıcıların yetkileri belirli roller ve iş pozisyonlarına göre atanır, böylece verilere sadece gereksinim duyanlar erişebilir ve olası güvenlik açıkları en aza indirilir.

- DLP (Data Loss Prevention)

Veri Kaybını Önleme (DLP), organizasyonların hassas verilerinin güvenliğini sağlamak için kullanılan teknolojileri ifade eder. Bu sistemler, verilerin izinsiz sızmasını engellemek amacıyla geliştirilir. DLP teknolojileri, verileri izler, analiz eder ve gerektiğinde engeller, böylece hassas bilgilerin yetkisiz erişim veya paylaşımlara karşı korunması sağlanır. Ayrıca, izinsiz veri paylaşımlarını tespit eder ve bu tür olaylar üzerine uyarılar veya engellemeler tetikler. DLP çözümleri, organizasyonların veri güvenliğini artırarak müşteri gizliliğini korumalarına yardımcı olurken, regülasyonlara uyum ve itibar koruma konularında da destek sağlar.

-Log Yönetimi

LOG yönetimi, organizasyonların sistem ve uygulamaların günlük kayıtlarını (log kayıtları) etkili bir şekilde yönetmeyi amaçlar. Bu kayıtlar, güvenlik olaylarını izlemek, tespit etmek ve anlamak için hayati öneme sahiptir. Günlük kayıtlar, olası saldırıları, sistem hatalarını veya diğer güvenlik sorunlarını tespit etmek için analiz edilir. Bu sayede, anormal aktiviteler veya potansiyel tehditler erken aşamada fark edilebilir. LOG yönetimi, organizasyonların güvenlik olaylarını belirlemelerini, buna hızla yanıt vermelerini ve gelecekteki güvenlik stratejilerini şekillendirmelerini sağlar. Ayrıca, yasal gerekliliklere ve düzenlemelere uyumu da destekler.

-Parola Yönetimi

Parola yönetimi, organizasyonların güvenliği artırmak için önemli bir adımdır. Güçlü parola politikaları ve düzenli parola değişiklikleri, yetkisiz erişimi önlemek amacıyla kullanılır. Bu politikalar, karmaşık ve tahmin edilmesi zor parolaların(büyük-küçük harf,sayı,özel karakter) kullanılmasını gerektirir. Parolaların düzenli olarak değiştirilmesi, olası güvenlik tehditlerine karşı bir savunma mekanizması oluşturur. Ayrıca, çok faktörlü kimlik doğrulama gibi güvenlik önlemleri de parola yönetimi stratejilerinin bir parçası olabilir. Böylelikle organizasyonlar, hassas verilere daha güvenli bir şekilde erişim sağlayarak veri güvenliğini artırabilir.

- BG Politika ve Prosedürlerinin Oluşturulması

Bilgi güvenliği politika ve prosedürleri, organizasyonun güvenlik vizyonunu ve uygulama yönergelerini belirler. Bu belgeler, tüm personelin bilgi güvenliği konusunda uyumlu davranmalarını sağlamak için önemlidir. Politika, genel yaklaşımı ve taahhütleri belirtirken, prosedürler daha spesifik adımları ve eylemleri içerir. Bu belgeler, güvenlik standartlarını, veri koruma yöntemlerini, erişim kontrollerini ve kriz durumlarında nasıl hareket edileceğini yönlendirir. Bilgi güvenliği politika ve prosedürleri oluşturmak, güvenlik kültürünü oluşturmanın yanı sıra, regülasyonlara ve en iyi uygulamalara uyumu sağlama açısından da kritiktir.