ŞİRVANLI
1980
Alüminyum Döküm ve Metal İşleme San. A.Ş.

BİLGİ YÖNETİMİ VE GÜVENLİĞİ POLİTİKASI

1. **Genel Esaslar**
   - Bilgi güvenliği yönetim sistemi, kurumun bilgi varlıklarını korumak, yetkisiz erişimleri önlemek ve bilgi sürekliliğini sağlamak amacıyla oluşturulur.
   - Bilgi güvenliği, gizlilik, bütünlük ve erişilebilirlik prensipleri doğrultusunda yönetilir ve sürekli olarak iyileştirilir.
   - Bilgi varlıklarının korunması için risk değerlendirmeleri gerçekleştirilir ve gerekli kontroller uygulanır.
   - Çalışanların bilgi güvenliği farkındalığını artırmak için düzenli eğitimler düzenlenir.
   - Politika güncellemeleri tüm çalışanlara bildirilir ve gerekli uyum süreci takip edilir.
2. **Bilgi Sistemleri Kullanımı**
   - Bilgi sistemleri yalnızca yetkilendirilmiş kişiler tarafından kullanılır ve erişim hakları belirlenen prosedürler çerçevesinde yönetilir.
   - Kullanıcı hesapları, güçlü kimlik doğrulama yöntemleriyle korunur ve düzenli aralıklarla gözden geçirilir.
   - Bilgi sistemlerinde kullanılan yazılımlar lisanslı olup, izinsiz yazılım kurulumu ve kullanımı engellenir.
   - Kullanıcılar, kendilerine tahsis edilen hesaplardan sorumludur ve kimlik bilgilerini üçüncü kişilerle paylaşamaz.
3. **Yönetimi ve Erişim Kontrolleri**
   - Kurum ağına erişimler yetkilendirilmiş kullanıcılarla sınırlandırılır.
   - Ağ altyapısı düzenli olarak izlenir ve güvenlik açıklarına karşı gerekli önlemler alınır.
   - Uzaktan erişimler, güvenli bağlantı yöntemleri (VPN, çok faktörlü kimlik doğrulama vb.) kullanılarak gerçekleştirilir.
   - Kablosuz ağ erişimleri, güvenlik politikalarına uygun olarak kontrol edilir ve yetkisiz erişimler engellenir.
4. **E-Posta ve Haberleşme Güvenliği**
   - Kurum e-posta sistemi kurumsal yazışmalar için kullanılır, kişisel amaçlarla kullanımı sınırlandırılır.
   - Zararlı e-postaların yayılmasını engellemek amacıyla güvenlik politikaları uygulanır.
   - Kullanıcılar, şüpheli e-posta içeriklerine karşı dikkatli olur ve kimlik avı girişimlerine karşı uyarılır.
   - E-posta içeriklerinde gizlilik derecesine sahip bilgiler yalnızca yetkilendirilmiş kişilere iletilir.
5. **Fiziksel Güvenlik**
   - Bilgi varlıklarının bulunduğu fiziksel alanlara yetkisiz erişimler engellenir.
   - Sistem odalarına yalnızca yetkili personel giriş yapar ve erişimler kayıt altına alınır.
   - Çalışma alanlarında gizli belgeler açıkta bırakılmaz, yazıcıdan alınan dokümanlar bekletilmeden alınır.
   - Çalışanlar, masa başından ayrıldığında bilgisayarlarını kilitleyerek yetkisiz erişimi önler.

6. **Veri Koruma ve Yedekleme**
   - Kritik veriler belirlenen aralıklarla yedeklenir ve güvenli alanlarda saklanır.
   - Veri yedekleme politikaları düzenli olarak gözden geçirilir ve güncellenir.
   - Yetkisiz kişilerin veri erişimini engellemek için şifreleme yöntemleri kullanılır.
   - Veri kayıplarını önlemek için gerekli tedbirler alınır ve sistemler sürekli izlenir.
7. **Siber Saldırılara Karşı Koruma**
   - Güvenlik duvarları (Firewall) ve saldırı tespit/önleme sistemleri (IPS/IDS) kullanılarak ağ güvenliği sağlanır.
   - Kurum sistemlerine yönelik siber tehditler düzenli olarak izlenir ve anormal aktiviteler tespit edildiğinde gerekli müdahaleler yapılır.
   - Kimlik avı (Phishing), kötü amaçlı yazılım (Malware), fidye yazılımı (Ransomware) ve diğer siber saldırı türlerine karşı proaktif önlemler alınır.
   - Çalışanlara düzenli olarak siber güvenlik farkındalık eğitimleri verilir ve olası saldırılara karşı bilinçlendirme yapılır.
   - Kritik sistemlerde çok faktörlü kimlik doğrulama (MFA) kullanılır ve kullanıcı erişimleri sıkı güvenlik denetimlerine tabi tutulur.
   - Yazılım ve sistem güncellemeleri düzenli olarak uygulanır ve güvenlik açıkları giderilir.
   - Siber saldırılar karşısında hızlı müdahale sağlamak amacıyla olay müdahale ekipleri oluşturulur ve kriz senaryoları geliştirilir.
   - Kurum bilgi sistemlerine yönelik düzenli sızma testleri (penetrasyon testleri) yapılır ve güvenlik açıkları tespit edilerek gerekli önlemler alınır.
8. **Güvenlik İzleme ve Denetim**
   - Bilgi sistemleri düzenli olarak denetlenir ve güvenlik açıkları tespit edilerek gerekli iyileştirmeler yapılır.
   - Kullanıcı faaliyetleri loglanarak izlenir ve olası ihlallere karşı önlemler alınır.
   - Penetrasyon testleri belirli periyotlarla gerçekleştirilir ve sistem güvenliği kontrol edilir.
   - Bilgi güvenliği ihlalleri tespit edildiğinde belirlenen prosedürler doğrultusunda aksiyon alınır.
9. **Kriz ve Acil Durum Yönetimi**
   - Bilgi güvenliği olayları için acil müdahale planları oluşturulur ve uygulanır.
   - Güvenlik ihlalleri durumunda ilgili birimler bilgilendirilerek gerekli aksiyonlar alınır.
   - Acil durum senaryoları düzenli olarak test edilir ve süreçler güncellenir.
10. **Uygunsuz Kullanım ve Yaptırımlar**
    - Kurum bilgi sistemleri ve kaynakları, yetkisiz amaçlarla kullanılamaz.
    - Kurum politikalarına aykırı hareket eden kullanıcılar hakkında disiplin süreçleri uygulanır.
    - Yetkisiz erişim, veri sızıntısı, zararlı yazılım kullanımı gibi ihlaller tespit edildiğinde gerekli hukuki ve idari işlemler gerçekleştirilir.

Bu politika, kurum bilgi güvenliği yönetim sisteminin bir parçası olarak uygulanır ve tüm çalışanlar tarafından eksiksiz şekilde yerine getirilir.

UĞUR KAŞIKIRIK

12.02.2025

Rev.1