OSASEC

Bilgi Güvenliği

Ve

Veri Koruma Politikası

2024

v.1.0

Bilgi Güvenliği ve Veri Koruma Politikası

1. Giriş

Bilgi güvenliği ve veri koruma, OSISEC'in güvenilir BT çözümleri sunma misyonunun merkezindedir. Bu politika, sistemlerin ve verilerin korunması için gerekli yönetişim çerçevesini sunar.

2. Amaç

- Bilgi varlıklarını yetkisiz erişim ve zarardan korumak
- İç ve dış tehditlere karşı riskleri azaltmak
- GDPR, KVKK, ISO 27001 gibi standartlara uyum sağlamak
- Güvenlik bilincini kurumsal kültür haline getirmek

3. Kapsam

- OSISEC çalışanları, yükleniciler ve iş ortakları
- OSISEC tarafından yönetilen tüm BT varlıkları
- Tüm veri türleri: kişisel, hassas, özel ve müşteri verisi

4. Yönetişim

4.1 Liderlik

- Bilgi Güvenliği Sorumlusu (CISO), uygulama ve denetimden sorumludur
- Alan uzmanları, tehditler doğrultusunda stratejileri günceller

4.2 Sorumluluk

- Tüm çalışanlar bu politikaya uymak ve olayları raporlamakla yükümlüdür
- Yöneticiler, güvenlik uygulamalarının takibini sağlar

5. Güvenlik İlkeleri

- **Gizlilik**: Bilgi sadece yetkililerle paylaşılır
- **Bütünlük**: Bilginin doğruluğu ve güvenilirliği korunur
- **Erişilebilirlik**: Sistemlere kesintisiz erişim sağlanır

6. Temel Kontroller

6.1 Erişim Yönetimi

- Rol tabanlı erişim kontrolü
- Çok faktörlü kimlik doğrulama
- Zaman kısıtlı erişim izinleri

6.2 Veri Koruma

- AES-256 şifreleme
- Test ortamlarında veri maskelenmesi
- Veri sınıflandırma ve etiketleme

6.3 Ağ Güvenliği

- Yeni nesil güvenlik duvarları
- Sıfır güven mimarisi
- Düzenli sızma testleri

6.4 Uç Nokta Güvenliği

- Uç nokta tehdit tespiti (EDR)
- Güvenlik yapılandırma standartları
- Otomatik çalıştırma devre dışı bırakılır

6.5 Uygulama Güvenliği

- Güvenli yazılım geliştirme süreçleri
- DevSecOps entegrasyonu
- Web uygulama güvenlik duvarları

6.6 Tehdit İzleme

- Tehdit istihbarat platformları
- Olay izleme ve anomali tespiti (SIEM)
- Sürekli risk değerlendirmeleri

7. Olay Yanıtı ve İş Sürekliliği

- Olay müdahale planı
- Siber olaylara özel rehberler
- Yılda iki kez felaket kurtarma testleri

8. Farkındalık ve Eğitim

- Zorunlu siber güvenlik eğitimleri
- Özel rollere yönelik ileri eğitimler
- Kimlik avı simülasyonları

9. Üçüncü Taraf ve Tedarik Zinciri

- Tedarikçilerle güvenlik sözleşmesi
- Periyodik risk değerlendirmeleri
- Tedarik zinciri güvenliği

10. Uyumluluk

- ISO/IEC 27001
- NIST Çerçevesi
- GDPR ve KVKK
- Sektörel düzenlemeler

11. Sürekli İyileştirme

- Politikalar 6 ayda bir gözden geçirilir
- Olay sonrası analizler ile güncellemeler yapılır
- Yeni güvenlik teknolojilerine yatırım yapılır

12. Uygulama

- Politika ihlalleri disiplin cezalarına yol açabilir
- Ciddi ihlaller yasal mercilere iletilir

13. Gözden Geçirme

- Yılda bir veya değişiklik sonrası
- Yeni araç/sistem entegrasyonu
- Olaylardan edinilen dersler

14. Raporlama

- **Olay Raporlama**: 24 saat içinde incident@osisec.com.tr
- **İhbar Koruması**: İyi niyetli bildirimler korunur

Onaylayan

CEO: Bulent KONUK
Onay Tarihi: 28 Kasım 2024