İş Ahlakı

ve

Etik Davranış Kuralları

2024

v.1.0

İş Ahlakı ve Etik Davranış Kuralları

Giriş

OSISEC İş Ahlakı ve Etik Davranış Kuralları (bundan böyle "Kod" olarak anılacaktır), OSISEC Bilişim Yazılım Ticaret Limited Şirketi ile (bundan böyle "Şirket" olarak anılacaktır) siber güvenlik araçlarının ve hizmetlerinin sağlanması, geliştirilmesi, uygulanması veya entegrasyonuna katılan tüm ortaklar, yükleniciler, taşeronlar ve iş birlikçileri (topluca "Ortaklar" olarak anılacaktır) tarafından uyulması gereken ilke, standart ve uygulamaları belirler. Bu Koda uyum zorunludur ve tüm mesleki faaliyetlerde en yüksek düzeyde etik, hukuki ve teknik bütünlük sağlanmasına yönelik bir taahhüdü yansıtır.

Temel İlkeler

Ortaklar, aşağıdakilerle sınırlı olmamak kaydıyla tüm yerel, ulusal ve uluslararası yasa ve düzenlemelere uymalıdır:

• Avrupa Birliği (AB): o Avrupa Birliği toprakları için Genel Veri Koruma Tüzüğü (GDPR).

• Amerika Birleşik Devletleri: o Kaliforniya Tüketici Gizlilik Yasası (CCPA) - Kaliforniyalı sakinleri kapsayan hizmetler için. o NIST Siber Güvenlik Çerçevesi - federal veya ABD merkezli operasyonlar için.

• Uluslararası: o Bilgi güvenliği yönetim sistemleri için ISO/IEC 27001 Standartları.

• Türkiye: o KVKK (Kişisel Verilerin Korunması Kanunu, Kanun No. 6698): Kişisel verilerin işlenmesini ve korunmasını düzenler, GDPR ilkeleriyle uyumludur. o Türk Ceza Kanunu (Maddeler 243–246): Yetkisiz erişim ve veri değiştirme dahil siber suçları kapsar. o Ulusal Siber Güvenlik Stratejisi ve Eylem Planı: Kritik altyapı ve siber güvenlik operasyonlarında uyumu yönlendirir. o Bilgi Teknolojileri ve İletişim Kurumu (BTK) düzenlemeleri: BİT ve siber güvenlikle ilgili operasyonları denetler. o e-Dönüşüm Türkiye Projesi: e-Devlet ve dijital iş operasyonları için yasal ve teknik standartları belirler.

2. Veri Güvenliğine Bağlılık

Ortaklar, hassas verileri korumak için güçlü siber güvenlik önlemleri uygulamalı ve sürdürmelidir. Buna şunlar dahildir ancak bunlarla sınırlı değildir:

• Şifreleme Standartları: Tüm veri aktarımı ve depolaması, endüstri standardı protokoller (örn. AES-256, TLS 1.3) kullanılarak şifrelenmelidir.

• Erişim Kontrolü: Verilere ve sistemlere erişim yalnızca gerekli yetkilendirilmiş personelle sınırlandırılmalıdır.

• Olay Müdahalesi: İhlalleri tespit etmek, raporlamak ve hafifletmek için, keşiften itibaren en fazla 24 saat içinde müdahaleyi içeren açık bir olay müdahale planı oluşturulmalı ve sürdürülmelidir.

Bu standartlara uyulmaması, bu Kodun ihlali anlamına gelir ve ortaklık sözleşmesinin derhal gözden geçirilmesiyle sonuçlanır.

3. Siber Güvenlik Araçlarının Etik Kullanımı

Ortaklar, Şirket tarafından sağlanan siber güvenlik araçlarını aşağıdaki amaçlarla kullanamaz:

• Yasadışı gözetim veya izleme yapmak.

• Bireylerin gizlilik haklarını ihlal etmek.

• Güvenlik açıklarından yetkisiz kazanç veya faaliyetler için yararlanmak.

Tüm araçlar yalnızca Şirket ile yapılan anlaşmada belirtilen amaçlar doğrultusunda kullanılmalı, şeffaflık ve etik kullanım sağlanmalıdır.

Teknik ve Operasyonel Standartlar

4. Sistem Bütünlüğü ve Testler

Ortaklar, tüm sistemlerin bütünlüğünü sağlamakla yükümlüdür:

• Düzenli Zafiyet Değerlendirmeleri: Sistemlerdeki ve araçlardaki zayıflıkları belirlemek ve gidermek için yılda iki kez değerlendirme yapılmalıdır.

• Sızma Testleri: Gerçek dünya dayanıklılığını sağlamak için her yıl sertifikalı profesyonellerle sızma testleri yapılmalıdır.

• Yazılım Güncellemeleri: Araçlara ve sistemlere üretici tavsiyeleri ve siber güvenlik en iyi uygulamaları doğrultusunda güncellemeler ve yamalar zamanında uygulanmalıdır.

5. Gizlilik ve Veri Koruma

Hassas verileri korumak için aşağıdaki önlemlere uyulmalıdır:

• Gizlilik Sözleşmeleri (NDA): Hassas veri işleyen tüm personel gizlilik sözleşmesi imzalamalı ve uymalıdır.

• Veri Minimizasyonu: Yalnızca sözleşme gerekliliklerini yerine getirmek için gereken asgari veri toplanmalı ve saklanmalıdır.

• Güvenli Veri İmhası: Fiziksel ortamlar için manyetik silme (degaussing) veya parçalama, elektronik veriler için onaylı silme protokolleri gibi güvenli imha yöntemleri uygulanmalıdır.

6. Tedarik Zinciri Güvenliği

Ortaklar, kendi tedarikçi ve taşeronlarının güvenlik uygulamalarını değerlendirmeli ve izlemelidir. Buna şunlar dahildir:

• Taşeronların bu Kodda belirtilen yasal ve etik standartlara uymalarının sağlanması.

• Güvenilmeyen veya yaptırım uygulanan kaynaklardan bileşen veya yazılım temininden kaçınılması.

• İşbirliğinden önce tedarik zinciri unsurları üzerinde gerekli özenin gösterilmesi.

Profesyonel Davranış

7. Yolsuzlukla Mücadele ve Adil Rekabet

Ortaklar, adil rekabet ilkelerine bağlı kalmalı ve aşağıdaki faaliyetlere katılmamalı veya tolerans göstermemelidir:

• Rüşvet veya Komisyonlar: Kararları etkilemek amacıyla herhangi bir değerli şeyin teklif edilmesi, alınması veya talep edilmesi.

• Çıkar Çatışması: Çıkar çatışmasına neden olabilecek herhangi bir ilişki veya faaliyetin açıklanması.

• Rekabet Karşıtı Uygulamalar: Piyasa koşullarının manipülasyonu veya rakiplerle işbirliği.

8. İnsan Haklarına Saygı

Ortaklar, aşağıdakilerle sınırlı olmamak üzere uluslararası tanınan insan haklarına saygı göstermelidir:

• Ayrımcılıktan Kaçınma: İstihdam uygulamalarında fırsat eşitliği ve adalet sağlanmalıdır.

• Çalışma Standartları: Çocuk işçiliği yasağı, zorla çalıştırma yasağı ve adil çalışma koşullarına uyum.

9. Şeffaflık ve Raporlama

Şirket ile tüm etkileşimler şeffaf olmalıdır. Ortaklar:

• Doğru Belgeler Sunmalıdır: Tüm raporlar, sertifikalar ve faturalar dürüst ve doğru olmalıdır.

• Usulsüzlükleri Proaktif Olarak Raporlamalıdır: Bu Kodun veya ilgili yasaların bilinen veya şüphelenilen ihlalleri, misilleme korkusu olmadan Şirkete bildirilmelidir.

Eğitim ve Sürekli İyileştirme

10. Zorunlu Eğitim

Ortaklar, ilgili tüm personelin aşağıdaki yıllık eğitim programlarını tamamlamasını sağlamalıdır:

• Siber Güvenlik Farkındalığı: Çalışanlara oltalama, sosyal mühendislik ve kötü amaçlı yazılım tehditleri hakkında eğitim verilmesi.

• Veri Gizliliği: İlgili veri koruma yasaları, güvenli veri işleme uygulamaları ve veri sahibi hakları hakkında eğitim.

• Etik Standartlar: Bütünlük ve etik karar alma konularının pekiştirilmesi.

11. Sürekli İyileştirme Girişimleri

Ortaklar, aşağıdaki yollarla sürekli iyileştirme sürecine katılmaya teşvik edilir:

• Siber güvenlik dayanıklılığını artırmak için yeni teknolojilerin benimsenmesi.

• Şirket ile bilgi, yenilik ve en iyi uygulamaların paylaşımı.

• İyileştirme fırsatlarını belirlemek için denetimlere ve incelemelere katılım.

Uygulama ve Hesap Verebilirlik

12. İzleme ve Denetimler

Şirket, aşağıdaki haklarını saklı tutar:

• Ortakların bu Koda uyumunu periyodik olarak denetlemek.

• Siber güvenlik standartları için üçüncü taraf denetim raporlarının sunulmasını talep etmek.

• Etik ve teknik gerekliliklere uyumu doğrulamak için rastgele denetimler yapmak.

13. Uyumsuzluk ve Düzeltici Önlemler

Uyumsuzluk durumlarında aşağıdaki işlemler uygulanabilir:

• Derhal Askıya Alma: Sorun çözülene kadar ortaklığın geçici olarak askıya alınması.

• Sözleşmenin Feshi: Ağır veya tekrarlanan ihlallerde kalıcı fesih.

• Hukuki İşlem: Uyumsuzluk nedeniyle oluşan zararlara yönelik yasal yolların uygulanması.

Kabul ve Onay

Tüm çalışanlar, yükleniciler ve iş ortakları bu Kodu okuyup anladıklarını ve bu Kodda belirtilen şartlara uyacaklarını Ek-A – Alındı ve Kabul Beyanı'nı imzalayarak beyan etmelidir. Bu onayın imzalanıp iade edilmemesi, hizmetlere katılımı veya devamını engelleyecektir.

Sonuç

Bu Kod, siber güvenlik araçlarının ve hizmetlerinin sunumunda etik, güvenli ve yasal uygulamalara yönelik karşılıklı taahhüdü vurgular. Bu ilkelere uymak suretiyle Ortaklar, tüm paydaşların çıkarlarını koruyan güvenilir ve güçlü bir siber güvenlik ekosistemine katkıda bulunur.

Onaylayan

CEO: Bulent KONUK
Onay tarihi: 28 Kasım 2024

EK-A : Alındı ve Kabul Beyanı

İşbu belgeyi imzalayarak, OSISEC İş Ahlakı ve Etik Davranış Kuralları belgesini okuduğumu, anladığımı ve belirtilen şartlara uyacağımı beyan ederim.

İş Ortağı Adı:_____
Yetkili Temsilci:_____

İmza:_____
Tarih:_____