BİLGİ GÜVENLİĞİ FARKINDALIK BİLDİRGESİ

1. Tanımlar:

Gizli bilgi yazılı veya sözlü, elektronik ortamda ifade edilmiş veya başka bir şekilde ifşa edilmiş bir bilgi olabilir ve maddi veya maddi olmayan bir bilgi olabilir. ŞİRKET'in ÜRETİCİ Personeline ifşa ettiği tüm materyallerin ve bilgilerin, Gizli Bilgi olduğu farz edilecek ve ÜRETİCİ Personeli bu materyal ve bilgilerin aşağıdaki tanımlara göre Gizli Bilgi olmadığını ispat edemediği sürece Gizli Bilgi olarak kabul edilecektir:

Gizli Olmayan Bilgi:

a) Kullanımı veya açıklanması konusunda hiçbir kısıtlama yapılmadan üçüncü kişilere açık olan, ŞİRKET tarafından zaten kamuya açıklanmış olan bilgiler.

b) Gizlilik ve Bilgi Güvenliği Taahhütnamesi herhangi bir şekilde ihlal edilmeksizin, Tarafların bağımsız bir şekilde tasarladıkları, üretip geliştirdikleri bilgiler.

c) Yürürlükte olan kanun, ilgili mevzuat, sair yasal düzenlemeler, mahkeme kararı ve/veya idari emir gereğince açıklanması gereken bilgiler.

Gizli bilgi örnekleri; müşteri bilgileri, çalışan bilgileri, maliyet bilgileri, kar bilgileri, satış bilgileri, hizmet bilgileri, ürün bilgileri, ürün geliştirme bilgileri, ödeme bilgileri, hesap bilgileri, banka bilgileri, finansal modeller, simülasyonlar, çalışma ve hizmet bilgileri, fiyatlandırma bilgileri, maaş politika ve düzeyleri, işletim yöntemleri, fikirler, buluşlar, know-howlar, markalar, logolar, patentler, yazılımlar, kaynak kodları, fikri ve sınai mülkiyet hakları, tasarım hakları, ticari sırlar, teknik prosesler, formüller, planlar, tasarılar, lisans ve izinler, çizimler, tertipler, modeller, projeksiyonlar, iş planları, pazar fırsatları, ŞİRKET ve/veya grup şirketleri ya da onun namına üçüncü bir tarafça hazırlanmış raporlar veya veriler dâhil ve fakat sayılanlarla sınırlı olmamak üzere her türlü bilgi ve/veya belge örnek olarak verilebilir.

2. Yükümlülükler:

ÜRETİCİ ve ÜRETİCİ personeli;

a) ÜRETİCİ'ye herhangi bir veri paylaşımı söz konusu ise;

- Her türlü bilgiyi sadece Sözleşme ve/veya Ek Protokol'ün ifası için kullanacağını, makul seviyede titizlik göstererek tüm gizli bilgilerin gizliliğini devam ettireceğini ve koruyacağını,
- ŞİRKET'in bilgilerinin bulunduğu bilgisayar, telefon, tablet, veri depolayan tüm cihazlar ve yazılımların veri güvenliğinden sorumlu olduğunu bildiğini; ŞİRKET dışına bu bilgilerin çıkması durumunun sadece iş amaçlı ve ŞİRKET'in yazılı onayı ile olabileceğini; bu bilgilerin saklanırken veya transfer edilirken şifreleme gibi teknik önlemler alacağını,
- Sözleşme gereği erişilen kişisel bilgilerin, Kişisel Verilerin Korunması Kanunu'na (KVKK) uygun olarak kullanılması, işlenmesi ve korunması gerektiğini bildiğini ve buna ilişkin önlemleri aldığını,

- Sözleşme gereği kişisel verisi alınan kişiye/kişilere KVKK kapsamında yerine getirilmesi gereken aydınlatmayı, bilgilendirmeyi sağlayacağını ve alınması gereken onayları alacağını,
- Elde edilen her türlü veriyi yetkisiz/sözleşme gereği erişim ihtiyacı olmayan kişilerle paylaşmayacağını/ifşa etmeyeceğini;
- ŞİRKET ile ilgili hukuki ilişkinin bitiminden sonra da gizliliğe ilişkin taahhütlerin süresiz şekilde devam ettiğini,

b) ÜRETİCİ yazılım/donanım sağlıyorsa;

- İlgili yazılımda güvenliğin sağlanmasına ilişkin kontrolleri alacağını, OWASP top 10'deki güvenlik açıklarına ilişkin kontrolleri yapacağını ve/veya yazılımın sızma testinden geçirilerek güvenlik açığı barındırmamasını sağlaması gerektiğini,

- Yazılımda, teknik şartnamede belirtilen şartların yanı sıra, minimumda aşağıdaki güvenlik kontrollerini almak zorunda olduğunu, alamadığı güvenlik kontrolleri için ŞİRKET'in some@enerjisa.com e-posta adresine bildireceğini,

- Aşağıdaki hususların sağlanacağını;

    - Kimlik doğrulama için LDAP, AD veya SAP entegrasyonunun sağlanması; eğer sağlanamıyorsa şifrenin zor tahmin edilmesini sağlayıcı, AD tarafında belirlenebilen minimum şifre uzunluğu, belirli sayıda başarısız deneme sonrasında şifrenin kilitlenmesi, tekrarlayan harf/rakam içerilmemesi vb. gibi kontrollerin uygulanabiliyor olması
    - Uygulamada rol bazlı yetkilendirmeye olanak sağlanması
    - Kullanıcı işlemlerinde ve uygulama admin panellerinde yapılan her işlemin, işlem tarihi, zamanı, kullanıcı adı ve detayını içerir şekilde loglanması
    - Logların IBM Qradar ürünü ile entegrasyonunun yapılabilir olması
    - Verilerin ve akışlardaki bütünlük kontrollerinin sağlanıyor olması
    - Tüm girdi alanlarında, girdilerin tipine göre, format, uzunluk, dosya tipi gibi kontrollerin yapılmasının sağlanması, kullanıcıya güvenliği tehdit etmeyecek şekilde bilgilendirme yapılmasının sağlanması (örneğin parolayı yanlış girdiniz değil, kimlik bilgilerini yanlış sağladınız şeklinde hatanın parolada olduğunun belli olmayacağı şekilde bilgilendirme dönülmesi)
    - Uygulamada gizli/kritik veri işleniyorsa, verilerin saklanma ve transferi esnasında geçerli bir şifreleme metodu ile şifrelenmesi (AES256, SSL vb.)
    - Uygulamaların local admin hakkıyla çalışmıyor olması

- Sağlanan yazılım/donanımda ŞİRKET'nin bilgisi haricinde bir arka kapı bırakılmayacağını,

- Uygulama ve sistem ile ilgili tüm dokümantasyon, kullanıcı kılavuzları ve kurulum esnasında sağlanan tüm kullanıcı kodlarının yazılı olarak ŞİRKET'e teslim edileceğini,

- Aksi Taraflarca yazılı olarak kararlaştırılmadıkça yapılacak işlerle ilgili ortaya çıkacak her türlü fikri ve sınai mülkiyet haklarının ŞİRKET'e ait olacağını,

- Sağlanan hizmet kapsamında ŞİRKET için kod geliştiriliyor ise ÜRETİCİ kodların güvenliğinin sağlanmasına azami hassasiyet gösterecek olup, kodlar github vb. ortamlarda kesinlikle paylaşılmayacaktır. Bu gizlilik taahhüdü taraflar arasındaki ilişkinin sonlanması sonrasında da devam edecek olup, tespit edilmesi durumunda paylaşan kişi hakkında hukuki yaptırımı uygulanacaktır.

c) ÜRETİCİ bir hizmetin sağlanmasında/ bir cihazın/uygulamanın işletilmesinde görev alıyorsa;

- Kendi sorumluluğu altındaki bilgi, sistem ve yazılımlarda; kimlik doğrulama, yetkilendirme, loglama, şifreleme, akış ve bilgi bütünlüğüne ilişkin kontrolleri alması gerektiğini ve bu kontrollerin minimumda aşağıdaki konuları içerdiğini,

    - Her kullanıcının kendine özel bir kullanıcı adı ve şifresi olmalıdır.
    - Sistemler üzerinde gerçek kullanıcıların, genel kullanıcı hesapları ve sistem/servis/uygulama kullanıcı hesaplarının kullanılması engellenmelidir.
    - Her türlü kişisel veriye erişim/işleme, yönetimsel (administrative) tüm işlemler ile sistem/uygulama üzerindeki kritik işlemler, işlemi yapan kullanıcı, erişim sağlanan cihaz (IP ve/veya MAC), tarih, zaman, işlem detayı olacak şekilde loglanmalıdır.
    - Loglar, sistem/uygulama yöneticileri tarafından değiştirilemeyecek/silinemeyecek şekilde farklı bir ortamda saklanmalıdır.
    - Sistemler bir atak denemesine karşı izlenmelidir.

- Kendi sorumluluğu altındaki bilgi, sistem ve hizmetlerin iş sürekliliği gereksinimlerine uygun olarak kurgulayacağını, istenildiği takdirde iş süreklilik planlarını ŞİRKET'e sunacağını ve ŞİRKET iş sürekliliği plan/test/tatbikatlarına istendiği takdirde eşlik edeceğini,

- Kendi sorumluluğu altındaki bilgi, sistem ve hizmetlerin sürdürebilirliği için ŞİRKET ile yedekleme periyodunda el sıkışılması gerektiğini, yedeklerin alındığının düzenli kontrol edilmesi gerektiğini ve bir problemin ortaya çıkması durumunda ŞİRKET'in işine olan etkisinin en aza indirgenmesi için gerekli kontrolleri alması gerektiğini,

- ŞİRKET'in bilgisi haricinde ve yazılı onayı olmaksızın herhangi bir altyükleniciye ŞİRKET'in işini veya işinin bir bölümünü yaptıramayacağını; yazılı onayı olması durumunda da işbu sözleşme ve eklerinde yer alan tüm şartların sağlanmasından firmanın sorumlu olduğunu,

- ŞİRKET'in kendi sistemleri veya verileri üzerinde yapılan her işlemi kaydedip, izleyebileceğini bildiğini,

d) Genel olarak;

- Şahit olduğu bilgi güvenliği ihlallerini en geç 24 saat içerisinde ŞİRKET SOME adresine some@enerjisa.com e-posta yolu ile bildireceğini,

- ŞİRKET'in sistem, uygulama veya tesislerine giriş için çalışana tanımlanmış olan erişim parolası, kimlik kartı gibi bilgilerini başka bir kişiyle paylaşmayacağını,

başkalarınınkini öğrenmeye çalışmayacağımı, kimlik kartı/parola bilgilerinin farklı bir kişinin eline geçmesi/kaybolması veya şifresinin ortak kullanılmaya zorlanması gibi bir risk oluştuğunda ŞİRKET SOME adresine bildireceğini;

- ŞİRKET tarafından firmaya sağlanan her türlü imkânın (yazılım/donanım/e-posta/internet/bilgi vb.) ŞİRKET'in işleri için kullanılacağını, yasadışı, etik kurallara aykırı, sözleşme gereksiniminin bir parçası olmayan ya da ŞİRKET'e doğrudan ve dolaylı olarak zarar verebilecek tüm kullanımlarda ŞİRKET SOME adresine e-posta yolu ile bildireceğini;

- İş gereksinimin bir parçası olan yedekleme ve arşivleme ihtiyaçları dışında yazılımları/bilgileri kopyalamayacağını, çoğaltmayacağını, değiştirmeyeceğini, başkaları tarafından kopyalanmasına, çoğaltılmasına ve değiştirilmesine izin vermeyeceğini,

- ŞİRKET Bilgi Güvenliği ekibinin yazılı izni olmadan, bilgi varlıklarına (yazılım, donanım, sistem, veri, bina vb.) erişim denemeleri yapmayacağını, kendisine verilen yetkileri arttırmaya yönelik teşebbüste bulunmayacağını, ŞİRKET Bilgi Güvenliği ekibinin yazılı izni olmadan ağı/ortamı dinlemeyeceğini, ŞİRKET bilişim ortamlarında Sızma ve Zafiyet Analizi Testleri yapmayacağını,

- ŞİRKET tarafından sağlanan cihazlara yüklenmemiş ya da yüklenmesine yazılı onay verilmemiş yazılımlar dışında herhangi bir işletim sistemi veya yazılım yüklemeyeceğini, yazılım veya donanımın güvenlik kontrollerini araştırmaya yönelik teşebbüste bulunmayacağını, devre dışı bırakmaya çalışmayacağını, ters mühendislik veya derleme işlemlerini yapmayacağını veya bunları analiz etmeyeceğini,

- İstendiğinde ya da hizmet bitimi sonunda, ŞİRKET ile ilişkili tüm bilgileri iade edeceğini veya geri dönülemeyecek şekilde imha edeceğini/ettireceğini, imhaya ilişkin tüm belgeleri ŞİRKET'e ibraz edeceğini; kendisine sağlanan tüm cihaz ve yazılımları iade edeceğini,

- ŞİRKET adına ve ŞİRKET'e ilişkin bilgileri kullanarak herhangi bir mecrada, açıklamada bulunmayacağını,

- ŞİRKET'in yazılı izni olmadan, ŞİRKET tesislerinde fotoğraf/kamera çekimi, ses kaydı vb. gerçekleştirmeyeceğini,

- ŞİRKET'in bilgi güvenliğine dair tabii olduğu bütün kanunlara, düzenlemelere ve yönetmeliklere uyacağını,

- ŞİRKET tarafından bilgi güvenliği ile ilgili kendisine bildirilen düzenlemelere, prosedürlere, etik kurallara uyacağını; bir güvenlik ihlali/açığı bildirilmesi durumunda veya ŞİRKET'in denetimleri esnasında durumun doğru tespiti, olayın aydınlatılması için gerekli bilgi, belge ve ortamı sağlayacağını; doğru bilgi vereceğini; bir güvenlik açığı mevcut ise ivedilikle önleyici ve düzeltici önlemleri alacağını, durumu derhal ŞİRKET'e bildireceğini, olayın aydınlatılmasında etkisi bulunacak denetim iz kayıtlarının (log) saklanmasını sağlayacağını bilerek, kabul ve taahhüt eder.

(ÜRETİCİNİN unvanı)

(ÜRETİCİ) adına,

(ÜRETİCİ yetkilisinin adı soyadı)

(ÜRETİCİNİN imzası)

(KAŞE)

(TARİH)