BELGELENDİRME KRİTERİ

CERTIFICATION CRITERIA

TSE K .....
Ay Yıl

ICS ……

KAMU GÜVENLİ VERİ PAYLAŞIM KRİTERİ

PUBLIC SAFETY DATA SHARING CRITERIA

TÜRK STANDARDLARI ENSTİTÜSÜ
Necatibey Caddesi No.112 Bakanlıklar/ANKARA

- Bugünkü teknik ve uygulamaya dayanılarak hazırlanmış olan bu standardın, zamanla ortaya çıkacak gelişme ve değişikliklere uydurulması mümkün olduğundan ilgililerin yayınları izlemelerini ve standardın uygulanmasında karşılaştıkları aksaklıkları Enstitümüze iletmelerini rica ederiz.

- Bu kriteri oluşturan uzmanların emeklerini; tasarılar üzerinde görüşlerini bildirmek suretiyle yardımcı olan bilim, kamu ve özel sektör kuruluşları ile kişilerin değerli katkılarını şükranla anarız.

Kalite Sistem Belgesi
İmalât ve hizmet sektörlerinde faaliyet gösteren kuruluşların sistemlerini TS EN ISO 9000 Kalite Standardlarına uygun olarak kurmaları durumunda TSE tarafından verilen belgedir.

Türk Standardlarına Uygunluk Markası (TSE Markası)
TSE Markası, üzerine veya ambalâjına konulduğu malların veya hizmetin ilgili Türk Standardına uygun olduğunu ve mamulle veya hizmetle ilgili bir problem ortaya çıktığında Türk Standardları Enstitüsü'nün garantisi altında olduğunu ifade eder.

Kritere Uygunluk Belgesi (TSEK Markası Kullanma Hakkı)
Kritere Uygunluk Belgesi; Türk Standardları bulunmayan konularda firmaların ürünlerinin ilgili uluslararası Standardlar, benzeri Türk Standardları, diğer ülkelerin milli standardları, teknik literatür esas alınarak Türk Standardları Enstitüsü tarafından kabul edilen Kalite Faktör ve Değerlerine uygunluğunu belirten ve akdedilen sözleşme ile TSEK Markası kullanma hakkı verilen firma adına düzenlenen ve üzerinde TSEK Markası kullanılacak ürünlerin ticari Markası, cinsi, sınıfı, tipi ve türünü belirten geçerlilik süresi bir yıl olan belgedir.

DİKKAT!

TS işareti ve yanında yer alan sayı tek başına iken (TS 4600 gibi), mamulün Türk Standardına uygun üretildiğine dair üreticinin beyanını ifade eder. **Türk Standardları Enstitüsü tarafından herhangi bir garanti söz konusu değildir.**

Standardlar ve standardizasyon konusunda daha geniş bilgi Enstitümüzden sağlanabilir.

Ön söz

- Bu belgelendirme kriteri, Türk Standardları Enstitüsü Belgelendirme Merkez Başkanlığı tarafından hazırlanmış ve Belgelendirme Kriteri Değerlendirme ve Onay Komitesinin …… tarihli toplantısında kabul edilerek yayımına karar verilmiştir.

- Bu kriterde kullanılan bazı kelime ve/veya ifadeler patent haklarına konu olabilir. Böyle bir patent hakkının belirlenmesi durumunda TSE sorumlu tutulamaz.

İçindekiler

Kamu Güvenli Veri Paylaşım Kriteri

1 Kapsam

Bu kriter, kamu kurumları arasında güvenli veri paylaşım kurallarını ve prosedürlerini kapsar. Kamu kurumlarının merkez ve taşra teşkilatları arasındaki veri paylaşımı da bu kriter kapsamındadır. Tasnif dışı verilerin paylaşılması bu kriter kapsamında değildir. Bu kriter de bahsedilen veri paylaşımı; taşınabilir manyetik ortamlar, posta, ses, faks, elektronik ortamlar ve yazıcı çıktısı gibi çeşitli formlarda olabilir.

2 Atıf yapılan standard ve/veya dokümanlar

Bu kriterde standard ve/veya dokümanlara atıf yapılmaktadır. Bu atıflar metin içerisinde uygun yerlerde belirtilmiş ve aşağıda liste halinde verilmiştir. (*) işaretli olanlar bu kriterin basıldığı tarihte İngilizce metin olarak yayımlanmış olan Türk standardlarıdır.

TS No	Türkçe adı	İngilizce adı
TS ISO/IEC 27001:2013	Bilgi teknolojisi – Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri – Gereksinimler	Information technology - Security techniques - Information security management systems – Requirements
TS ISO/IEC 19790:2012	Bilgi teknolojisi - Güvenlik teknikleri - Kriptolama modülleri için güvenlik gereksinimleri	Information technology - Security techniques - Security requirements for cryptographic modules
TS 13638	Bilgi teknolojileri - Güvenlik teknikleri - Sızma testi yapan personel ve firmalar için şartlar	Administrative criteria for penetration testers and organizations conducting penetration tests

3 Terimler, tarifler ve semboller

Bu kriter için aşağıdaki terim ve tarifler geçerlidir.

3.1 Kaynak kurum

Paylaşıma açılacak/açılan verinin sahibi kamu kurumu,

3.2 Alıcı kurum

Paylaşıma açılacak verilerden, yapılacak protokol çerçevesinde yararlanan kamu kurum ve kuruluşları,

3.3 Veri

Çeşitli yöntemlerle toplanan kişisel ve/veya kurumsal nicel ve/veya nitel bilgileri.

3.4 Gizli veri

Açıklanması hâlinde Devletin emniyetine, dış ilişkilerine, millî savunmasına ve millî güvenliğine açıkça zarar verecek ve niteliği itibarıyla Devlet sırrı olan gizlilik dereceli bilgi veya belgeler ile gerçek ya da tüzel kişilerin doğrudan veya dolaylı bir şekilde özellikleri ile birlikte tanınabilmesine ve bu şekilde bireysel bilgilerin açığa çıkarılmasına imkân sağlayan bireysel veya tablo halinde saklı tutulan veriler,[1]

3.5 Sanal Özel Ağ

Güvenilmeyen ağlar üzerinden güvenli bir ağ oluşturularak uzak sistemlerin birbirleri arasında iletişim kurmasını sağlayan ağ yapısını,

4 Veri paylaşımı protokolü

Sürekli veri paylaşımı ve tek seferlik gizli veri taleplerinde, kurumlar bir protokol metni imzalamalıdır.

Veri paylaşımını düzenleyen mevzuatın bulunduğu durumlarda, ihtiyaç duyulan konularda protokol imzalanması mevzuatın sahibi kuruluşça değerlendirilir.

[1] 09/10/2003 tarih ve 4982 sayılı Bilgi Edinme Hakkı Kanunu ve 10/11/2005 tarih ve 5429 sayılı Türkiye İstatistik Kanunu

4.1 Verilerin kullanım amacı
Verilerin hangi amaçlar için kullanılacağı protokollerde belirtilmelidir. Verilerin üçüncü taraflarla paylaşılıp paylaşılmayacağı da bu kapsamda belirtilerek paylaşılacaksa yükümlülükler açıklanmalıdır.

4.2 Kişisel verilerin korunması
Veri paylaşımı esnasında kişisel verilen paylaşılması hususunda doğabilecek tüm yükümlülükler protokollerde belirtilmelidir.

4.3 Personel listesi
Verilerin paylaşımında görev alacak karşılıklı personel bilgilerine (ad soyad, unvan, telefon, faks, e-posta) ve görevli personelin üye olduğu eposta grubunun adına protokolde yer verilmelidir. Personel değişikliğinde izlenecek prosedür açıklanmalıdır. Görev alacak personel e-posta yoluyla yapılacak iletişimde sadece kurumsal e-posta adresini kullanmalıdır.

4.4 Değişiklik taplepleri
Veri paylaşımı esnasında ileride ihtiyaç duyulabilecek protokol içeriğindeki değişiklik taleplerinin nasıl ele alınacağı protokolde belirtilmelidir.

4.5 Protokol nüshaları
Protokol, hem kaynak kurum da ve hem de alıcı kurum da muhafaza edilmelidir.

4.6 Veri deseni listesi
Paylaşılacak verilerin deseni protokol ekinde yer almalıdır.

4.7 Verilerin paylaşıma başlanılması ve paylaşımın sonlandırılması
Verilerin ne zaman paylaşıma açılacağı ve paylaşımın ne zaman sonlandırılacağı protokollerde belirtilmelidir. Eğer, teknik bir çalışma veya yatırım beklenecekse, bu hususun gerçekleşmesi için tarafların yükümlülükleri yanlış anlaşılmalara mahal vermeyecek bir biçimde belirtilmelidir.

4.8 Hizmet kesintisi
Veri hizmetinin sürekli olması durumunda, öngörülen kesintiler ve kesinti esnasında alınacak önlemler protokolde belirtilmelidir.

4.9 Verilerin depolanması
Paylaşılan verilerin depolanıp depolanmayacağı, depolanacak ise ne kadar süre zarfında ve hangi şartlarda depolanacağı, nasıl imha edileceği protokollerde açıkça belirtilmelidir.

4.10 Ek yatırım maliyetleri
Hizmetlerin sürekli veya tek seferlik ek yatırım gerektirmesi durumunda ek yatırım maliyetlerinin hangi tarafça karşılanacağı protokolde belirtilmelidir.

4.11 Gizlilik taahhüt belgesi
Taraflar, verilere erişen personele “Gizlilik Taahhüt Belgesi” imzalattırmalı ve saklanmasını sağlamalıdır. Taraflar, birbirlerinden bu gizlilik taahhüt belgesinin bir örneğini isteyebilir. Gizlilik Taahhüt Belgesi içeriğinde aşağıdaki hususların yer alması tavsiye edilir;

a) Korunacak verilerin tanımı,
b) Gizliliğin süresi,
c) Taahhüttün ihlali durumunda işletilmesi gereken prosedür.

4.12 Hukuki sonuçlar
Taraflarca alınacak verilerin kullanılmasının hukuki sonuçlarından tarafların ne derece de yükümlü olacağı belirtilmelidir. Bu kapsamda verilerin kullanılmasında ve paylaşımında Anayasa, uluslararası sözleşmeler ve ulusal mevzuatta yer alan özel ve ticari hayatın gizliliğine ilişkin hükümler uygulanır.

4.13 Veri paylaşım türleri
Bölüm 6’da belirtilen veri paylaşım türlerinden hangisinin kullanılacağı protokol metninde belirtilmelidir.

4.14 Elektronik ortam kullanıcı kodu ve şifre politikası

Taraflar arasında kullanıcı kodları ve şifre uzunluğu, karmaşıklığı, değişim süresi vb. gibi konularda mutabakata varılması ve bu hususun protokolde yer alması tavsiye edilir.

5 Yükümlülükler

5.1 Alıcı kurum yükümlülükleri

5.1.1 İz kayıtlarının tutulması

Alıcı kurum; kaynak kurum tarafından sağlanan verilere erişen sistemlerin ve kullanıcıların erişim kayıtlarını güvenli bir ortamda tutmalıdır. İz kayıtlarının içeriği; kullanıcı kimliği, oturum açma ve oturum kapama gibi anahtar olayların tarihleri, saatleri ve detayları, başarılı ve reddedilmiş sistem erişim bilgileridir. İz kayıtları kimlerin veriye eriştiğini açıklayacak şekilde olmalıdır, ortak kullanıcı adları ve şifreler gibi kimin kullandığı belli olmayan erişim yetkileri doğru bir uygulama değildir. İz kayıtları, bütünlüğü ve güvenilirliği temin etmek amacıyla zaman damgası kullanılarak imzalanmalı ya da verinin bütünlüğünü garanti eden yazılımlar ile imzalanmalıdır ve en az 1 (bir) yıl süre ile saklanmalıdır. İz kayıtlarının güvenliği sağlanmalı ve iz kayıtları yetkisiz erişimlere karşı korunmalıdır.

5.1.2 Güvenlik

Alıcı kurum, veri talebine uygun olarak yaptığı çalışmaların gizli verilerin açıklanmasına imkân vermeyecek şekilde yürütülmesini sağlar. Verilerin istenilen amaç dışında kullanılmaması için her türlü önlemi alır ve verinin incelenip değerlendirilmesi aşamasındaki gizli verinin bulunduğu ortama fiziksel veya elektronik yollarla yetkisiz erişimin engellenmesi için gerek duyulan güvenlik sistemini kurar ve/veya gerekli tedbirleri alır.

5.2 Kaynak kurum yükümlülükleri

5.2.1 İz kayıtlarının tutulması

Kullanıcı işlemleri, kural dışı durumlar ve hatalar saklanmalı ve düzenli olarak gözden geçirilmelidir. Olağan dışı durumlar olduğunda ilgili Alıcı Kurum ile iletişime geçilmelidir. İz kayıtları, bütünlüğü ve güvenilirliği temin etmek amacıyla zaman damgası kullanılarak imzalanmalı ve en az 1 (bir) yıl süre ile saklanmalıdır. İz kayıtlarının güvenliği sağlanmalı ve iz kayıtları yetkisiz erişimlere karşı korunmalıdır.

5.2.2 Bildirim

Bakım, güncelleştirme ve diğer değişiklikler nedeni sistemde öngörülen her türlü kesintiler en az 24 saat öncesinde kaynak kurum tarafından alıcı kuruma bildirilir. Bildirim, protokolde belirlenen personel tarafından iletişim yollarından biri ile yapılır ve kaydı tutulur.

.

5.3 Ortak yükümlülükler

5.3.1 Saat senkronizasyonu

İz kayıtlarının incelenmesinde herhangi bir yanlış anlaşılmaya mahal verilmemesi amacıyla saat senkronizasyonu konusunda tarafların bir uzlaşıya varılması önerilir.

5.3.2 Teknik güvenlik

Taraflar, sisteme erişim ve/veya web servislerin kullanılması için birbirlerine vereceği kullanıcı adı, parola ve sertifikalar ile diğer bilgilerin gizliliğinden ve korunmasından, kendi sistemlerinin güvenliğini sağlamak üzere gerekli tedbirlerin alınmasından sorumludur.

Bu hususu temin etmek maksadı ile söz konusu hizmetler ve hizmetlerin kullanıldığı sistemler yılda en az 1 (bir) kez sızma testine tabi tutulmalıdır. Bu kritere uyum kapsamında yapılacak tetkiklerde dikkate alınmak üzere geriye dönük olarak en az 5 (beş) yıllık test yapıldığına dair belgeleri saklanmalıdır. Sızma testleri; TS 13638 Bilgi teknolojileri - Güvenlik teknikleri - Sızma testi yapan personel ve firmalar için şartlar standardına uygunluğu olan personel veya firmalar tarafından yapılmalıdır.

5.3.3 Kriptografi kullanımı

Verilerin paylaşımı için kriptografi kullanılacaksa; taraflarca ISO/IEC 19790:2012 Bilgi güvenliği – Güvenlik teknikleri – Kriptolama modülleri için güvenlik gereksinimleri standardı ile uyumlu kriptografik anahtarların kullanımı, korunması ve yaşam süresine dair bir politika geliştirilmeli ve tüm yaşam çevirimleri süresince uygulanmalıdır.

6 Veri Paylaşımı ve Türleri

6.1 Fiziksel ortamda veri paylaşımı

Verilerin fiziksel ortamda paylaşılmasıdır. Fiziksel verilerin alıcı kurum tarafından alındığının teyit edilmesi gereklidir. Veri paylaşımında kullanılan parola/şifre/anahtar veri paylaşım yönteminden farklı bir yolla paylaşılmalıdır.

6.1.1 Kurye ile yığın veri paylaşımı

Elektronik ortamda paylaşımın mümkün olmadığı yığın verilerde kullanılır. Bir kere veya tekrarlı olarak harici bellek ile iletilecek veriler protokolde yazılan bir standart dosya şifreleme yöntemleriyle (AES, RSA, SHA, MD5 vb.) ve protokolde belirtilen esaslar çerçevesinde görevlendirilen kurye ile taşınır ve paylaşım gerçekleştikten sonra protokolde yazılan silme yöntemleriyle harici bellekten silinir.

6.1.2 Posta ile veri paylaşımı

Posta ile iletilecek veriler şifreleme yöntemleriyle (AES, RSA, SHA, MD5 vb.) şifrelenerek CD, DVD vb. ile kapalı bir zarf içerisinde gönderilir. Zarf taahhütlü ya da iadeli taahhütlü olarak gönderilir ve alıcısına ulaşıp ulaşmadığı kontrol edilir.

6.1.3 Telefon ile veri paylaşımı

Telefonla hiçbir veri iletilmez.

6.2 Elektronik ortamda veri paylaşımı

Verilerin elektronik olarak siber ortamda paylaşılmasıdır. Alıcı ile veri paylaşımında verinin içeriği dikkate alınarak ve risk değerlendirmesi yapılarak uygun elektronik alt yapı olan web servis, VPN, SFTP, HTTPS vb. uygulamalar güvenli bir şekilde kullanılmalıdır.

Elektronik ortamda veri paylaşımında her türlü bilgi paylaşımı için kullanılan kriptografik anahtarlar ve parolalar en az yılda 1 (bir) kez değiştirilir. Kritere uyumluluk kapsamından değişikliklerin yapıldığı tarih kayıt altına alınır.

Elektronik ortamda veri paylaşımında web uygulamaları kullanıldığında; Web Uygulamaları, Türk Standardları Enstitüsü tarafından yayınlanan Web Uygulamaları Koruma Profiline uygun olmalıdır

6.2.1 Elektronik posta

Veriler elektronik posta ortamında iletilirken sadece kaynak ve alıcı kurumların kurumsal uzantılı e-posta adresleri kullanılır, veri ulaştıktan sonra bilgi verilmesi istenir. Hem alıcı hem de kaynak kurum geçerli bir SSL sertifikası kullanmalıdır. Elektronik posta gönderimi sırasında güvenlik ve kullanıcı doğrulama amacıyla şifreleme yazılımları kullanılabilir.

6.2.2 Web servisler

Veri deseninin düzenli olduğu ve veri paylaşımının sistemler tarafından yapılması durumunda web servisler kullanılmalıdır. Verilerin transfer seviyesinde hem alıcı hem de kaynak kurum tarafından geçerli bir SSL sertifikası kullanılmalıdır. Elektronik ortamdaki veri sağlama metotlarında geliştirme ve test ortamları gerçek ortamdan muhakkak ayrılmış olmalıdır. Geliştirme ve test ortamları birlikte kullanılabilir. Web servis bileşenlerini tanımlamada en az WSDL 1.1 kullanılmalıdır ve söz konusu bileşenleri sadece izin verilen IP adresi görebilmelidir.

Web servislerin güvenliğinde;

- WS-Security 1.1, WS-Trust 1.3 ve WS-SecurityPolicy 1.2 web servis güvenliği standartlarının desteklenmesi gerekmektedir.
- Veriye erişim için parola ve kriptografi göz önünde bulundurulmalıdır.
- Kaynak kurum ile alıcı arasında sanal özel ağ (VPN) kurulması tavsiye edilir. Özel ağ sağlanamadığı durumlarda kaynak kurum güvenlik duvarında (Firewall) sadece alıcı kurumun IP adresine, kullanılacak port numaralarına ve protokollere izin verilmelidir.
- Web servis istemleri SOAP 1.2 standardına uygun olmalıdır.

- Web servisler Türk Standardları Enstitüsü tarafından yayınlanan Web Servis Güvenliği için Ortak Kriterler Koruma Profiline uygun olmalıdır.

6.2.3 Güvenli dosya paylaşım protokolü

Güvenli dosya taşıma yöntemi (SFTP), web servis ile paylaşılamayan veri deseni ile daha büyük veriler için kullanılır. Kaynak kurum ile alıcı arasında sanal özel ağ (VPN) kurulması tavsiye edilir. Özel ağ sağlanamadığı durumlarda kaynak kurum güvenlik duvarında (Firewall) sadece alıcı kurumun IP adresine izin verilmelidir. Veri erişim kullanıcı kodu ve parola ile olmalıdır.

Veri paylaşımı kaynak kurumun dosya paylaşım sunucusundan alıcıya veya dosya paylaşım istemci uygulaması ile alıcı kurumun dosya paylaşım sunucusuna olmak üzere iki yönlü olarak kullanılabilir. Alıcı veya kaynak kurumun hangisinin dosya paylaşım sunucusunu yöneteceğine protokolde yer verilir. Paylaşım gerçekleştikten sonra dosyaların hangi sıklıkla silineceği protokolde belirtilmelidir.

6.2.4 Sanal özel ağ

Sanal özel ağ (VPN) ile daha önce ifade edilen elektronik veri paylaşım yöntemleriyle beraber kullanılabilir. Sadece ilgili servislerin çalıştığı cihazlar arasında erişim açılmalıdır. Bunun dışındaki tüm haberleşme ve protokol/adres kapatılmalıdır.

6.2.5 E-formlar

HTTPS protokolü üzerinden çalışan web sayfalarında doldurulacak e-formlar aracılığı ile veri paylaşımı yapılabilir.

7 Çeşitli hükümler

Verilerin paylaşımında; Anayasa, uluslararası sözleşmeler ve ulusal mevzuatta yer alan özel hayatın gizliliğine ve ticari sır niteliğindeki verilerin korunmasına ilişkin hükümler esas alınır. Mevzuata aykırı bir şekilde veri paylaşımı yapılamaz.

Bu kritere uyum maddelerinin sağlanması ile kontrol edilir.

Bu kriter, hem veri alan, hem veri sağlayan ve her iki işlevi birden yapan kurumlar için düşünülmüştür. Kamu kurumları tüm veri alışverişlerinde bu kriterin yükümlülüklerine uymalıdır.