Bilgi Transferi Prosedürü

DEĞİŞİKLİK TAKİP LİSTESİ

No	Tarih	Açıklama
00	29.11.2021	İlk Yayın

İÇİNDEKİLER

1. **AMAÇ**

Bu prosedür, kurum içi ve dışı olası bilgi alışverişinden kaynaklanacak risklerin önüne geçmek için gerekli kuralları tanımlamayı amaçlar.

2. KAPSAM

Bu prosedür, kurumdaki bilgi sistemlerini meydana getiren varlıkları, personeli, üçüncü tarafları ve iş süreçlerini kapsamaktadır.

3. UYGULAMA

3.1. Bilgi Transferi

Bilgi İşlem Daire Başkanlığı, iç ve dış taraflar ile bilgi değişimini yazışmalar, web servisleri, elektronik iletişim, dosya paylaşımı ve medya transferi gibi farklı yollarla gerçekleştirmektedir. Bu değişim yöntemleri ile ilgili güvenlik kontrolleri ve uygulamaları aşağıdaki başlıklarda belirtilmiştir.

3.1.1. Kurum İçi Bilgi Transferi

3.1.1.1. Kurum birimleri arasındaki bilgi değişimi iç yazışma esasına dayanır

3.1.1.2. Birimler arasında bilgi değişimi onayları birim amiri seviyesinde verilir.

3.1.1.3. Kurum içerisindeki yazışmalar, kurum teamüllerine uygun olarak sağlanır, saklanır ve imha edilir.

3.1.1.4. Birime gelen evraklar Elektronik Belge Yönetim Sistemi (DYS) aracılığı ile kişilerin ilgileri doğrultusunda yönetimce sevk edilir. İlgili işlem tamamlandıktan sonra evrak sonlandırılarak ya da cevap yazılarak süreç tamamlanır.

3.1.2. Kurumlar arası / Müşteri / Üçüncü Taraflar ile Bilgi Transferi

Kurum, diğer kurum ve kuruluşlar ile kritik bazı bilgi değişimleri gerçekleştirmektedir. Kurum, üçüncü taraflarla bu bilgi değişimi ve paylaşımını web servisleri, dosya paylaşımı, elektronik iletişim, uygulamalar, elden teslim vb. gibi farklı yöntemler ile gerçekleştirir.

3.1.2.1. Bilgi transferleri için yapılan anlaşmalar, muhatap kurum ve kuruluşun sağladığı bir protokol/sözleşme metni ile olabilir.

3.1.2.2. Anlaşmada bilgi transferi için bilgi transferinden sorumlu kişiler, bilgileri saklama, kullanım ve paylaşım koşulları, bilgi değişiminin nasıl gerçekleşeceği, ne tür güvenlik önlemlerinin alınacağı ve tarafların sorumlulukları belirtilir.

3.1.2.3. Bilgi transferinin güvenliği, protokol/sözleşmede belirtildiği şekilde gerek kurum gerekse üçüncü taraf tarafından sağlanır.

3.1.2.4. Bilgi transferi yapılmadan önce, transfer edilecek bilginin hassasiyet / kritikliği seviyesine göre Bilgi Güvenliği Yöneticisi tarafından şartlarını değerlendirir ve hassasiyet / kritiklik seviyesine bağlı olarak (gizli / çok gizli) transferi onaylar.

3.1.2.5. “Hizmete özel” ve daha düşük hassasiyetteki bilgi transferi için Bilgi Güvenliği Yönetici onayı aranmaz.

3.1.2.6. “Çok Gizli” bilgiler herhangi bir kişi veya kurum ile güvenli olmayan yöntemler ile paylaşılmaz.

3.1.2.7. Kuruma ait bilgilerin diğer taraflarla paylaşılması tüm yasal, düzenleyici kurallar ve kurum politikaları ile uyumlu olmalıdır.

3.1.2.8. Özel olarak kişisel verilerin korunması, insan hakları ve genel gizlilik kurallarına uyulacaktır.

3.1.2.9. Yazılım geliştirme hizmeti alınan 3. taraflar ile yapılacak bilgi değişiminde, bilgiye yetkisiz erişim ve yetkisiz ifşanın engellenmesi için, sözleşmelerde gizlilik maddelerine yer verilir ve hem Üçüncü Taraf Kurumsal Güvenlik Sözleşmesi hem de personel düzeyinde Üçüncü Taraf Personeli Güvenlik Taahhütnamesi imzalanır.

3.1.3. Fiziksel Bilgi Taşıma

Kurum, diğer kurum ve kuruluşlar ile bilgi transferini gerektiğinde basılı evrak, taşınabilir disk, cd/dvd, flash disk, taşınabilir depolama ünitesi, hafıza kartı vb. ortamlar aracılığıyla yapabilir.

3.1.3.1. Periyodik veya sürekli gerçekleştirilen bilgi transferi için madde 3.1.2'de belirtildiği şekilde, taraflar arasında bilgi transferinin güvenliği için gerekli protokol/sözleşmenin yapılmış olması gerekmektedir.
3.1.3.2. Ancak, seyrek veya tek seferlik yapılan fiziksel bilgi aktarımı (resmi yazı ile bilgi iletme, bilgi edinme taleplerine cevap verme vb.) için 3.1.2 maddesindeki protokol/sözleşme yapılması şartı aranmaz.
3.1.3.3. Ancak bu tür bilgi transferi işlemlerinin güvenli olarak gerçekleştirilmesi için karşı tarafla görüşerek mutabakata varılır.
3.1.3.4. Taşıma işlemi öncesi bilgi değişiminin yetkilendirilmesi için madde 3.1.1.2'de belirtildiği gibi Bilgi Güvenliği Yöneticisinin onayı alınır.
3.1.3.5. Taşıma öncesi "**FR.20 Varlık Transfer Formu"** doldurularak Bilgi Güvenliği Yöneticisinin onayı alınır.
3.1.3.6. Onay verilmeyen taşıma işlemleri gerçekleştirilmez.
3.1.3.7. Taşınacak olan bilgi, taşıma ortamında mümkün ise şifreli/kilitli/görülemeyecek şekilde taşınmalıdır (şifreler sadece gönderen ve alacak olan taraflarda bulunmalıdır).

3.1.4. Kurumsal E-posta Hizmeti

Kurumsal e-posta Hizmeti Bilgi İşlem Daire Başkanlığı tarafından verilmektedir. Web üzerinden kullanıcılar e-postalarına ulaşabilmektedir. Exchange ActiveSync özelliği ile kullanıcılar, e-postalarına mobil cihazlardan da ulaşabilmektedirler. Elektronik mesajlaşma için sunucular ile istemciler arasında SSL sertifikası kullanılmaktadır.

3.1.4.1. Kurum dışı elektronik posta alışverişinde SMTP protokolü kullanılmaktadır.
3.1.4.2. E-posta sunucusu tarafından sunulan Web Application Roundcube ve Outlook hizmetlerinin tamamında SSL sertifikası kullanılır.
3.1.4.3. Spam ve virüslere karşı SMTP gateway olarak Korumail ürünü kullanılmaktadır.
3.1.4.4. İç ve dış bağlantıları karşılayan ve e-posta trafiğini yöneten sunucular birbirleriyle yedekli olarak çalışmaktadır.

3.1.5. Gizlilik ve İfşa etmeme Anlaşmaları Çerçevesi

3.1.5.1. Bilgi gizliliğinin, kurum ile üçüncü taraflar ve yükleniciler arasında sağlanması için gizlilik sözleşmeleri imza altına alınır.

3.1.5.2. Kapsam dahilindeki personelle ilgili gizlilik ve ifşa etmeme şartları Disiplin Süreci ve 4857 sayılı İş Kanunu hükümlerine tabidir.
3.1.5.3. Yükleniciler ve 3.taraf hizmet sağlayıcılar ile imzalanan sözleşmeler, imzalı sözleşmeler ilgili birim tarafından saklanır.

3.1.6. Kayıtlı Elektronik Posta / Elektronik Tebligat Uygulaması

3.1.6.1. Bu tipteki işlemler Elektronik Belge Yönetim Sistemine entegre şekilde yetkilendirilmiş işlem yetkilisi tarafından gerçekleştirilir.

3.1.7. Sayıştay, Emniyet Müdürlüğü Gibi Kuruluşlar ile İlgili Uygulama

3.1.7.1. Bu tip kuruluşlar ile ilgili işlemler yukarıdaki maddelerde bahsedilen kapsamlara göre yürütülecektir.

3.1.8. Web Servisleri Üzerinde Bilgi Transferi

3.1.8.1. Resmi yükümlülük olarak kamu kurumlarına gönderilen verilerde ilgili kurumun şartlarına uyum sağlanır.
3.1.8.2. Kamu kurumları dışındaki kuruluşlara yapılacak Bilgi Transferinde web servisleri SSL üzerinden APIKEY ile güvenlik altına alınır.

4. İLGİLİ DOKÜMANLAR