

MAKÜ

BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ

BİLGİ İŞLEME PROSEDÜRÜ

	BİLGİ İŞLEME PROSEDÜRÜ	Doküman No	PR.10
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 2 / 8

İçindekiler

1	Amaç	3
2	Kapsam	3
3	Sorumluluk.....	3
4	Tanımlamalar ve Kısaltmalar.....	3
5	İşlem Detayı.....	4
5.1	Güvenli Bilgi Transferi	4
5.1.1	Elektronik Ortamda Güvenli Bilgi Transferi.....	4
5.1.2	Fiziksel Ortamda Güvenli Bilgi Transferi.....	5
5.1.3	Sözlü ve Görsel Olarak Güvenli Bilgi Transferi	5
5.2	Güvenli Bilgi Depolama.....	6
5.2.1	Elektronik Ortamda Bilgi Depolama.....	6
5.2.2	Fiziksel Ortamda Bilgi Depolama	7
5.3	Anlık Mesajlaşma Uygulamaları Kullanım Kuralları	7
5.4	Gizlilik ya da ifşa etmeme anlaşmaları	7

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi
KURUMA ÖZEL	

	BİLGİ İŞLEME PROSEDÜRÜ	Doküman No	PR.10
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 3 / 8

1 Amaç

Bu doküman kuruluşa ait transfer edilen ve saklanan bilginin güvenliğini sağlamak amacıyla oluşturulmuştur.

2 Kapsam

Bu doküman, Bilgi Güvenliği Kapsam Analizi dokümanında belirtilen tüm bilgi varlıklarının transferini kapsamaktadır.

3 Sorumluluk

Görev Rol/Unvan	Dokümanın Hazırlanması	Dokümanın Kontrolü	Dokümanın Onaylanması	Dokümanın Yayınlanması	Dokümanın Güncellenmesi	Dokümanın Uygulanması	Dokümanın Uygulamadan Kaldırılması
Üst Yönetim			X			X	X
Üst Yönetim Temsilcisi			X			X	X
BGYS Yöneticisi	X	X		X	X	X	
BGYS Birim Sorumlusu	X	X				X	
Diğer Çalışanlar						X	

4 Tanımlamalar ve Kısaltmalar

Terim	Tanım/Açıklama
Kurum	Kuruluşumuzun Kapsam Analizi Dokümanı'nda belirtilen birimleri
BGYS	Bilgi Güvenliği Yönetim Sistemi
USB	Universal Serial Bus (Evrensel Seri Veriyolu)
CD	Compact Disc (Yoğun Disk)
DVD	Digital Versatile Disc (Çok Amaçlı Sayısal Disk)

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi
KURUMA ÖZEL	

	BİLGİ İŞLEME PROSEDÜRÜ	Doküman No	PR.10
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 4 / 8

5 İşlem Detayı

5.1 Güvenli Bilgi Transferi

Gizlilik dereceli bilgilerin aktarımından önce, bilgiyi talep edenin bu bilgiye erişim yetkisi bulunduğundan emin olunur. Erişim yetkisinin bulunduğu belgelendirme sorumluluğu bilgiyi talep eden taraftadır. Şifahi olarak gizlilik dereceli bilgilerin kurum içinde ve dışında aktarımı söz konusu olamaz.

5.1.1 Elektronik Ortamda Güvenli Bilgi Transferi

- İstemci bilgisayarlar arasında dosya alışverişi söz konusu olduğunda dosyalar şifrlenerek paylaşılır. Şifreli iletilen dosyaların açılması için alıcıya iletilecek bilgiler (parola vb.) iletiye kesinlikle dâhil edilmez, ikinci bir kanaldan (örneğin telefon ile) doğrudan alıcısına iletilir.
- Gizlilik dereceli bilgilerin Kurum içinde veya Kurum dışına elektronik posta olarak aktarılması söz konusu olduğunda, bilgiler e-postanın ekindeki bir dosyada yer alır ve şifrelenir.
- Elektronik postalar yetkisiz erişime değiştirilmeye ve hizmet kesintisine karşı korunur.
- Gizlilik dereceli elektronik bilgilerin taşınabilir depolama ortamları ile (USB bellek vb.) aktarımı söz konusu ise, işlem tamamlanıp gizli bilgiler uygun şekilde bu taşınabilir ortamdan silinmedikçe, bu taşınabilir depolama cihazları başka bir amaç için kullanılamaz ve başka bilgisayarlara bağlanamaz. Gizlilik derecesine göre şifrlenerek saklanır.
- Sistemlere yönetim amaçlı erişimler güvenli protokoller ile yapılır.
- Sistemlere yönetim amaçlı yapılan uzaktan erişimler VPN gibi güvenli metotlar ile yapılır.
- Uygulamalardaki bilginin transferi esnasında aşağıdaki kontrollere uyulur:
 - Şifreleme yöntemi ile güvenlik sağlandığı durumlarda kullanıcıdan bağlantının sonlandığı noktaya kadar sertifika/imza yönetimi süreç boyunca bütünleşik olarak sağlanır.
 - Veritabanı bileşenleri doğrudan internete açılmaz.
 - İletişim için güvenli protokoller kullanılır.
 - Kullanıcı kimlik doğrulaması yapılır.

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi
KURUMA ÖZEL	

	BİLGİ İŞLEME PROSEDÜRÜ	Doküman No	PR.10
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 5 / 8

- e. İletimin/iletişimin güvenilir olduğu doğrulanır.
- f. Uygulamalarda parola yönetimi “Parola Politikası”na uygun olarak yapılandırılır.
- g. Kullanıcılar ile uygulama sunucusu arasında ağ güvenliği kurallarına uygun iletişim sağlanır.

5.1.2 Fiziksel Ortamda Güvenli Bilgi Transferi

- Gönderilen ortam fiziksel ve çevresel değişkenlerden etkilenmeyecek şekilde özenle paketlenir.
- Gönderilen ortamların kayıtlar tutulur.
- Gönderen taraf, aktarılan varlığın alıcının eline geçip geçmediğini kontrol eder. (örneğin telefon ile teyit alınır)
- Bilgi varlığı, zarf içine sığabilecek boyutlarda ise (CD, Kâğıt gibi), zarfa konularak yapıştırılmak suretiyle kapatılır. Gönderen kişi, zarf kapağını imzalayarak kuryeye teslim eder.
- Gizlilik dereceli bilgilerin fiziksel gönderimi sırasında iki ayrı ambalaj kullanılacak, dış ambalajda özel bir işaretleme yapılmayacak, iç ambalaj ise ambalaj içeriğini belli etmeyecek şekilde koruyucu olacak, gönderinin alıcısı dışında kişilerce açılmasını engelleyecek şekilde işaretlenecektir. (ör: gizlilik derecesini belirtir kaşe basılması)
- Bilgi varlığı, disk, bilgisayar gibi zarf içine sığmayacak boyutlarda ise, uygun şekilde paketlenir. Paketler, gönderilen varlığa zarar gelmesini önleyecek nitelikte ve sağlamlıkta olmalıdır. Paketlerin yolda açılmadığından emin olmak için kapak bölümü imzalanır.
- Alıcı taraf, aktarım esnasında gönderilen paketin açılmadığından emin olmalıdır.
- Aktarımların dolaylı yollarla, elden ele teslimat şeklinde değil, bir seferde gönderenden alıcıya ulaşacak şekilde gerçekleşmesi esastır.

5.1.3 Sözlü ve Görsel Olarak Güvenli Bilgi Transferi

- Elektronik ve fiziksel ortamlarda bilginin aktarımı konusunda olduğu gibi, sözlü iletişimde de bilgi güvenliğinin korunması sağlanır.
- Kuruma özel konular hakkında, kamuya açık alanlarda yüksek sesle konuşulmaz.

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi
KURUMA ÖZEL	

	BİLGİ İŞLEME PROSEDÜRÜ	Doküman No	PR.10
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 6 / 8

3. Telefon görüşmelerinde, toplantılarda, vb. sözlü iletişimin sağlandığı ortamlarda karşı tarafın (telefonla görüşülen kişi, toplantı katılımcıları gibi) gizlilik dereceli bilgiye erişim yetkisi yoksa veya erişim yetkisinden emin olunamıyorsa, gizlilik dereceli bilgiler paylaşılmaz.
4. Çalışanlar “sosyal mühendislik” yöntemi konusunda bilgilendirilir ve yetkisiz kişilere bilgi vermez.
5. Kurum’un kamuoyundaki imajını oluşturan, reklam, web sitesi, afiş, tanıtım videosu gibi tanıtım materyallerinde, bir bilgi güvenliği ihlali olup olmadığı (gizlilik dereceli bilgilerin dâhil edilmiş olması, teknik altyapıya ilişkin detaylı bilgilerin bulunması vb.) kontrol edilerek kamuoyuna sunulur.
6. Yapılan toplantılar veya çalışma gruplarında hazırlanan görseller (Kâğıt üzerinde veya yazı tahtasında bulunan topolojiler) saklanır ya da yok edilir.

5.2 Güvenli Bilgi Depolama

Bilginin formu ne olursa olsun, gizlilik dereceli tüm bilgiler için bir saklama süresi belirlenecektir ve süre sonunda bilginin imha edilmesi veya saklanmasına devam edilmesi kararını vermek üzere ilgili birim yöneticisinden görüş istenecektir. Ayrıca, önemli kayıtlar, kaybedilmeye, yok edilmeye ve sahteciliğe karşı yasal, düzenleyici, anlaşmalarla doğan gereksinimler ve iş gereksinimlerine uygun olarak korunur.

5.2.1 Elektronik Ortamda Bilgi Depolama

1. Çalınma ve bilgisayara fiziksel olarak yetkisiz kişilerin erişebilmesi riskine karşı taşınabilir bilgisayarların disklerinde bulunan Gizlilik dereceli bilgiler veya disklerin tamamı şifrelenmelidir.
2. “Gizli” ve “Kuruma Özel” gizlilik dereceli veriler, Kurum tarafından sağlanacak olan merkezi sunucularda depolanmalı ve yetkisiz erişime karşı korunmalıdır.
3. Veri tabanlarında saklanan, işin ve yasaların gereği olarak gizli tutulması gereken bilgiler (ör; audit loglar, kullanıcı şifreleri, gibi) şifrelenerek saklanır.
4. Taşınabilir ortamda bulunan ve artık kullanılmayacak veriler kurtarılamaz şekilde silinir.
5. Taşınabilir ortamın saklanmasında ürün fiziksel ve çevresel değişkenler göz önünde bulundurulur.

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi
KURUMA ÖZEL	

 BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ	BİLGİ İŞLEME PROSEDÜRÜ	Doküman No	PR.10
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 7 / 8

6. Gizli veri taşıyan taşınabilir ortamlarda veriler şifrelenerek saklanır.
7. Taşınabilir ortamda imha edilmesi durumunda içindeki kullanılabilir veriler yedeklenir.

5.2.2 Fiziksel Ortamda Bilgi Depolama

1. Arşivlenmemiş gizlilik dereceli fiziksel bilgi varlıkları ilgili birim tarafından kilitli ortamlarda saklanır.
2. Depolanan varlıkların su baskını, yangın gibi felaketlerden etkilenmemesi; rutubet, toz gibi çürüme ve bozulmalara neden olacak etkilere maruz kalmaması için “Fiziksel Güvenlik Prosedürü” ne uygun olarak fiziksel önlemler alınır.
3. Gizlilik dereceli veya uzun süreli saklama gerektiren bilgilerin saklandığı ortamların kullanım ömrü dikkate alınarak önlem alınır. (Örneğin termal kâğıtlar üzerine basılı belgeler uzun dönemli kullanım için uygun değildir.)
4. Depolama ortamının kendisi (ör. sabit disk) bakım, onarım gibi amaçlarla kurum dışına çıkarıldığı durumlarda bakım, onarım çalışması yapacak firma ile gizlilik sözleşmesi düzenlenmelidir.
5. Yasal olmayan elektronik haberleşme dinleme ve/veya izleme tehdidi oluşturacak unsurların bakım ve onarım sırasında saptanması durumunda ilgili bileşenin kullanımına son verilir. Bu durum kayıt altına alınarak raporlanır ve oluşan tehdidi bertaraf edecek önlemler alınır.
6. Fiziksel Sunucu ve depolama ünitelerinin kalıcı olarak devre dışı bırakılması “Teçhizat Güvenliği Prosedürü” kullanılarak gerçekleştirilir.

5.3 Anlık Mesajlaşma Uygulamaları Kullanım Kuralları

1. Anlık mesajlaşma uygulaması olarak kurumun kullanılmasına izin verdiği ürün kullanılabilir ve gizli bilgiler bu uygulamalar üzerinden paylaşılmaz.

5.4 Gizlilik ya da ifşa etmeme anlaşmaları

Bilgi transferi için alınacak önlemler bu prosedür dışında “Varlıkların Kabul Edilebilir Kullanımı” prosedürüyle, “Kurumsal Kullanıcı Taahhütnamesi”, “3. Taraf Gizlilik Sözleşmesi” ve “3. Taraf Bireysel Kullanıcı Taahhütnamesi” ile de kontrol edilmektedir.

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi
KURUMA ÖZEL	

	BİLGİ İŞLEME PROSEDÜRÜ	Doküman No	PR.10
		Yayın Tarihi	01.04.2022
		Revizyon No	00
		Revizyon Tarihi	-
		Sayfa No	: Sayfa 8 / 8

Revizyon Kayıtları

Rev. No	Tarih	Hazırlayan	Revizyon Nedeni /Sayfa No	Onaylayan	İmza
1					
2					
3					
4					
5					

HAZIRLAYAN	ONAYLAYAN
BGYS Yöneticisi	Üst Yönetim Temsilcisi
KURUMA ÖZEL	