BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ

VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI POLİTİKASI

İçindekiler

1. Amaç

Bu doküman, "BGYS Kapsam Analizi Dokümanı"nda belirtilen personelin ve üçüncü tarafların Kurum varlıklarını kullanırken uyması gereken kuralları tanımlamak amacıyla oluşturulmuştur.

2. Kapsam

Bu doküman, "BGYS Kapsam Analizi Dokümanı"nda belirtilen tüm personeli, geçici görevlendirilmiş personeli ve Kurum'un bilgi varlıklarına erişim izin verilmiş olan diğer kurum/kuruluş/üçüncü taraf çalışanlarını kapsamaktadır.

3. Sorumluluk

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

4. Tanımlamalar ve Kısaltmalar

Terim	Tanım/Açıklama
Kurum	Kuruluşumuzun Kapsam Analizi Dokümanı'nda belirtilen birimleri
BGYS	Bilgi Güvenliği Yönetim Sistemi
Politika	Bir şirket, kurum veya kişinin görüş, felsefe, amaç ve tutumunun belirli şekilde ifadesini, bu görüş, felsefe veya amaç doğrultusunda bir hareket planını içeren doküman tipidir.
GPRS	General Packet Radio Service – Genel Radyo Paket Hizmeti, cep telefonu şebekesi üzerinden veri iletimi ve internet erişimi sağlayan bir teknoloji.

Terim	Tanım/Açıklama
ADSL	Asymmetric Digital Subscriber Line – Asimetrik Sayısal Abone Hattı, internet bağlantısı için kullanılan bir bağlantı tekniğidir.
3/4G	3rd Generation / 4th Generation – 3'üncü Nesil / 4'üncü Nesil, cep telefonu şebekesi üzerinden veri iletimi ve internet erişimi sağlayan bir teknoloji.
Taşınabilir Veri Depolama Cihazları	USB, CD, DVD, SD Card, taşınabilir harici disk vb. üzerinde veri depolanabilen araçlardır.
Mobil Cihaz	Dizüstü bilgisayar, el bilgisayarı, akıllı telefon ve tablet gibi, üzerinde bilgi barındıran taşınabilir tüm cihazlardır.
Varlık	Kurum için değeri olan ve bu nedenle uygun şekilde korunması gereken bilgi ve bilginin üretilmesi, saklanması, transfer edilmesi, korunması vb. amaçlar için kullanılan tüm unsurlardır (internet, e-posta, faks cihazı, yazıcı, tarayıcı, bilgisayar, tablet, cep telefonu ve benzeri mobil cihazlar da dâhil olmak üzere, kurumsal bilgi ve haberleşme sistemleri ve donanımları).

5. Varlıkların Kabul Edilebilir Kullanımı Politikası

Varlıkların kabul edilebilir kullanımı için uyulması gereken kurallar aşağıdaki maddelerde tanımlanmıştır.

5.1. Genel Kurallar

Uyulması gereken kurallar en az aşağıdaki kontrolleri içerir:

(1) Kurumsal varlıklar; kurumsal amaçlar doğrultusunda yapılan çalışmalar için kullanılır. Bu varlıklar yasa dışı, rahatsız edici, Kurum'un diğer prosedür, politika, standart ve rehberlerine aykırı veya Kurum'a zarar verecek herhangi bir şekilde kullanılamaz.
(2) Kullanıcılar, Kurum tarafından kendilerine sağlanmış olan program lisans bilgilerini sadece Kurum faaliyetleri doğrultusunda kullanabilir.
(3) Taşınabilir veri depolama araçlarında gizli ve üzeri gizlilik derecesine sahip bilgi bulundurulamaz. Zorunlu durumlarda uyulması gereken esaslar "Mobil Cihaz Kullanımı Politikası"nda belirtilmiştir.
(4) Kurumsal varlıklarda parola ile girilmesi gereken sistemlerde, parolalar "Parola Politikası"na uygun şekilde tanımlanır ve kullanılır.
(5) Kullanıcılar Kurum kaynaklarına erişim için kullandıkları hesap bilgilerini Kurum yetkili personelleri dahil kimseyle paylaşmamalı, başkalarının ele geçirmesine imkân sağlayacak şekilde açıkça söylememeli, yazmamalı, kaydetmemeli ve elektronik ortamda depolamamalıdır. İlgili kullanıcı hesabı ile yapılan tüm işlemlerin sorumluluğu hesap sahibi olan kullanıcıya aittir.
(6) Kurumsal varlıklara her türlü erişim için "Erişim Kontrol Politikası"na uygun olarak hareket edilir.
(7) Kuruma ait tüm bilgisayarlar, teknik yetersizlikler haricinde etki alanına dâhil edilerek kullanılır.

(8) Bilgisayarlar, teknik gereklilikler haricinde aktif kullanım dışında iken parolalı ekran koruyucular devreye alınacak şekilde ayarlanır.
(9) Bilgisayarlar, mecbur olmadıkça mesai zamanları dışında kapalı tutulur.
(10) Kullanıcılar, sorumlu oldukları Kurumsal varlıkları yetkisiz kişilerle paylaşmaz. Gerekli özenin gösterilmesi ve yetkisiz erişime karşı dikkatli olunması kullanıcı sorumluluğundadır.
(11) Çalışma alanlarında, "Temiz Masa Temiz Ekran Politikası"na uyulur.
(12) Herkese açık bilgiler dışındaki bilgiler internet üzerinde, haber gruplarında, e-posta listelerinde, sosyal medyada ve forumlarda paylaşılmaz.
(13) Gizlilik dereceli bilgiler içeren belgeleri, elektronik ortamları ve bilgi işlem sistemlerini korumak için gerekli fiziksel önlemler "Fiziksel Güvenlik Prosedürü"ne uygun şekilde yerine getirilir.
(14) Gizlilik dereceli bilgilerin ve bilgi içeren ortamların imhasında "Teçhizat Güvenliği Prosedürü"ne uygun şekilde davranılır.
(15) Kurum tarafından açıkça belirtilen durumlar ve yöntemler dışında kurum/kuruluş/üçüncü taraflar ile Kurum bilgileri paylaşılmaz, aktarılmaz ve yayınlanmaz.
(16) Üçüncü taraflar ile gizlilik taahhütnamesi/sözleşmesi imzalanmadan üçüncü taraf çalışanlarının Kurum bilgi işlem sistemlerine, donanımlarına bağlanmasına ve çalışmasına izin verilmez. Erişimler "Erişim Kontrol Politikası"'na uygun olarak yapılır.
(17) Çalışanlar, çalıştıkları ortamlardaki bilgi varlıklarını korumak amacıyla masa ve dolap çekmecelerini kilitli tutmaya özen gösterir ve anahtarları sorumlu kişiler haricinde kimseyle paylaşmaz.
(18) Kurumsal varlıklar, zararlı yazılımlara karşı korunması için "Zararlı Yazılımlardan Korunma Prosedürü"ne uygun şekilde kullanılır.
(19) Kurumsal varlıklar izinsiz olarak kullanım dışı bırakılmaz, izinsiz olarak kalıcı yer değişikliği yapılamaz ve Kurum dışına çıkartılmaz. Mobil cihazların Kurum dışına çıkartılması "Mobil Cihaz Kullanımı Politikası"na göre yapılır.
(20) E-posta programları, ofis uygulamaları, yazılım geliştirme araçları, ağ test araçları gibi uygulamalar kurumsal amaçlı kullanım dışında ya da zorunlu haller dışında sunucu sistemleri üzerine kurulmaz ve kullanılmaz.
(21) Kurum bilgisayarlarından, kurumsal ağ bağlantısı ile aynı anda ADSL, 3G, 4G, GPRS vb. yöntemlerle internete veya başka ağlara bağlanılmaz.
(22) İnternet ve e-posta erişim kuralları için "İnternet Kullanım Politikası" ve "E-Posta Kullanım Politikası"na uygun hareket edilir.
(23) Yazıcıya gönderilen ve daha sonra iptal edilen tüm dokümanlar yazıcı üzerinde kalmaması için mutlaka kontrol edilir.
(24) Kullanılmayan kurumsal varlıklar için "Teçhizat Güvenliği Prosedürü"ne göre işlem yapılır.
(25) Gizlilik dereceli bilgiler işlenirken, saklanırken, iletilirken, imha edilirken "Varlık Yönetimi Prosedürü"ne göre hareket edilir.
(26) Kullanıcılar kurumsal varlıkları aşağıdaki durumlar için kullanamaz:
(a) Kurumsal varlıklara yetkisiz erişmek.
(b) Kurumsal varlıklara zarar vermek.
(c) Diğer kullanıcılara ait varlıklara kasıtlı yetkisiz erişmek ve zarar vermek.

(d) Diğer kullanıcılara ait varlıkları yetkisiz kullanmak.
(e) Kurumsal varlıkları izinsiz veya yetkisiz kopyalamak ve kullanmak.
(f) Bilgisayar iletişim imkânlarını kasten gereksiz olarak kullanmak kaydıyla diğer kullanıcıların bilişim faaliyetlerini engellemek.
(g) Kurum'un çok gizli/gizli/hizmete özel bilgisini ifşa etmek.
(h) Kurum hizmetlerinin ulaşılamaz hale gelmesini sağlamak.
(i) Kurumsal faaliyetler ile ilişkisi olmayan, özel iş veya eğlence amacıyla kullanmak.
(j) Kurumsal varlıklara lisansı kırılmış, lisanssız her türlü yazılımlar ile şifre / parola mekanizmalarını kırmaya yönelik yazılımları indirmek, saklamak, yüklemek ve kullanmak.
(k) Kurumsal varlıklar üzerinde, Kurumun bilgisi ve izni olmadan değişiklik yapmak.
(l) Telif hakları ile korunan müzik, film, elektronik kitap gibi elektronik içerikleri Kurum bilgisayarlarına ve bilgi işlem sistemlerine indirmek, saklamak, çoğaltmak ve paylaşıma açmak.
(m) Yetkili kullanıcılar dışında ağ izlemek, port taraması veya güvenlik taraması yapmak.

5.2. Genel Donanım Kullanım Esasları

(1) Bilgisayar donanımları ile ilgili kullanım esasları Bilgi İşlem Birimi tarafından bu politikada yazıldığı gibi belirlenmiştir.
(2) Kullanıcılar, Bilgi İşlem Birimi'nin bilgisi ve onayı dışında mevcut donanımlara yeni bileşenler ekleyemezler veya mevcut donanımlardan herhangi bir bileşen çıkartamazlar. Bileşene ekleme ve/veya çıkarma gereksinimleri ile ilgili Bilgi İşlem Birimi'ne talepte bulunulur.
(3) Kullanıcılar, kullandıkları bilgisayarların işletim sistemlerinde Bilgi İşlem Birimi bilgisi ve onayı dışında değişiklik yapamazlar.
(4) Kurumsal donanımlar üzerindeki tüm bilgilerin de kurumsal nitelikte olduğu kabul edilir. Kurum, kurumsal donanımları, bu donanımlarla gerçekleştirilen etkinlikleri ve bu donanımlar üzerinde bulunan bilgileri izleme, kaydetme ve dönemsel olarak denetleme hakkını saklı tutar.
(5) Kullanıcılar, donanım güvenliğini tehdit edecek eylemlerden sakınmakla yükümlüdürler. Kullanıcılar bu doğrultuda; kendilerine teslim edilen donanımların üzerindeki ayarları değiştiremezler, anti-virüs yazılımı gibi makine güvenliği ile ilgili ayarlara müdahale edemezler. İlgili programlarda bir sorun gözlemlendiğinde Bilgi İşlem Birimi'ne bildirirler.
(6) Kullanıcılar, kurumsal yazılım deposunda bulunan yazılımlar haricinde bir yazılımı yükleyemez, yüklü ise kaldıramaz veya devre dışı bırakamazlar.
(7) Kullanıcılar, güvenlik riski oluşturabilecek internet sitelerine giremezler.
(8) Kullanıcılar, Kurum ile ilişiklerini kesmeden önce kendilerine zimmetli olan tüm donanımları teslim etmekle yükümlüdürler.
(9) Kullanıcılar, donanım üzerine bir sıvının dökülmesi, donanımın düşürülmesi, yetkisiz donanım eklenmesi/çıkarılması gibi kullanım hataları nedeniyle oluşan donanım arızalarından sorumludurlar.
(10) Kullanıcılar, kullanım hatalarından kaynaklı arızaların ve problemlerin Bilgi İşlem Birimi'ne iletilmesinden ve oluşan maddi zararlardan sorumludurlar.

6. Politika İhlali

Varlıkların Kabul Edilebilir Kullanım Politikasına ve burada belirtilen diğer politika ve prosedürlere uymadığı tespit edildiğinde "Bilgi Güvenliği İhlal Olayı Yönetimi Prosedürü"ne göre işlem yapılır. Gerekli durumlarda Kurum tarafından disiplin süreci işletilir.

7. İlgili Dokümanlar

7.1. İç Kaynaklı Dokümanlar

(1) KA.01 BGYS Kapsam Analizi
(2) PL.04 E-Posta Kullanım Politikası
(3) PL.06 İnternet Kullanım Politikası
(4) PL.07 Erişim Kontrol Politikası
(5) PL.08 Parola Politikası
(6) PL.10 Temiz Masa Temiz Ekran Politikası
(7) PR.02 Varlık Yönetimi Prosedürü
(8) PR.04 Zararlı Yazılımlardan Korunma Prosedürü
(9) PR.11 Fiziksel Güvenlik Prosedürü
(10) PR.12 Teçhizat Güvenliği Prosedürü

7.2. Dış Kaynaklı Dokümanlar

(1) TS ISO/IEC 27001:2013 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler

Revizyon Kayıtları

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