SAKARYA ÜNİVERSİTESİ

"Geleceğinize Yön Verin"

BİLGİ GÜVENLİĞİ PAYDAŞ KILAVUZU

Bu kılavuz, Sakarya Üniversitesi Bilgi Güvenliği Politikalarını destekleyen ve tüm kullanıcılar için geçerli olan temel güvenlik sorumluluklarını özetler.

00.BGYS.KL.01 - 0

İÇİNDEKİLER

1. GİRİŞ 1
2. GENEL KULLANICI SORUMLULUKLARI 2
3. HESAP GÜVENLİĞİ ve PAROLA KULLANIMI 2
4. CİHAZ KULLANIMI, YAZILIM KURULUMU ve GÜNCELLEMELER 3
5. İNTERNET, AĞ ve SİSTEM ERİŞİMİ KULLANIMI 4
6. BİLGİ SINIFLANDIRMA ve BİLGİ YÖNETİMİ 5
7. BİLGİ AKTARIMI ve PAYLAŞIMI (E-posta, USB, Bulut, Sözlü Aktarım) 6
8. ZARARLI YAZILIM, ŞÜPHELİ E-POSTA ve SOSYAL MÜHENDİSLİK 7
9. TEMİZ MASA ve TEMİZ EKRAN KURALLARI 8
10. TAŞINABİLİR BİLGİ DEPOLAMA ORTAMLARI (USB, Harici Disk, SSD vb.) 9
11. KURUMSAL VARLIKLARIN KULLANIMI ve İADESİ 9
12. OLAY BİLDİRİMİ ve GÜVENLİK İHLALLERİ 10
13. TEDARİKÇİ ve ÜÇÜNCÜ TARAF KULLANICILAR 11
14. UZAKTAN ÇALIŞMA ve MOBİL ERİŞİM 12
15. BİLGİ GÜVENLİĞİ DESTEK ve İLETİŞİM 13

1. GİRİŞ

Bilgi Güvenliği Paydaş Kılavuzu, Sakarya Üniversitesi'nin tüm akademik ve idari personeli, öğrencileri, üçüncü taraf çalışanları ve üniversite kaynaklarını kullanan tüm ilgili taraflar için hazırlanmış olup; bilgi varlıklarının ***gizlilik, bütünlük ve erişilebilirliğinin korunmasını*** sağlamak için temel kullanıcı sorumluluklarını açıklar.

Bu Kılavuz, ***Sakarya Üniversitesi Bilgi Güvenliği Politikası, Erişim Kontrol Politikası***, Yedekleme Politikası ve Üniversitenin ***BGYS kapsamındaki tüm prosedürleriyle*** birlikte ele alınmalıdır. Bu politikalarda tanımlanan prensipler, bu Kılavuzda kullanıcı düzeyinde uygulanması beklenen davranışlara yön verir.

Bu kılavuzda belirtilen kurallar, Sakarya Üniversitesi bilgi güvenliğinin ayrılmaz bir parçasıdır; bu politika, prosedür ve kuralların ihlali durumunda uygulanacak disiplin süreçleri, üniversitenin yürürlükteki disiplin mevzuatı çerçevesinde ve ilgili birimler (Hukuk Müşavirliği, Personel Daire Başkanlığı vb.) tarafından yürütülür; ihlaller, söz konusu süreçlere girdi teşkil edecek şekilde değerlendirilerek personel ve öğrenciler için disiplin işlemleri, dış paydaşlar için ise gerekli idari ve hukuki süreçler uygulanır.

Kurum, bilgi güvenliğinin sağlanması amacıyla bilişim sistemleri ve kullanıcı işlemlerini yürürlükteki mevzuata uygun şekilde izleme ve kayıt altına alma hakkını saklı tutar.

2. GENEL KULLANICI SORUMLULUKLARI

Tüm kullanıcıların bilgi güvenliğine ilişkin temel sorumlulukları şunlardır:

- Kurumsal hesaplarını, cihazlarını ve erişim yetkilerini yalnızca görevleri kapsamında ve yetkilendirildikleri ölçüde kullanmak; yetki dışı kullanım, paylaşım veya müdahalelerden kaçınmak
- Üretilen, işlenen ve paylaşılan bilgileri sınıflandırma kurallarına uygun şekilde korumak
- Yetkisiz erişimi, şüpheli hareketleri veya güvenlik ihlallerini gecikmeden bildirmek
- Kendisine zimmetlenen cihazları, medya ve ekipmanları güvenli kullanmak
- Prosedürlerde tanımlanmış teknik süreçlere uygun davranmak

Bilgi güvenliği, tüm kullanıcıların ortak sorumluluğudur. Her kullanıcı kendi hesabı ve işlemleriyle doğrudan sorumludur.

3. HESAP GÜVENLİĞİ ve PAROLA KULLANIMI

Kullanıcılar hesap güvenliğini sağlamak için aşağıdaki davranışlara dikkat etmelidir:

- Parolalar kimseyle paylaşılmaz ve hiçbir yerde açık olarak saklanmaz.
- İşlem yapılmadığında veya bilgisayar gözetimsiz bırakıldığında ekran kilitlenir.
- Parolaların güçlü olması ve belirlenen sürelerde yenilenmesi esastır.
- Kurum tarafından desteklenen sistemlerde çok faktörlü kimlik doğrulama (MFA) kullanılmalıdır.
- Parola üçüncü kişilerce öğrenilmişse derhal bildirilmelidir.

İlgili doküman: Erişim Kontrol Prosedürü

4. CİHAZ KULLANIMI, YAZILIM KURULUMU ve GÜNCELLEMELER

Kurum cihazları ile kullanıcı kişisel cihazlarını güvenli kullanmak için:

- Kullanıcılar yalnızca güvenli ve lisanslı yazılımları yüklemelidir. Bu süreç tamamen kullanıcının sorumluluğundadır.
- Yazılım kurulumlarında yetkisiz içerik kullanımının doğurabileceği risklere karşı dikkatli olunmalıdır.
- Antivirüs, ekran kilidi ve işletim sistemi güncellemeleri düzenli tutulmalıdır.
- Cihazlar halka açık alanlarda gözetimsiz bırakılmamalıdır.
- Kaybolma veya çalınma şüphesi varsa derhal resmi olarak bildirilmelidir.
- Destek yazılımları (AnyDesk, TeamViewer vb.) yalnızca kullanıcının onayıyla ve geçici süreyle kullanılabilir.
- Kullanıcılar, çalışma dosyalarını düzenli aralıklarla güvenli alanlarda yedeklemelidir. Bu işlem, kurumsal teknik yedeklemeden bağımsız olarak kullanıcı yükümlülüğündedir.

İlgili dokümanlar: Ağ ve Sistem Güvenliği Prosedürü, Varlık ve Konfigürasyon Yönetimi Prosedürü

5. İNTERNET, AĞ ve SİSTEM ERİŞİMİ KULLANIMI

Kullanıcılar:

- Kurumsal ağda yasa dışı içerik indirmemeli, torrent ve benzeri araçlar kullanmamalıdır.
- Kurumsal sistemlere yalnızca yetkilendirilmiş yollarla (VPN, kurumsal Wi-Fi vb.) erişmelidir.
- Yetkisiz kablosuz erişim noktası oluşturulmamalıdır.
- Kurumsal ağa bağlanan cihazların güvenlik ayarlarının güncel olması kullanıcı sorumluluğundadır.
- Sunucu odaları, ağ kabinleri ve kritik sistem odalarına yalnızca yetkilendirilmiş personel girebilir. Bu alanlara izinsiz giriş teşebbüsleri veya şüpheli fiziksel erişim durumları derhal ilgili birimlere bildirilmelidir.

İlgili doküman: Ağ ve Sistem Güvenliği Prosedürü

6. BİLGİ SINIFLANDIRMA ve BİLGİ YÖNETİMİ

Üniversitede üretilen tüm bilgi varlıkları sınıflandırma kurallarına göre korunmalıdır.

Kullanıcılar:

- Belgenin sınıflandırmasına uygun olarak erişim paylaşımı yapmalıdır.
- Gizli ve hassas bilgiler yalnızca yetkili kişilerle paylaşılmalıdır.
- Bilgi paylaşımı yaparken doğru kanal (EBYS, kurumsal e-posta, güvenli dosya alanı vb.) tercih edilmelidir.
- Kurumsal e-posta üniversite hizmetleri dışında kullanılmamalıdır.
- Sınıflandırılmış bilgilerin etiketlerini kaldırmamalı veya değiştirmemelidir.

Sınıflandırma kuralları hem fiziksel hem elektronik belgeler için geçerlidir.

İlgili doküman: Varlık ve Konfigürasyon Yönetimi Prosedürü, Kayıtların Kontrolü Prosedürü

7. BİLGİ AKTARIMI ve PAYLAŞIMI (E-posta, USB, Bulut, Sözlü Aktarım)

Bilgi transferi dikkatle yürütülmelidir:

- Hassas bilgiler şifrelenmeden veya uygun kanal seçilmeden aktarılmamalıdır.
- Kişisel veri işleme süreçlerinde KVKK'ya uyulmalıdır.
- USB, harici disk ve benzeri çıkarılabilir ortamlarda sadece görev gereği kullanım yapılmalıdır.
- Kritik sistemlerde taşınabilir medya kullanımı engellenmiş olabilir; kullanıcılar bu sınırlamalara uymalıdır.
- Sözlü bilgi aktarımı yapılacaksa yetkisiz kişilerin duyamayacağı bir ortam seçilmelidir.
- Telesekreterlere veya sesli mesajlara gizli bilgi bırakılmamalıdır.
- Bulut hizmetlerine bilgi yüklerken Sakarya Üniversitesi Bilgi Güvenliği Politikaları dikkate alınmalıdır. Kurum tarafından kullanım şartları tanımlanmamış genel bulut hizmetleri, yalnızca "Halka Açık Bilgi" ve "Birim İçi (Birim Özel)" olarak sınıflandırılmış bilgiler için kullanılabilir; "Kurumsal Gizli" ve "Kurumsal Çok Gizli" seviyesindeki bilgiler bu ortamlarda saklanamaz.

İlgili dokümanlar: Varlık ve Konfigürasyon Yönetimi Prosedürü, Erişim Kontrol Prosedürü, Ağ ve Sistem Güvenliği Prosedürü

8. ZARARLI YAZILIM, ŞÜPHELİ E-POSTA ve SOSYAL MÜHENDİSLİK

Kullanıcıların farkındalık düzeyi bilgi güvenliğinin en kritik bileşenidir. Kullanıcılar, güncel siber tehditler konusunda farkındalık sahibi olmalı, kurum tarafından yapılan bilgilendirme ve eğitimleri takip etmeli ve paylaşılan güvenlik uyarılarını dikkate alarak gerekli önlemleri almalıdır.

- Bilinmeyen göndericilerden gelen, kişinin kendisinden gelmiş gibi görünen (spoofing) veya kimlik avı (phishing) şüphesi taşıyan e-postalar açılmamalı, bağlantı ve ekler tıklanmamalı ve derhal Bilgi Güvenliği Olay Bildirim süreci kapsamında ilgili birimlere iletilmelidir.
- Dosya uzantıları (.exe, .js, makrolu Word/Excel dosyaları vb.) konusunda dikkatli olmalıdır.
- Kurumsal bilgilerle ilgili aciliyet içeren, şüpheli talepler sosyal mühendislik olabilir.

İlgili doküman: Ağ ve Sistem Güvenliği Prosedürü, Bilgi Güvenliği Olay Yönetimi Prosedürü

9. TEMİZ MASA ve TEMİZ EKRAN KURALLARI

Çalışma alanlarının düzeni bilgi güvenliği için önemlidir. Kullanıcılar:

- Masada gizli bilgi içeren evrakları açık bırakmamalıdır.
- Gereksiz çıktılar alınmamalı, alınan çıktı unutulmadan toplanmalıdır.
- Bilgiler kilitli dolap veya yetkisiz erişim riski bulunmayan yerde saklanmalıdır.
- Çalışma alanı terk edilirken bilgisayar ekranı mutlaka kilitlenmelidir.
- Kişisel cihazlarda iş verisi saklanmamalıdır.
- Kimlik bilgisi isteyen formlar, linkler veya QR kodlar şüpheli kabul edilmelidir.
- Şüpheli içerikle karşılaşıldığında derhal bildirim yapılmalıdır.

İlgili doküman: Fiziksel ve Çevresel Güvenlik Prosedürü, Bilgi Güvenliği Olay Yönetimi Prosedürü

10. TAŞINABİLİR BİLGİ DEPOLAMA ORTAMLARI (USB, Harici Disk, SSD vb.)

Kullanıcılar çıkarılabilir medya kullanırken:

- Görev gereği kullanmalı ve hassas veriler mümkünse şifrelemelidir.
- Çevresel tehditlere (ısı, nem, kaybolma, hasar) karşı önlem almalıdır.
- Kullanılmayan veya arızalı medyayı güvenli şekilde bertaraf edilmek üzere ilgili birime teslim etmelidir.
- Bilgi kaybı şüphesi varsa derhal bildirim yapmalıdır.

İlgili doküman: Erişim Kontrol Prosedürü, Varlık ve Konfigürasyon Yönetimi Prosedürü

11. KURUMSAL VARLIKLARIN KULLANIMI ve İADESİ

Kullanıcıya tahsis edilen cihazlar, medya ve ekipmanlar:

- Kişisel amaçlarla kullanılmamalıdır.
- Hasar, kayıp veya arıza durumunda vakit kaybetmeden bildirilmelidir.
- Görev değişikliği veya kurumdan ayrılma durumunda eksiksiz şekilde iade edilmelidir.
- Kişisel cihazlar kurum adına kullanıldığında üzerindeki kurumsal bilgilerin güvenliği kullanıcı sorumluluğundadır.

İlgili doküman: Varlık ve Konfigürasyon Yönetimi Prosedürü

12. OLAY BİLDİRİMİ ve GÜVENLİK İHLALLERİ

Aşağıdaki durumlar bilgi güvenliği olayıdır ve gecikmeden bildirilmelidir:

- Yetkisiz erişim / hesap ihlali
- Kötü amaçlı yazılım (virüs, zararlı yazılım, ransomware vb.)
- Veri kaybı / veri sızıntısı
- Sistem veya hizmet kesintisi
- Şüpheli e-posta / oltalama (phishing)
- Fiziksel güvenlik ihlali
- Cihaz veya medya kaybı (laptop, USB vb.)
- Diğer güvenlik olayları

Bildirim **SABİS > Kalite Yönetim Sistemi > Bilgi Güvenliği İhlali** üzerinden yapılır.

İlgili doküman: Bilgi Güvenliği Olay Yönetimi Prosedürü

13. TEDARİKÇİ ve ÜÇÜNCÜ TARAF KULLANICILAR

Dış paydaşlar:

- Sözleşme ve gizlilik yükümlülüklerine uygun davranmakla yükümlüdür.
- Kuruma ait bilgilere yalnızca yetkilendirildiği ölçüde erişebilir.
- Bakım-onarım, yazılım geliştirme veya hizmet sağlama süreçlerinde bilgi güvenliği kurallarına uymalıdır.
- Üniversite sistemlerine erişim yalnızca kontrol ve kayıt altında sağlanabilir.

Tedarikçi ve Üçüncü Taraflarla Çalışırken Dikkat Edilecek Hususlar:

- Kullanıcılar, tedarikçi veya üçüncü taraflarla bilgi paylaşımı yapmadan önce ilgili birim yöneticisinin onayını almakla yükümlüdür.
- Paylaşılacak bilgiler, yalnızca işin gerektirdiği ölçüde ve bilgi sınıflandırma seviyesine uygun olarak aktarılmalıdır.
- "Kurumsal Gizli" ve "Kurumsal Çok Gizli" seviyesindeki bilgiler, gerekli güvenlik önlemleri alınmadan ve resmi sözleşme/taahhüt bulunmadan üçüncü taraflarla paylaşılmamalıdır.
- Kullanıcılar, tedarikçilerin yalnızca yetkilendirildikleri sistem ve verilere erişmesini sağlamakla yükümlüdür.
- Kurumsal veriler, yetkisiz iletişim araçları (kişisel e-posta, mesajlaşma uygulamaları, izinsiz bulut hizmetleri vb.) üzerinden üçüncü taraflarla paylaşılmamalıdır.
- Tedarikçilerle yürütülen çalışmalar sırasında bilgi güvenliği ihlali şüphesi oluşması durumunda, kullanıcılar durumu derhal Bilgi Güvenliği Olay Bildirim mekanizması üzerinden raporlamakla yükümlüdür.
- Tedarikçi ile iş ilişkisinin sona ermesi durumunda, kullanıcılar erişimlerin kaldırılması, verilerin iadesi veya güvenli şekilde imha edilmesi süreçlerinin tamamlandığından emin olmalıdır.
- Tedarikçi ile yürütülen çalışmalar sırasında kullanılan verilerin güvenliği, paylaşımı ve saklanması süreçlerinde kurum politika ve prosedürlerine uyulmalıdır.

İlgili doküman: Üçüncü Taraf Gizlilik ve Bilgi Güvenliği Taahhütnamesi, Erişim Kontrol Prosedürü, Bilgi Güvenliği Olay Bildirim Prosedürü

14. UZAKTAN ÇALIŞMA ve MOBİL ERİŞİM

Uzaktan erişim gerektiren durumlarda:

- Uzaktan erişim, Erişim Kontrol Politikasında tanımlanan yetkilendirme kuralları doğrultusunda sağlanır.
- VPN dışında kurumsal sisteme erişim kullanılmamalıdır.
- Uzaktan çalışma sırasında kullanılan cihazların güvenliği sağlanmalı, ekran kilidi, parola ve güncel güvenlik yazılımları kullanılmalıdır.
- Hassas bilgiler yalnızca güvenli ortamlarda işlenmeli, ortak ağlar ve yetkisiz erişim riski bulunan ortamlarda işlenmemelidir.
- Kurum dışı ortamlarda bilgi varlıklarının fiziksel güvenliği sağlanmalı ve yetkisiz kişilerin erişimi engellenmelidir.
- Uzaktan çalışma kapsamında kişisel cihaz kullanımı, kurumun belirlediği güvenlik şartlarına tabidir.
- Uzaktan çalışma ortamında, aile bireyleri ve diğer üçüncü kişilerin kurumsal cihazlara ve bilgi varlıklarına erişimi engellenmelidir.
- Ev ağları ve kablosuz bağlantılar güvenli şekilde yapılandırılmalı; mümkün olduğunca güvenilir ve şifreli ağlar kullanılmalıdır.
- Uzaktan çalışma sona erdiğinde, erişim yetkileri gözden geçirilir ve gerekli durumlarda iptal edilir.

İlgili doküman: Ağ ve Sistem Güvenliği Prosedürü

BİLGİ GÜVENLİĞİ DESTEK ve İLETİŞİM

Bilgi güvenliğiyle ilgili her türlü soru, talep veya güvenlik ihlali bildirimi için kullanıcılar Bilgi İşlem Daire Başkanlığı bünyesindeki ilgili birimlere başvurabilir. Gerekli iletişim bilgileri ve bildirim kanalları, Sakarya Üniversitesi Bilgi İşlem web sayfasında güncel olarak yayımlanmaktadır

E-posta	:	bim@sakarya.edu.tr
Telefon	:	0264 295 5101
SABİS Bildirim	:	https://kys.sakarya.edu.tr/tr/Talep/BilgiGuvenligi