1. AMAÇ

Bu politikanın amacı; Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında bilgi varlıklarına, bilgi teknolojileri kaynaklarına, fiziksel alanlara, sistemlere, uygulamalara, ağlara, veri tabanlarına ve diğer bilgi işleme ortamlarına erişimlerin yalnızca yetkili kişi, kullanıcı ve süreçler tarafından, görev ve sorumluluklar doğrultusunda ve ihtiyaç duyulan asgari yetki seviyesinde gerçekleştirilmesini sağlamaktır.

Bu politika ile yetkisiz erişimlerin önlenmesi, erişim yetkilerinin kontrollü olarak verilmesi, değiştirilmesi ve kaldırılması, erişim faaliyetlerinin izlenebilirliğinin sağlanması ve bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğinin korunması amaçlanmaktadır.

2. KAPSAM

Bu politika; Süleyman Demirel Üniversitesi EYS kapsamında;

- Daire Başkanlıkları,
- Genel Sekreterliği,
- Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimini,
- Üniversitenin bilgi işlem altyapısını kullanan diğer ilgili birimleri,
- Üniversite çalışanlarını,
- öğrencileri,
- hizmet alınan tedarikçi ve yüklenicileri,
- danışmanları ve diğer yetkili dış paydaşları, ve bunların Üniversite bilgi varlıklarına, bilgi sistemlerine, ağlara, uygulamalara, veri tabanlarına ve fiziksel alanlara erişimlerini kapsar.

Politika; fiziksel erişim ile mantıksal erişim, kullanıcı hesapları, ağ erişimi, uygulama ve veri tabanı erişimi, internet erişimi, uzaktan erişim ve erişim kayıtlarının yönetimini kapsar.

3. SORUMLULUK

Bu politikanın uygulanmasından tüm ilgili çalışanlar, kullanıcılar ve erişim yetkisi verilen paydaşlar sorumludur.

Erişim yetkilerinin yönetimi ve teknik kontrollerin uygulanmasına ilişkin sorumluluklar görev, yetki ve sorumluluklar doğrultusunda ilgili birimler tarafından yerine getirilir.

Bilgi İşlem Daire Başkanlığı; bilgi sistemleri, ağ, kullanıcı hesapları, teknik erişim kontrolleri, uzaktan erişim, kimlik doğrulama ve erişim kayıtlarının yönetimi kapsamında sorumluluklarını yerine getirir.

Bilgi varlığı veya sistem sahibi olan birimler; kendi sorumluluklarındaki bilgi varlıklarına ilişkin erişim ihtiyaçlarının belirlenmesi, yetkilendirilmesi ve gerektiğinde gözden geçirilmesinden sorumludur.

Kullanıcılar; kendilerine tahsis edilen kullanıcı adı, parola, erişim yetkisi ve diğer kimlik doğrulama bilgilerinin güvenliğini sağlamak ve yalnızca görevleri kapsamında kendilerine verilen yetkileri kullanmakla sorumludur.

Personel süreçlerinden sorumlu birimler ile ilgili yöneticiler; işe başlama, görev değişikliği ve işten ayrılma gibi durumlarda erişim yetkilerinin güncellenmesine yönelik bilgilerin ilgili birimlere zamanında iletilmesini sağlar.

4. UYGULAMA

4.1. Genel Erişim kontrol Prensipleri

Erişim kontrolü; bilgi varlıklarına ve bilgi işleme ortamlarına yalnızca yetkili kişi veya süreçlerin, belirlenmiş kurallar ve yetkiler dahilinde erişebilmesini sağlayan kontroller bütünüdür. Erişim kontrolü fiziksel ve mantıksal erişimleri kapsar.

Erişim kontrollerinde aşağıdaki temel prensipler uygulanır:

- Erişimler görev, sorumluluk ve iş ihtiyacına göre belirlenir.
- Kullanıcılara yalnızca görevlerini yerine getirebilmeleri için gerekli olan asgari erişim yetkisi verilir.
- Yetkiler görev ile ilişkilendirilir ve görev gerektirmediği sürece genişletilmez.
- Kullanıcıların kendilerine ait kullanıcı hesaplarını kullanmaları esastır.
- Kullanıcı hesapları ve erişim yetkileri kişiye özel olarak tanımlanır.
- Kullanıcı adı, parola, çok faktörlü kimlik doğrulama bilgileri ve benzeri kimlik doğrulama unsurları başkalarıyla paylaşılmaz.
- Yetkilendirme işlemleri uygun onay mekanizmaları üzerinden gerçekleştirilir.
- Görev değişikliği, birim değişikliği veya işten ayrılma durumlarında erişim yetkileri gözden geçirilir ve gerekli değişiklikler yapılır.
- Gereksiz, kullanılmayan veya süresi sona ermiş hesaplar kapatılır veya erişimleri kaldırılır.
- Kritik sistemlere ve hassas bilgi varlıklarına erişimler kayıt altına alınır ve gerektiğinde izlenir.
- Erişim kayıtları yalnızca yetkili kişiler tarafından ve görev gereği erişilebilir şekilde korunur.
- Erişim kontrolleri bilgi güvenliği, kişisel verilerin korunması, iş sürekliliği ve kalite yönetimi gereklilikleriyle uyumlu şekilde uygulanır.

4.1.1. En Az Yetki İlkesi

Kullanıcılara yalnızca görevlerini yerine getirmek için ihtiyaç duydukları bilgi, sistem, uygulama ve kaynaklara erişim yetkisi verilir.

Kullanıcının görevini yerine getirmesi için gerekli olmayan erişim, değiştirme, silme, yönetici yetkisi veya benzeri ayrıcalıklar verilmez.

Ayrıcalıklı kullanıcı hesapları yalnızca ihtiyaç halinde ve belirlenmiş yetkilendirme süreçlerine uygun olarak kullanılır.

4.1.2. Görevlerin Ayrılığı

Bilgi güvenliği açısından kritik işlemlerde mümkün olduğu ölçüde görevlerin ayrılığı sağlanır.

Yetkilendirme, uygulama, kontrol, onay ve izleme faaliyetlerinin tek bir kullanıcı üzerinde toplanmasının oluşturabileceği riskler dikkate alınır.

Kritik sistemlerde yönetici yetkilerinin kullanımı kontrol altında tutulur ve gerekli durumlarda kayıt altına alınır.

4.1.3. Kullanıcı Hesaplarının Yönetimi

Kullanıcı hesapları kişiye özel olarak oluşturulur. Kullanıcı hesaplarının oluşturulması, değiştirilmesi, askıya alınması ve kapatılması ilgili erişim talebi ve yetkilendirme süreçleri doğrultusunda gerçekleştirilir.

Ortak kullanıcı hesaplarının kullanılması mümkün olduğunca engellenir. Teknik veya operasyonel zorunluluk nedeniyle ortak hesap kullanılması gerektiğinde ilgili hesaplar sorumlu birim tarafından kontrol altında tutulur ve gerekli kayıtlar oluşturulur.

Kullanıcı hesaplarında görevle ilgisi olmayan veya gereksiz yetkiler tanımlanmaz.

4.1.4. İşe Başlama, Görev Değişikliği ve İşten Ayrılma

Yeni başlayan personel için erişim yetkileri, görev tanımı ve iş ihtiyacı doğrultusunda oluşturulur.

İşe başlama sürecinde, internet sistemine erişim hakkı ve e-posta alt yapısı Bilgi İşlem Daire Başkanlığı tarafından sağlanmaktadır.

Personelin görev veya birim değişikliğinde mevcut erişim yetkileri gözden geçirilir. Yeni görev için gerekli yetkiler tanımlanırken eski görev kapsamında verilen ve artık ihtiyaç duyulmayan yetkiler kaldırılır.

İşten ayrılma veya Üniversite ile ilişiğin sona ermesi durumunda kullanıcı hesapları ve erişim yetkileri ilgili süreç doğrultusunda zamanında sonlandırılır.

Öğrencilerin kaydı yapıldıktan sonra yine Bilgi İşlem Daire Başkanlığı tarafından alt yapısı sağlanır. Öğrencilerin internet ve sisteme girişleri ile ilgili erişim yetkisi Bilgi İşlem Daire Başkanlığı tarafından verilir.

Bilgi İşlem Daire Başkanlığı tarafından ilgili yazılımlar vasıtası ile işten ayrılan personel ve mezun olan / ilişiği kesilen öğrencinin veya personelin hesabı özel kuralların oluşturulduğu bir alana taşınır. Bu özel alanın özelliği kişinin paydaşlarından mail alabilmesine olanak sağlar ancak bu hesap artık mail gönderebilir özelliğini yitirir. Bu işlem "İlişik Kesme Formu " kapsamında yapılır.

4.1.5. Erişim Talepleri ve Yetkilendirme

Erişim talepleri Üniversite tarafından belirlenen elektronik sistemler veya ilgili erişim talep süreçleri üzerinden gerçekleştirilir.

Erişim yetkisi verilmeden önce talebin iş ihtiyacı, görev tanımı ve ilgili bilgi varlığının sahibi tarafından belirlenen yetkilendirme kriterleri dikkate alınır.

Kritik veya ayrıcalıklı erişimlerde ilave onay mekanizmaları uygulanabilir.

Verilen erişim yetkileri gerektiğinde periyodik olarak gözden geçirilir.

4.1.6. Erişim Kontrol Politikasının İlkeleri

- Kullanıcıların internet ve e-posta erişimlerinin sağlanmasından Bilgi İşlem Daire Başkanlığı Ağ ve Sistem Birimi sorumludur. Kuruluş üst yönetimin onayını alarak istediği erişim haklarını kısıtlama yetkisine sahiptir.
- Talepler sistem üzerinden gelmekte ve Bilgi İşlem Daire Başkanlığı tarafından onaylanmaktadır.
- Kullanıcılar SDU 'nün bilgi işlem altyapısını kullanabileceği gibi kendi özel bilgi işlem araçlarını da kullanabilirler. Özel bilgi işlem araçları yine Bilgi İşlem Daire Başkanlığı tarafından hazır hale getirilir ve kampüs ağına gerekli güvenlik ayarları yapılarak dâhil edilir.
- Kullanıcıların erişim yetkisi olmayan yazılım ve sistemlere girmemeleri için gerekli altyapı Bilgi İşlem Daire Başkanlığı tarafından sağlanır.

Erişim ile ilgili kriterler aşağıda verilmiştir.

4.2. Ağ Erişim Kontrolleri

Üniversitenin ağ altyapısına erişim, yetkilendirilmiş kullanıcılar ve yetkili cihazlar üzerinden gerçekleştirilir.

Ağ cihazları, sunucular, güvenlik cihazları ve diğer kritik ağ bileşenlerine yönetim erişimleri yalnızca görev gereği yetkilendirilmiş personel tarafından gerçekleştirilir.

Ağ yönetim cihazlarına erişimde güçlü kimlik doğrulama ve güvenli yönetim protokolleri kullanılır.

Ağ altyapısında;

- Yetkisiz bağlantıların engellenmesi,
- Ağ segmentasyonu,
- Güvenlik duvarı kontrolleri,
- VLAN ve benzeri mantıksal ayrımlar,
- Erişim kontrol listeleri,
- Güvenli uzaktan yönetim,
- Ağ trafiğinin izlenmesi, gibi teknik kontroller riskler doğrultusunda uygulanır.

Sunucu, yazıcı, tarayıcı, güvenlik duvarı, yönlendirici, anahtar ve benzeri kritik ağ bileşenlerinin yapılandırma bilgileri yetkisiz kişilerin erişimine karşı korunur.

Ağ cihazlarında yapılan kritik yapılandırma değişiklikleri kontrollü olarak gerçekleştirilir ve gerektiğinde kayıt altına alınır.

Firmware, işletim sistemi ve ağ cihazlarına ilişkin güncellemeler uygun test ve değişiklik yönetimi süreçleri kapsamında gerçekleştirilir.

4.2.1. Kablosuz Ağ Erişimi

Üniversitenin kablosuz ağ hizmetleri, Üniversite tarafından belirlenen ağlar ve erişim yöntemleri üzerinden sağlanır.

Üniversitemizde kablosuz ağ altyapısında eduroam/SDU_WiFi_Orenci/SDU_WIFI_Personel/ SDUMisafir olarak hizmeti verilmektedir

Kablosuz ağlara erişimde kullanıcıya tahsis edilmiş kimlik doğrulama bilgileri kullanılır.

Kullanıcılar kendilerine tahsis edilen kullanıcı adı ve parola gibi kimlik doğrulama bilgilerini üçüncü kişilerle paylaşamaz.

Üniversite ağını gerekli prosedürleri yerine getirerek misafir kullanıcıları da kullanabilir. SDU Misafir ağına bağlanılır. Ardından açılan web sayfası https://misafirerisim.sdu.edu.tr üzerinden misafir kayıt işlemleri formunun doğru bir şekilde doldurulması gerekir. Cep telefonuna gelen doğrulama kodundan sonra bu kullanıcı kısıtlı bir ağa dâhil olur ve yine diğer kullanıcılar gibi tüm ağ trafiği kayıt altına alınır.

Misafir kullanıcıların Üniversite ağına erişimleri, misafir erişimi için belirlenmiş ayrı ve kontrollü ağlar üzerinden sağlanır.

Misafir kullanıcıların Üniversitenin iç ağ kaynaklarına erişimleri, gerekli olmadığı sürece sınırlandırılır.

4.2.2. Ağ Hizmetlerinin Kullanımı

Üniversite ağ kaynakları eğitim, öğretim, araştırma, idari hizmetler ve Üniversitenin görev alanındaki diğer faaliyetlerin yürütülmesi amacıyla kullanılır.

Ağ kaynaklarının;

- Yetkisiz erişim,
- Ağ güvenliğini tehdit eden faaliyetler,
- Yetkisiz yazılım veya hizmetlerin çalıştırılması,
- Telif ve fikri mülkiyet haklarının ihlali,
- Kurumsal bilgi ve kaynakların yetkisiz paylaşımı,
- Üniversitenin bilgi güvenliğini veya hizmet sürekliliğini olumsuz etkileyen faaliyetler, amacıyla kullanılması yasaktır.

Ağ kaynaklarının şahsi kazanç veya ticari faaliyet amacıyla kullanılması yasaktır.

Ağ üzerinde diğer kullanıcıların bilgi güvenliğini veya mahremiyetini tehdit edecek dinleme, tarama, yetkisiz erişim veya benzeri faaliyetler gerçekleştirilemez.

4.2.3. Ağ Trafiğinin İzlenmesi ve Kayıt Altına Alınması

Bilgi güvenliği, olay yönetimi, hizmet sürekliliği ve yasal yükümlülüklerin yerine getirilmesi amacıyla ağ ve internet erişimlerine ilişkin kayıtlar oluşturulabilir.

Kayıtların oluşturulması, saklanması, erişilmesi ve imhası ilgili mevzuat, Üniversite politikaları ve belirlenen saklama süreleri doğrultusunda gerçekleştirilir.

Kişisel veri içeren erişim kayıtlarına yalnızca yetkili kişiler tarafından, görev gereği erişilir.

4.3. Veri Tabanı ve Uygulama Erişimi

Kritik veri tabanlarına ve uygulamalara erişim kişiye özel kullanıcı hesapları üzerinden gerçekleştirilir.

Veri tabanlarına erişim yetkileri görev ve iş ihtiyacı doğrultusunda belirlenir.

Kritik veri tabanlarında gerçekleştirilen okuma, ekleme, değiştirme ve silme işlemleri risk ve teknik imkânlar doğrultusunda kayıt altına alınır.

Veri tabanı erişim kayıtları yetkisiz erişime karşı korunur.

Veri tabanlarında tutulan bilgiler, bilgi sınıflandırma kuralları doğrultusunda değerlendirilir ve uygun güvenlik kontrolleri uygulanır.

Veri tabanı yedekleri belirlenen yedekleme planına uygun şekilde alınır ve yedeklerin bütünlüğü ile erişilebilirliği korunur.

Yedeklerin geri yüklenebilirliği belirlenen plan ve prosedürler doğrultusunda test edilir.

Veri tabanlarında bakım, onarım, güncelleme, yama ve yapılandırma değişiklikleri kontrollü değişiklik yönetimi kapsamında gerçekleştirilir.

Üretim ortamında gerçekleştirilecek kritik değişikliklerden önce gerekli yedekleme, test ve geri dönüş planlaması yapılır.

Test ve geliştirme ortamlarında gerçek ortamdan alınan kişisel veya hassas verilerin kullanılması gerektiğinde, gerekli güvenlik ve kişisel veri koruma tedbirleri uygulanır.

4.4. İnternet Erişimi

Üniversitenin internet kaynakları; eğitim, öğretim, araştırma, idari faaliyetler ve Üniversitenin görev ve sorumluluklarının yerine getirilmesi amacıyla kullanılır.

İnternet erişimleri kullanıcı hesapları ve teknik erişim kontrolleri üzerinden yönetilir.

Bilgi İşlem Daire Başkanlığı, bilgi güvenliği, hizmet sürekliliği, ağ kapasitesi ve operasyonel gereklilikler doğrultusunda internet erişimlerine yönelik kısıtlama ve filtreleme uygulayabilir.

İnternet erişiminde aşağıdaki kurallara uyulur:

- Yetkisiz dosya paylaşım ve peer-to-peer hizmetleri kullanılmaz.
- Bilgi İşlem Daire Başkanlığı tarafından onaylanmamış yazılımlar Üniversite bilgi sistemlerine kurulmaz.

- Zararlı yazılım içerebilecek güvenilmeyen kaynaklardan dosya ve yazılım indirilmez.
- Üniversiteye ait bilgi, belge ve yazılımlar yetkisiz kişilere veya üçüncü taraflara gönderilmez.
- Üniversiteye ait gizli veya erişimi kısıtlı bilgiler yetkisiz internet ortamlarında paylaşılmaz.
- Telif ve fikri mülkiyet haklarına uyulur.
- Üniversite ağının güvenliğini veya hizmet sürekliliğini olumsuz etkileyebilecek faaliyetlerde bulunulmaz.
- Üniversite kaynakları kullanılarak yetkisiz kripto para madenciliği ve benzeri kaynak tüketen faaliyetler yürütülmez.
- İnternet erişimi, yürürlükteki mevzuata ve Üniversite politikalarına uygun olarak gerçekleştirilir.

4.4.1. İnternet Erişim Kayıtları

İnternet erişimlerine ilişkin kayıtlar, bilgi güvenliği ve yürürlükteki mevzuat kapsamında oluşturulur ve korunur.

Kayıtların saklama süreleri ilgili mevzuat, Üniversitenin kayıt yönetimi ve bilgi güvenliği gereklilikleri doğrultusunda belirlenir.

Erişim kayıtlarına yalnızca yetkili personel tarafından, görev gereği erişilebilir.

Kişisel veri içeren kayıtların işlenmesi ve saklanması KVYS ve ilgili kişisel verilerin korunması mevzuatına uygun şekilde gerçekleştirilir.

4.5. Uzaktan Erişim

Üniversite bilgi sistemlerine uzaktan erişim yalnızca yetkilendirilmiş kullanıcılar tarafından ve Üniversite tarafından belirlenen güvenli erişim yöntemleri kullanılarak gerçekleştirilir.

Uzaktan erişimde güvenli iletişim protokolleri ve gerekli durumlarda çok faktörlü kimlik doğrulama gibi ilave güvenlik kontrolleri uygulanır.

Uzaktan erişim yetkileri görev ve iş ihtiyacına göre verilir ve gerektiğinde periyodik olarak gözden geçirilir.

Uzaktan erişim sağlayan kullanıcılar;

- Kullanıcı adı, parola ve diğer kimlik doğrulama bilgilerini başkalarıyla paylaşamaz.
- Uzaktan erişim yetkisini başka kişilere kullandıramaz.
- Kullandıkları cihazların güncel ve güvenli olmasını sağlar.

- Zararlı yazılım bulaştığından şüphelenilen cihazlarla Üniversite bilgi sistemlerine bağlantı kurmaz.
- Üniversite bilgilerini yetkisiz kişilere aktaramaz.
- Üniversite bilgi sistemlerine yalnızca kendilerine verilen yetki kapsamında erişir.

Uzaktan erişim sırasında Üniversite bilgi sistemlerine aktarılan veri trafiğinin güvenliği uygun teknik kontrollerle sağlanır.

Uzaktan erişimlerde kullanılan cihazların güvenlik durumu gerekli görüldüğünde kontrol edilebilir.

İşten ayrılan, görev veya birim değiştiren kullanıcıların uzaktan erişim yetkileri gözden geçirilir ve gerekli durumlarda kaldırılır.

Tedarikçi ve dış hizmet sağlayıcıların uzaktan erişimleri; sözleşme, yetkilendirme ve bilgi güvenliği gereklilikleri doğrultusunda sınırlandırılır.

Uzaktan erişim yetkisi gerektiğinde belirli zaman aralıkları, belirli sistemler veya belirli kaynaklarla sınırlandırılabilir.

Güvenlik riski veya yetkisiz erişim şüphesi tespit edilmesi halinde uzaktan erişim yetkisi geçici olarak askıya alınabilir veya sonlandırılabilir.

4.6. Ayrıcalıklı Erişim Yönetimi

Sistem yöneticisi, veri tabanı yöneticisi, ağ yöneticisi ve benzeri ayrıcalıklı erişim yetkileri yalnızca görev gereği ihtiyaç duyan yetkili personele verilir.

Ayrıcalıklı hesapların kullanımı mümkün olduğunca kişiye özel olarak gerçekleştirilir.

Ayrıcalıklı hesaplar normal kullanıcı hesaplarından ayrı tutulur.

Ayrıcalıklı erişimlerin kullanımına ilişkin kayıtlar risk ve teknik imkânlar doğrultusunda izlenir ve korunur.

Ayrıcalıklı yetkiler periyodik olarak gözden geçirilir ve ihtiyaç ortadan kalktığında kaldırılır.

4.7. Fiziksel Erişim Kontrolü

Bilgi işlem altyapısı, sunucu odaları, ağ odaları, arşivler ve bilgi güvenliği açısından kritik diğer fiziksel alanlara erişim yalnızca yetkili kişilerle sınırlandırılır.

Kritik alanlara girişlerde kartlı geçiş, anahtar, biyometrik sistem, güvenlik görevlisi veya benzeri fiziksel erişim kontrolleri kullanılabilir.

Ziyaretçilerin kritik alanlara erişimleri yetkili personel eşliğinde ve gerekli güvenlik kuralları çerçevesinde gerçekleştirilir.

Fiziksel erişim kayıtları gerekli görülen alanlarda tutulur ve yetkisiz erişime karşı korunur.

Kritik alanlara erişim yetkileri görev değişikliği ve işten ayrılma durumlarında güncellenir.

4.8. Erişim Haklarının Gözden Geçirilmesi

Kullanıcıların erişim hakları, bilgi varlıklarının kritiklik düzeyi ve riskler dikkate alınarak belirlenen periyotlarda gözden geçirilir.

Gözden geçirme sırasında;

- Kullanıcının mevcut görevi,
- Birimi,
- Yetkinin iş ihtiyacı,
- Erişilen bilgi varlığının sınıflandırması,
- Ayrıcalıklı yetkiler,
- İşten ayrılmış veya görev değiştirmiş kullanıcılar,
- Kullanılmayan veya gereksiz hesaplar, dikkate alınır.

Gereksiz veya artık ihtiyaç duyulmayan erişim yetkileri kaldırılır.

4.9. Kimlik Doğrulama ve Parola Güvenliği

Kullanıcıların bilgi sistemlerine erişiminde Üniversite tarafından belirlenen kimlik doğrulama yöntemleri kullanılır.

Parolalar kişiye özel tutulur ve üçüncü kişilerle paylaşılmaz.

Kritik sistemlerde risk durumuna göre çok faktörlü kimlik doğrulama gibi ek kontroller uygulanabilir.

Kullanıcıların varsayılan parolaları değiştirmesi ve güvenli parola kullanması sağlanır.

Kimlik doğrulama bilgilerinin ele geçirildiğinden şüphelenilmesi durumunda kullanıcı tarafından ilgili birime derhal bildirim yapılır.

4.10. Erişim Kayıtlarının İzlenmesi

Bilgi sistemleri, uygulamalar, veri tabanları, ağ cihazları ve diğer kritik bilgi varlıklarında gerçekleştirilen erişim ve işlemler, risk ve teknik imkânlar doğrultusunda kayıt altına alınır.

Erişim kayıtlarında mümkün olduğu ölçüde kullanıcı, tarih-saat, kaynak, hedef ve gerçekleştirilen işlem gibi bilgiler bulunur.

Kayıtlar yetkisiz değişiklik, silme ve erişime karşı korunur.

Şüpheli veya yetkisiz erişim tespit edilmesi durumunda ilgili olay yönetimi süreçleri uygulanır.

4.11. Kişisel Verilere Erişim

Kişisel verilere erişim yalnızca görev gereği ihtiyaç duyan ve yetkilendirilmiş kişiler tarafından gerçekleştirilir.

Kişisel verilerin bulunduğu sistemlerde erişim yetkileri veri işleme amacı, görev tanımı ve ihtiyaç duyulan erişim seviyesi dikkate alınarak belirlenir.

Özel nitelikli kişisel verilere erişimlerde daha yüksek güvenlik seviyesine sahip teknik ve idari tedbirler uygulanır.

Kişisel veri içeren erişim kayıtları, KVYS kapsamında belirlenen kurallara uygun şekilde korunur.

Kişisel verilere yetkisiz erişim veya erişim şüphesi oluşması halinde ilgili bilgi güvenliği ve kişisel veri ihlali yönetimi süreçleri işletilir.

4.12. Erişim İhlalleri

Yetkisiz erişim, yetki aşımı, hesap paylaşımı, parola paylaşımı, yetkisiz sistem kullanımı veya erişim kontrol mekanizmalarının ihlal edildiğinin tespit edilmesi halinde ilgili olay kayıt altına alınır.

Gerekli durumlarda ilgili kullanıcı hesabı veya erişim yetkisi geçici olarak askıya alınabilir.

Olayın niteliğine göre Olay Yönetimi, Kişisel Veri İhlali Yönetimi, Düzeltici Faaliyet ve ilgili diğer EYS süreçleri uygulanır.

5. YAPTIRIM

Bu politika kapsamında belirlenen erişim kontrol kurallarına aykırı hareket edilmesi durumunda, ilgili olay ve uygunsuzluk Üniversitenin yürürlükteki mevzuatı, ilgili yönetmelikleri, kurum içi düzenlemeleri ve EYS süreçleri kapsamında değerlendirilir.

Yetkisiz erişim, erişim yetkisinin amacı dışında kullanılması, kullanıcı hesabı veya kimlik doğrulama bilgilerinin paylaşılması, yetkisiz kişilere erişim sağlanması, erişim kontrol

mekanizmalarının devre dışı bırakılması veya Üniversite bilgi varlıklarının yetkisiz kullanımının tespit edilmesi halinde;

- İlgili erişim yetkisi geçici olarak askıya alınabilir veya kaldırılabilir.
- Gerekli durumlarda kullanıcı hesabı kapatılabilir.
- Bilgi güvenliği olayı veya kişisel veri ihlali süreçleri başlatılabilir.
- İlgili uygunsuzluk için Düzeltici Faaliyet süreci işletilebilir.
- Fiilin niteliğine göre ilgili mevzuat ve Üniversitenin yürürlükteki disiplin hükümleri uygulanabilir.
- Gerekli görülmesi halinde hukuki ve idari süreçler başlatılabilir.

Uygulanacak yaptırım, olayın niteliği, etkisi, tekrarlanma durumu ve yürürlükteki mevzuat ile Üniversite düzenlemeleri dikkate alınarak belirlenir.