1. AMAÇ

Bu politikanın amacı; Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında kullanılan bilgi sistemleri, ağ bileşenleri, yazılımlar, sunucular, güvenlik cihazları, uygulamalar ve bunlara bağlı hizmetlerde gerçekleştirilecek değişikliklerin kontrollü, planlı ve güvenli bir şekilde yönetilmesine ilişkin esasları belirlemektir.

Bu politika ile değişikliklerin bilgi güvenliği, hizmet sürekliliği, veri bütünlüğü ve sistemlerin kullanılabilirliği üzerindeki olası etkilerinin değerlendirilmesi, gerekli onayların alınması, test edilmesi, uygulanması ve kayıt altına alınması amaçlanmaktadır.

2. KAPSAM

Bu politika; Süleyman Demirel Üniversitesi Daire Başkanlıkları, Genel Sekreterlik ve Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi kapsamında kullanılan veya yönetilen;

- Bilgi sistemlerini,
- Sunucu ve istemci sistemlerini,
- Ağ ve güvenlik cihazlarını,
- İşletim sistemlerini,
- Kurumsal uygulamaları,
- Veritabanlarını,
- Sistem ve uygulama konfigürasyonlarını,
- Bilgi sistemleri ile ilişkili hizmet ve servisleri etkileyebilecek değişiklikleri ve bu değişiklikleri gerçekleştiren personel ile yetkilendirilmiş üçüncü tarafları kapsar.

3. SORUMLULUK

3.1. Bilgi İşlem Daire Başkanlığı

- Değişiklik yönetimi sürecinin uygulanmasını sağlamak,
- Değişiklik taleplerinin değerlendirilmesini ve kayıt altına alınmasını sağlamak,
- Değişikliklerin bilgi güvenliği ve hizmet sürekliliği üzerindeki etkilerinin değerlendirilmesini sağlamak,
- Gerekli onayların alınmasını sağlamak,
- Değişikliklerin kontrollü şekilde uygulanmasını ve sonuçlarının kayıt altına alınmasını sağlamak.

3.2. Değişikliği Gerçekleştiren Personel

- Değişiklik talebini ve yapılacak işlemleri kayıt altına almak,
- Değişiklik öncesinde gerekli kontrolleri ve hazırlıkları yapmak,
- Onaylanan değişikliği belirlenen kapsam ve yöntem doğrultusunda gerçekleştirmek,
- Değişiklik sonrasında gerekli kontrolleri yapmak,

- Başarısız değişikliklerde geri dönüş planını uygulamak ve durumu ilgili sorumlulara bildirmek.

3.3. Yetkili Yönetici / Değişiklik Onaylayıcısı

- Değişiklik talebini değerlendirmek,
- Değişikliğin gerekliliği, kapsamı ve olası etkilerini göz önünde bulundurarak onay veya ret kararı vermek,
- Kritik değişikliklerde gerekli ilave kontrollerin uygulanmasını sağlamak.

4. UYGULAMA

4.1. Değişiklik Talebinin Oluşturulması

Bilgi sistemleri, ağ bileşenleri, yazılımlar, işletim sistemleri, uygulamalar, veritabanları, konfigürasyonlar ve hizmetlerde gerçekleştirilecek değişiklikler mümkün olduğunca değişiklik yönetimi süreci üzerinden kayıt altına alınır.

Değişiklik kaydında, değişikliğin;

- Amacı ve gerekçesi,
- Etkilenecek sistem veya varlıklar,
- Değişikliğin kapsamı,
- Planlanan uygulama zamanı,
- Sorumlu personel,
- Olası risk ve etkileri,
- Test yöntemi,
- Geri dönüş yöntemi belirtilir.

4.2. Değişikliğin Değerlendirilmesi ve Onaylanması

Gerçek ortamdaki kritik sistemleri etkileyebilecek değişiklikler uygulanmadan önce değerlendirilir ve yetkili kişi tarafından onaylanır.

Değişikliğin onaylanmasından önce;

- Bilgi güvenliği üzerindeki etkisi,
- Hizmet sürekliliği üzerindeki etkisi,
- Veri bütünlüğü ve erişilebilirlik üzerindeki etkisi,
- Diğer sistem ve hizmetlere olası etkileri,
- Oluşabilecek riskler değerlendirilir.

Gerekli görülmesi halinde değişiklik öncesinde risk değerlendirmesi gerçekleştirilir.

Acil durumlarda yapılması gereken değişiklikler, hizmetin veya bilgi güvenliğinin korunması amacıyla ilgili acil değişiklik süreci kapsamında gerçekleştirilebilir. Acil değişiklikler sonrasında yapılan işlem ve alınan kararlar kayıt altına alınır.

4.3. Değişiklik Öncesi Hazırlık

Değişiklik uygulanmadan önce;

- Gerekli yedeklerin alınması,
- Mevcut sistem veya konfigürasyon bilgilerinin kayıt altına alınması,
- Değişiklikten etkilenebilecek hizmetlerin belirlenmesi,
- Geri dönüş yönteminin belirlenmesi,
- Gerekli personel ve teknik kaynakların hazır bulundurulması sağlanır.

4.4. Test ve Doğrulama

Değişikliklerin mümkün olduğu ölçüde test ortamında veya kontrollü bir ortamda test edilmesi sağlanır.

Test sonuçları kayıt altına alınır.

Kritik sistemleri etkileyen değişiklikler, gerekli testler başarıyla tamamlanmadan gerçek ortama uygulanmaz.

Değişiklik sonrasında ilgili sistem, uygulama ve hizmetlerin beklenen şekilde çalıştığı doğrulanır.

4.5. Değişikliğin Uygulanması

Onaylanan değişiklik, belirlenen kapsam ve plan doğrultusunda yetkili personel tarafından uygulanır.

Uygulama sırasında yapılan işlemler ve karşılaşılan önemli durumlar değişiklik kaydına işlenir.

Değişiklik sırasında beklenmeyen bir durum oluşması ve hizmet güvenliğinin veya sürekliliğinin olumsuz etkilenmesi halinde gerekli görülürse değişiklik durdurulur ve önceden belirlenen geri dönüş yöntemi uygulanır.

4.6. Geri Dönüş

Başarısız olan veya bilgi güvenliği, veri bütünlüğü ya da hizmet sürekliliği açısından kabul edilemeyecek sonuçlara yol açan değişikliklerde, değişiklik öncesinde belirlenen geri dönüş yöntemi uygulanır.

Geri dönüş işlemi ve sonucu kayıt altına alınır.

Gerekli durumlarda değişiklik yeniden değerlendirilerek yeni bir değişiklik talebi oluşturulur.

4.7. Değişiklik Sonrası Kontrol

Değişiklik tamamlandıktan sonra;

- Sistemlerin çalışırlığı,
- Uygulamaların işlevselliği,
- Ağ bağlantıları,
- Güvenlik kontrolleri,
- İlgili servisler,
- Veri bütünlüğü kontrol edilir.

Kontrol sonuçları değişiklik kaydına işlenir ve değişikliğin başarıyla tamamlandığı doğrulanır.

4.8. İşletim Sistemi ve Güvenlik Güncellemeleri

İşletim sistemi, uygulama ve güvenlik güncellemeleri değişiklik yönetimi sürecinde değerlendirilir.

Güncellemelerin uygulanmasında sistemin kritiklik seviyesi, güvenlik riski, hizmet sürekliliği ve üretici tarafından yayımlanan güvenlik duyuruları dikkate alınır.

Kritik güvenlik güncellemeleri ve güvenlik açıklarına yönelik yamalar, ilgili riskin seviyesine ve hizmet sürekliliği gereksinimlerine göre önceliklendirilir.

Güvenlik açığı ve yama yönetimine ilişkin ayrıntılı uygulamalar Zaafiyet ve Yama Yönetimi Politikası kapsamında yürütülür.

Güncelleme sonrasında ilgili sistem ve servislerin çalışırlığı kontrol edilir ve sonuçlar kayıt altına alınır.

4.9. Konfigürasyon Değişiklikleri

Sistem, ağ ve güvenlik cihazlarının varsayılan veya mevcut konfigürasyonlarında yapılan değişiklikler kayıt altına alınır.

Kritik konfigürasyon değişikliklerinde değişiklik öncesindeki mevcut yapılandırmanın yedeği veya geri dönüş için gerekli bilgiler korunur.

Yetkisiz konfigürasyon değişikliklerine izin verilmez.

4.10. Üçüncü Taraflar Tarafından Gerçekleştirilen Değişiklikler

Üçüncü taraf hizmet sağlayıcılar tarafından Üniversite bilgi sistemlerinde gerçekleştirilecek değişiklikler, yetkilendirme ve değişiklik yönetimi kurallarına uygun olarak yürütülür. Üçüncü tarafların gerçekleştirdiği değişikliklerin kapsamı, zamanı ve sonuçları kayıt altına alınır.

Gerekli durumlarda üçüncü tarafların erişimleri değişiklik tamamlandıktan sonra kaldırılır veya yetkileri gözden geçirilir.

4.11. Değişiklik Kayıtlarının Saklanması

Gerçekleştirilen değişikliklere ilişkin talep, onay, risk değerlendirmesi, test sonucu, uygulama sonucu ve geri dönüş kayıtları EYS doküman ve kayıt yönetimi kurallarına uygun şekilde saklanır.

5. YAPTIRIM

Bu politikaya aykırı gerçekleştirilen yetkisiz veya kontrolsüz değişiklikler EYS kapsamında uygunsuzluk olarak değerlendirilir. Çalışanların politika hükümlerine aykırı hareket etmesi halinde ilgili mevzuat, Üniversite düzenlemeleri ve Disiplin Prosedürü hükümleri uygulanır.