1. AMAÇ

Bu doküman, bursa uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesindeki bilgi varlıklarının etkili bir şekilde yönetilmesini, yapılacak konfigürasyon değişikliklerinin standartlaştırılmış yöntemlerle etkin bir şekilde
gerçekleştirilmesini, yapılan konfigürasyon değişikliği işlemlerinin kayıt altına alınmasını, konfigürasyonlar üzerinde yapılabilecek olası insan hatalarının doğuracağı risklerin önceden öngörülerek azaltılmasını, başarısızlık durumunda önceki kararlı konfigürasyona geri dönülebilmesi için gerekli planların yapılarak zararların azaltılmasını sağlamak amacıyla konfigürasyon yönetimi süreçlerini tanımlar ve yönlendirir.

Ayrıca, ISO 27001 Ek-A gereksinimlerine uygunluk sağlar.

2. KAPSAM

Bu prosedür, bilgi sistemlerine yönelik her türlü konfigürasyon değişikliği faaliyetini kapsamaktadır.

3. TANIMLAR VE KISALTMALAR

3.1. TANIMLAR

Bilgi Güvenliği: Kurumdaki bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik özelliklerinin korunmasıdır.
Güvenlik Konfigürasyonları: Bilgi Sistemlerinde güvenliği sağlamak, artırmak, teknik açıklıkları önlemek adına yapılan her türlü yapılandırma faaliyeti
CMDB (Central Management Database): Merkezi Yönetim Veri Tabanı. Bilgi Sistemlerine ait IP adresi, donanım adresi, işletim sistemi versiyonu, konfigürasyon versiyonu ve konfigürasyon yedeklerinin tutulduğu merkezi veri tabanı sistemi.
Değişiklik İsteği: Bir değişikliğin yapılması için sunulan resmi öneridir. Bir değişiklik isteği değişikliğe ilişkin tüm detayları içerir.
Değişiklik: Bilgi sistemlerini etkileyen herhangi bir şey değiştirme, ekleme veya ortadan kaldırma işlemleridir.
İdare (Kurum): Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı
JIRA: Holding bünyesinde değişiklik yönetimi sürecinin işletildiği sistemdir.

3.2. KISALTMALAR

CAB: Change Advisory Board – Değişiklik Danışma Kurulu

4. SORUMLULUKLAR

4.1. BİLGİ GÜVENLİĞİ EKİBİ

Bilgi Güvenliği Ekibi, konfigürasyon yönetimi politika ve prosedürlerinin oluşturulması, uygulanması ve sürdürülmesinden sorumludur. Konfigürasyon yönetimi ile ilgili riskleri tanımlar ve bu risklere karşı uygun kontrolleri belirler.

4.2. TEKNOLOJİ VE AR-GE EKİPLERİ

BT Yönetimi, konfigürasyon yönetimi süreçlerini uygular ve günlük işleyişini sağlar. Konfigürasyonları belirler, izler ve dokümante eder.

4.3. TÜM ÇALIŞANLAR

Tüm çalışanlar, konfigürasyon yönetimi politikalarına ve prosedürlere uyar ve bu konuda iş birliği yapar

5. UYGULAMA

5.1. KONFİGÜRASYON TANIMLAMA

a. Tüm bilgi varlıkları ve bunların konfigürasyonları belirlenir ve CMDB'de benzersiz bir şekilde tanımlanır.
b. Bilgi varlıklarının önem dereceleri saptanır ve bunlara göre sınıflandırılır.
c. Konfigürasyonlar, belirlenen güvenlik politikalarına ve gereksinimlerine uygunluğu sağlayacak şekilde güncel tutulur.

5.2. KONFİGÜRASYON YETKİLERİ

a. Konfigürasyon Değişiklik Yetkileri için Aktif Dizindeki Yetki Grupları kullanılır
b. Değişiklik Yetkileri sadece ilgili varlığın kendisine zimmetlendiği departmandaki uzman ve üzeri pozisyonundaki kişisel için verilir
c. Değişiklik yetkileri yetkili hesaplara; isimleri adreslenecek şekilde verilir

5.3. KONFİGÜRASYON DEĞİŞİKLİK TALEPLERİ VE TEST SÜREÇLERİ

a. Tüm değişiklikler için bir değişiklik kontrol süreci uygulanır.
b. Tüm Konfigürasyon Değişiklik Talepleri için, Değişiklik Yönetimi Prosedürü referans alınır
c. Konfigürasyon Değişiklikleri eğer yedek ortam mevcutsa önce yedek ortamda test edilir

5.4. ÖNCEKİ KONFİGÜRASYON YEDEKLERİNİN ALINMASI

a. Yedekleme Prosedüründe detayları belirtilen rutin yedekler dışında her konfigürasyon değişikliği öncesi son yedek alınır
b. Değişiklik öncesi alınan son Yedekler değişiklik süreci başarılı şekilde tamamlanıncaya kadar güvenli ortamda muhafaza edilir
c. Değişiklik süreci başarı ile tamamlanan yedekler güvenli ortamdan silinir

5.5. YENİ KONFİGÜRASYONLARIN CANLIYA ALINMASI VE İZLENMESİ

a. Yeni konfigürasyonlar oluşturulurken üretici kılavuzları, best practise guideline ları, güvenlik otoritelerinin önerileri referans alınır
b. Canlıya alım sürecinde Değişiklik Yönetimi Prosedürü referans alınır
c. Yeni konfigürasyonlar Merkezi Sunucu, Ağ ve Servis İzleme Yazılımı tarafından sürekli izlenir
d. İzleme sonuçları, herhangi bir güvenlik ihlali veya kaybı engellemek için gerekli düzeltici faaliyetlerin başlatılmasına yol açarsa, bu düzeltici faaliyetler hızla uygulanır

5.6. KONFİGÜRASYON DOKÜMANTASYONU

a. Tüm konfigürasyon değişiklik talepleri ve alınan aksiyon bilgileri ITSM Yazılımı üzerinde kaydedilir.

b. Yapılan konfigürasyon değişiklikleri Merkezi Sunucu, Ağ ve Servis İzleme Yazılımı tarafında kayıt altına alınır.

5.7. UYUMLULUK

Bu Prosedürün ihlali durumunda, Bilgi Güvenliği Taahhütnamesi ve Disiplin Prosedüründe belirtilen

hususlar ve ilgili maddeleri esas alınarak işlem yapılır.

6. KAYITLAR

Bu doküman ile ilgili kayıtlar QDMS doküman yönetim uygulaması içerisinde elektronik olarak tanımlanmıştır. Kayıt listesi için QDMS doküman yönetim uygulamasını kullanınız.

Kayıt Saklama Sorumlusu (İlgili Birim) Saklama Süresi Kayıt Yeri

7. İLİŞKİDE OLDUĞU DÂHİLİ DOKÜMANLAR (SÜREÇLER, PROSEDÜR, TALİMAT, FORM, VB)

Bu doküman ile ilgili ilişkili dokümanlar QDMS doküman yönetim uygulaması içerisinde elektronik olarak tanımlanmıştır. Doküman listesi için QDMS doküman yönetim uygulamasını kullanınız.

Doküman Adı Doküman No:

Bilgi Teknolojileri Güvenlik Prosedürü GN-0704-PR-11

Bilgi Teknolojileri Değişiklik Yönetimi Prosedürü GN-0704-PR-15

Varlık Envanteri

Bilgi Teknolojileri Erişim Kontrol Prosedürü GN-0704-PR-16

8. REFERANSLAR VE EKLER (DIŞ KAYNAKLI DOKÜMANLAR)

Doküman Adı Doküman No:

ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı

9. REVİZYON TAKİP ÇİZELGESİ

Revizyon No Revizyon Tarihi Revizyon Nedeni

0 18.10.2023 İlk Yayın