1. Amaç

Bu doküman, Kütüphane ve Dokümantasyon Daire Başkanlığı'nın bilgi varlıklarına erişimi güvenli hale getirmek için uyulması gerekli hususları belirlemek amacıyla oluşturulmuştur.

2. Kapsam

SDÜ0PL06 BGYS Erişim Güvenliği Politikası, SDÜ6GE01 BGYS Kapsamı dokümanında belirtilen tüm fiziksel varlıkları kapsar.

3. Tanımlar

Kurum: Kütüphane ve Dokümantasyon Daire Başkanlığı

BGYS: Bilgi Güvenliği Yönetim Sistemi

4. Uygulama

4.1 Temel Prensipler

Bilgi varlıklarına erişim yetkileri "Açıkça izin verilmedikçe her şey yasaklanır" prensibine göre verilir.

Veri türündeki bilgi varlıklarına erişim yetkileri, "Bilmesi gerektiği kadar" prensibine göre verilir.

Donanım, yazılım, hizmet ve tesis türündeki bilgi varlıklarına erişim yetkileri, "Kullanması gerekli" prensibine göre verilir.

Bilgi varlıklarına erişimde, iş rolleri ile erişim yetkilerini bağlamak için rol tabanlı erişim kontrolü uygulanır.

Kullanıcılara, yalnızca kullanımları için yetkilendirildikleri ağ ve ağ hizmetlerine erişim yetkisi verilir.

Bilgi varlıklarına erişimde kimlik doğrulama (Authentication), yetkilendirme (Authorization) ve aktivitelerin izlenmesi (Auditing) işlevleri uygulanır.

Sistemlerde ve uygulamalarda varsayılan gizli kimlik bilgileri kullanılamaz

4.2 Ağ Erişimi

Kullanıcılar, sistemler ve ağ cihazları ayrı mantıksal ağ bölümlerinde (VLAN) konumlandırılmıştır.

Ağ bölümlerine erişimde "Açıkça izin verilmedikçe her şey yasaklanır" prensibi uygulanır.

Kuruluş ağına ve ağ hizmetlerine yalnızca kuruluş çalışanları, izin verilen cihazlarla erişebilir. Hizmet sağlayıcıların kuruluşa ait ağ ve ağ hizmetlerine erişimi, kuruluş ait cihazlar aracılığıyla kontrollü şekilde sağlanır.

Misafirlere yalnızca, misafir ağı aracılığıyla internete erişim yetkisi verilir.

4.3 Kullanıcı Erişimi

Tüm kullanıcılar, bilgi varlıklarına kendilerine ait gizli kimlik bilgileri ile erişebilirler.

Kullanıcı hesabının açılması kapatılması ve görev değişikliklerinde güncellenmesi, Bilgi İşlem Daire Başkanı'nın onayına tabidir.

Birden fazla kullanıcının ortak hesap kullanımı, yalnızca gerekli olan durumlarda ve BGYS Komisyonu'nun onayı ile mümkündür.

İş sözleşmesi sona eren kullanıcı ve hizmet sağlayıcıların hesapları ile fiziksel erişim yetkileri, sözleşmenin bittiği tarih itibarıyla kapatılır. Bilgi İşlem Daire Başkanı, gerekli gördüğü durumlarda hesap kapatma tarihini öne çekebilir. Kapatma tarihinin uzatılması, BGYS Komisyonu'nun yazılı onayına tabidir.

Sistemlere ve uygulamalara erişim için kullanılan tüm hesaplar, 6 ayda bir kontrol edilerek belirli süreyle erişim kaydı olmayan hesaplar kapatılır.

Bilgi varlıklarına erişim yetkileri, en çok 6 ayda bir, varlık sahipleri tarafından kontrol edilir.

Görev değişikliği, hizmet sözleşmesinin sonlandırılması ya da terfi gibi değişikliklerden sonra erişim yetkileri kontrol edilir.

Sistemlere ve uygulamalara ilişkin ayrıcalıklı erişim yetkilerinin kaydı tutulur.

Geçici gizli kimlik bilgileri, kullanıcılara açık olmayan, güvenli yollarla iletilir.

Parolalar, kaba kuvvet saldırılarından savunmak amacıyla, en az 8 karakterden oluşur.

4.4 Ayrıcalıklı Erişim

Ayrıcalıklı erişim yetkileri, yalnızca işin gerektirdiği kadar verilir.

Sistemlere ve uygulamalara, teknik açıdan mümkün olduğu durumlarda, ayrıcalıklı erişim yetkisi verilmiş kullanıcı hesaplarıyla girilir, -administrator, root, SA gibi- genel adlı ayrıcalıklı hesaplar kullanılmaz.

Teknik zorunluluk nedeniyle, genel adlı ayrıcalıklı hesap kullanımı durumunda, BGYS Komisyonu, her bir hesap kullanım girişimine ilişkin gerekçe ile bilgilendirilir.

Ayrıcalıklı erişim yetkileri, en çok 6 ayda bir, BGYS Komisyonu Başkanı tarafından BİDB Müdürü'ne raporlanır.

Ayrıcalıklı hesaplara ilişkin parolalar 1Password sisteminde saklanır ve 6 ayda bir değiştirilir.

Ayrıcalıklı erişim yetkilerine sahip bir kullanıcının işten ayrılması ya da görev değişikliği durumunda, ilgili sistemlere ilişkin parolalar hemen değiştirilir.

Kullanıcı cihazlarına, onay almaksızın, ayrıcalıklı destek programları kullanılarak erişilemez. Bilgi ihlal olayı şüphesiyle izleme yapılması durumunda, önceden BGYS Komisyonu'nun onayı alınır.

Ayrıcalıklı destek programlarının kullanım kayıtları en az 1 yıl süreyle tutulur

4.5 Sistem ve Uygulama Erişimi

Kullanıcılar, sistemlerde yalnızca iş tanımlarına uygun menü ve fonksiyonlara eriştirilir.

Kritik sistem ve uygulamalarda, yetkiler veri yazma, silme ve değiştirme gibi detayda kontrol edilir.

Oturum açma esnasında kullanıcılara ait gizli kimlik bilgileri görüntülenmez.

Oturum açma esnasında, güvenlik süreçlerini atlatacak şekilde yardım mesajları görüntülenmez.

Parolalar, 6 ayda bir değiştirilir. Kullanıcıların, bir önceki parolalarını seçmesini engelleyecek teknik kontroller gerçekleştirilir.

Parolalar, kolayca tahmin edilme ve kaba kuvvet saldırısı tehdidine karşı, en az 8 karmaşık karakterli olarak seçilir.

Parolalar, sözlük saldırılarından korunmak amacıyla, bilinen sözcüklerden oluşamaz.

Başarılı ve başarısız girişimlere ilişkin kayıtlar tutulur.

Parolalar ağ üzerinden açık metin olarak iletilmez.

Sistem ve uygulamalarda, tanımlanan süreyle işlem yapılmadığı durumda oturum sonlandırılır.

Uygulamaların kaynak kodu ve ilgili öğelere erişim, istenmeyen değişiklikler, yetkisiz işlevsellik ve fikri mülkiyet haklarının istismarı tehditlerine karşı engellenir.

Uygulamaların kaynak kodu, canlı sistemler üzerinde tutulmaz.

4.6 Kullanıcı Sorumluluğu

Kullanıcılar, kendilerine ve sistemlere ilişkin gizli kimlik bilgilerini korumaktan sorumludur.

Kullanıcıların gizli kimlik bilgileri, hiçbir koşulda paylaşamaz. Paylaşıldığı durumda, hukuki sorumluluk kullanıcıya aittir.

Kullanıcılar, geçici kimlik bilgilerini aldıklarını bildirmekten ve en kısa zamanda değiştirmekten sorumludur.

Parolalar, kolayca tahmin edilme tehdidine karşı, doğum tarihi, isim, telefon numarası gibi bilgileri içermez, tekrarlı rakamlardan oluşmaz.

Parolalar, sözlük saldırılarından korunmak amacıyla, bilinen sözcüklerden oluşmaz.

Kurumsal sistemlerde kullanılan gizli kimlik bilgileri, kişisel sistemlerde kullanılmaz.