1. AMAÇ:
Erzurum Teknik Üniversitesi Bilgi İşlem Dairesi Başkanlığı'nın kritik kurumsal bilgilerinin korunması amacıyla sistem odalarına, kurumsal bilgilerin bulundurulduğu sistemlerin yer aldığı tüm hassas çalışma alanlarına yetkisiz girişlerin yapılmasını önlemektir.

2. KAPSAM:
Bilgi İşlem Daire Başkanlığı bünyesinde yer alan bilgi varlıklarına erişim sağlayan sistemlerin ve kurumsal bilgilerin bulundurulduğu hassas alanların güvenliğini kapsar.

3. TANIMLAR:
SSL (Secure Socket Layer): Kişisel gizlilik ve güvenilirlik sağlayan, network üzerindeki bilgi transferi sırasında bilginin bütünlüğü ve gizliliği için sunucu ile istemci arasındaki iletişimin şifrelenmiş şekilde yapılabilmesine imkan veren bu sayede gizliliğinin ve bütünlüğünün korunmasını sağlayan bir güvenlik protokolüdür.

Güvenli Alan: Sistem odaları, arşivler vb. kurumsal bilgi barındıran yetkilendirilmiş alanlar.

4. UYGULAMA:

4.1. **Fiziksel Güvenlik Uygulamalarında Dikkat Edilecek Hususlar;**

4.1.1. Kurumun binalarının fiziksel olarak korunması, farklı koruma mekanizmaları ile donatılması temin edilmelidir.

4.1.2. Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binalarda ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanmalı ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol alt yapıları teşkil edilmelidir.

4.1.3. Kurum dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili görevliler gözetiminde gerçekleştirilmelidir.

4.1.4. Kritik bilgilerin bulunduğu alanlara girişlerin kontrolü akıllı kartlar veya farklı sistemler ile yapılmalı ve izlenmelidir.

4.1.5. Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin güncelliği sağlanmalıdır. Personel akıllı kartların düzenli olarak taşınması sağlanmalıdır.

4.1.6. Kritik sistemler sistem odalarında tutulmalıdır.

4.1.7. Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmalı, yangın ve benzer felaketlere karşı koruma altına alınmalıdır.

4.1.8. Yazıcı vb. cihazların yetkisiz kullanıma karşı koruma altına alınmalıdır.

4.1.9. Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve kontrol altında tutulması temin edilmelidir.

4.1.10. Fotoğraf, video, ses vb. kayıt cihazlarının yetki verilmeyen kişiler tarafından güvenli alanlara sokulmasının yasaklanmalıdır.

4.2. **Veri Tabanı Güvenliğinde Uygulamalarında Dikkat Edilecek Hususlar;**

4.2.1. Veri tabanı sistem logları tutulmalı ve izlenmelidir.

4.2.2. Veri tabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli alınması kontrol altında tutulmalıdır.

4.2.3. Yedekleme planları dokümante edilmelidir.

4.2.4. Veri tabanı erişim politikaları **"Kimlik Doğrulama ve Yetkilendirme"** politikaları çerçevesinde oluşturulmalıdır.

4.2.5. Hatadan arındırma, bilgileri yedekten dönme kuralları **"Acil Durum Yönetimi"** politikalarına uygun olarak oluşturulmalı ve dokümante edilmelidir.

4.2.6. Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.

4.2.7. Veri tabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmaları yetkili bir personel gözetiminde yapılmalıdır.

4.2.8. Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulmalı ve sonrasında ilgili uygulama kontrolleri gerçekleştirilmelidir.

4.2.9. Bilgi saklama ortamlarının kurum dışına çıkarılması için yetkilendirme yapılması ve bu durum izleme takip amacıyla kaydedilmelidir.

4.2.10. Veri Tabanı işletim sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için kurulacak temaslar belirlenmelidir.

4.3. Sunucu Güvenliği Uygulamalarında Dikkat Edilecek Hususlar;

4.3.1. Sahip Olma ve Sorumluluklar

Kurum bünyesindeki bütün dahili sunucuların yönetiminden Bilgi İşlem Daire Başkanlığı sorumludur. Sunucu konfigürasyonları sadece bu grup tarafından yapılacaktır. Bütün bilgiler tek bir merkezde güncel olarak tutulmalıdır. Bütün cihazlar kurumun Ayniyat Saymanlığı envanterinde kayıtlıdır.

4.3.2. Genel Konfigürasyon Kuralları

- İşletim sistemi konfigürasyonları Bilgi İşlem Daire Başkanlığı talimatlarına göre yapılacaktır. Kullanılmayan servisler ve uygulamalar kapatılacaktır. Eğer mümkünse servislere erişimler için log tutulacaktır. Sunucu üzerinde çalışan işletim sistemlerinin, hizmet sunucu yazılımlarının ve anti-virüs vb. koruma amaçlı yazılımların sürekli güncellenmesi sağlanmalıdır. Sunucu güncellemelerini **"Denetim ve Değişim Yönetimi Prosedürü"** kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanmalıdır.
- Sistem yöneticileri gerekli olmadığı durumlar dışında "Administrator" ve "root" gibi genel kullanıcı hesapları kullanmamalı, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmalıdır. Genel yönetici hesapları yeniden adlandırılmalıdır. Gerekli olduğunda önce kendi hesapları ile log-on olup, daha sonra genel yönetici hesaplarına geçiş yapmalıdırlar. Ayrıcalıklı bağlantılar teknik olarak mümkünse güvenli kanal (SSH veya IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
- Sunucular fiziksel olarak erişim kontrollü sistem odalarında bulunmalıdırlar.

4.3.3. Gözlemleme

- Kritik sistemlerde oluşan bütün hareketler loglanmalıdır.
- Güvenlikle ilgili loglar minimum 12 ay saklanmalıdır.
- Güvenlikle ilgili loglar sorumlu kişi tarafından değerlendirilecek ve gerekli tedbirleri alacaktır.

4.3.4. Uygunluk

- Denetimler yetkili organizasyonlar tarafından Kurum bünyesinde belli aralıklarda yapılacaktır. Denetimler Bilgi İşlem Daire Başkanlığı tarafından yönetilecektir. Denetimler organizasyonun işleyişine zarar vermemesi için maksimum gayret gösterilecektir.

4.3.5. İşletim

- Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir. Sunucuların yazılım ve donanım bakımları belirlenmiş aralıklarla, Teknik Destek Şube Müdürlüğü tarafından yapılmalıdır. Sistem odalarına yetkisiz girişler engellenmelidir. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve kaydedilmelidir.

4.3.6. **Şifreleme Güvenliği**

- Şifreleme politikası gereği mevcut sistem, sunucuya bağlanma yetisine sahip her kullanıcının 90 günde bir şifresini resetlemektedir. Güçlü şifre ön şartı ile çalışan sistemde değiştirilen şifreler büyük ve küçük karakter, rakam ve noktalama işareti kullanımını zorunlu kılmaktadır. Kullanıcılara ait değiştirilen şifreler en son 2 şifre ile aynı olamaz ve en az 8 karakter olmalıdır. Kullanıcı hesapları minimum 10 denemeden sonra otomatik olarak kitlenmelidir.

4.4. **Program Kaynak Kodlarına Erişimin Kontrolü**

4.4.1. Mümkün olduğu takdirde programların kaynak kütüphaneleri operasyonel sistemler üzerinde tutulmaz.

4.4.2. Programların kaynak kodları ve kaynak kodu kütüphaneleri kontrol altında bulundurulur.

4.4.3. Program kaynak kodu kütüphanelerine yazılım geliştirme personeli dışında kimseye erişim yetkisi verilmez.

4.4.4. Program kaynak kütüphanelerinin, ilgili öğelerin ve program kaynaklarının programcılara yayımı uygun yetkiler alındıktan sonra yapılır.

4.4.5. Program kaynak kütüphanelerine erişimlerin izleme kayıtları (log) tutulur.

4.5. Dışarıdan Sağlanan Geliştirme Desteği

4.5.1. Dışarıdan geliştirme desteği alınırken kurum içinde önem gösterilen güvenlik kuralları birebir olarak uygulanır.

4.5.2. PR.14 Tedarikçi Değerlendirme Prosedürü izlenerek tedarikçi seçilir ve tedarikçi değerlendirmeleri yapılır.

4.5.3. Her tedarikçi ile yapıldığı gibi yazılım tedarikçisi ile de gizlilik sözleşmeleri imzalanır.

4.5.4. Yazılım tedarikçileri ile yapılan anlaşmalarda geliştirilecek yazılımla ilgili Lisans ve Fikri Mülkiyet Hakları göz önünde bulundurulur.

4.5.5. Tedarikçilerin, tedarik ettiği yazılımın çalıştığı canlı ortama bağlanmalarına Bilgi İşlem Daire Başkanlığı onayı ile izin verilir.

4.5.6. Tedarikçinin canlı ortama bağlanması sonrasında erişim yetkileri kaldırılarak veya giriş şifresi değiştirilerek tedarikçinin erişimi engellenir.

4.5.7. Tedarikçi geliştirme ve test ortamlarını güvenli ortamlar olarak işletmekle yükümlüdür.

4.5.8. Kurum haberli ve/veya habersiz olarak tedarikçinin yazılım geliştirme prosedürlerine uyumluluğunu denetleyebilir.

4.6. Test Verisinin Kullanımı

Test verileri korunması için gerekli kontroller uygulanır. Sistem test verisi gerçek sistemdeki veri ile boyut ve içerik olarak kabul edilebilir düzeyde yakındır. Kişisel bilgilerin bulunduğu veriler, test verisi olarak kullanılmaz ya da kullanılacak ise değiştirilir. Kişisel veri benzeri veri kullanılacaksa kullanılan veri kişisel gizli bilgi içeriğine sahip olamayan anonimleşmiş veriden seçilir. Eğer gerçek sistemdeki operasyonel veri, test için kullanılacak ise aşağıdaki kontrollere dikkat edilir.

- Sistem verilerine uygulanan erişim kontrolü aynı şekilde test verisine uygulanır.
- Operasyonel sistem verisinin test sistemine kopyalanması aşamasında yetki kontrolleri uygulanır.
- Test işlemi bittikten sonra ihtiyaç yok ise test verisi silinir.
- Operasyonel sistem verisinin kopyalanması kayıt altına alınır.

4.7. WEB Filtreleme

Kötü amaçlı içeriğe maruz kalmayı azaltmak için harici web sitelerine erişim yönetilmelidir.

a) İş gereksinimleri ile ilgili web içeriğine erişim kuralları yönetim tarafından kararlaştırılır.
b) Sosyal medya, mesajlaşma uygulamaları ve diğer iş dışı web sitelerine erişim, çalışanların iş performansını olumsuz etkileyebileceği için kısıtlanabilir.
c) Yasalara ve düzenlemelere aykırı web içeriği engellenecektir.
d) Kurum gizlilik ve güvenlik politikalarına aykırı web içeriği engellenecektir.

4.7.1. Web Filtresi Kullanımı ve Yapılandırması

a) Web filtreleme hizmeti, firewall ve DNS üzerinden sağlanır.
b) Web filtreleme politikaları, USOM tarafından sağlanan kara liste kullanılır.
c) Web filtreleme politikaları, zararlı web sitelerini otomatik olarak engelleyecek şekilde yapılandırılır.

4.8. İzleme Faaliyetleri

4.8.1. Ağ, sistemler ve uygulamaların izlenmesi

Ağ, sistemler ve uygulamaların izlenmesi, sızma girişimlerinin veya zararlı yazılım bulaşmasının tespit edilmesi amacıyla gerçekleştirilir.

Bu izleme işlemi, ağ trafiğinin analiz edilmesi, olay günlüklerinin incelenmesi, performans metriklerinin takip edilmesi ve varlık envanterinin güncel tutulması yoluyla gerçekleştirilir.

İzlenen ağ, sistem ve uygulamalar için, güncel antivirüs yazılımları, güvenlik duvarı, saldırı tespit sistemi ve benzeri güvenlik araçları mümkünse kullanılmalıdır.

4.8.2. Olayların değerlendirilmesi

Olası bir bilgi güvenliği olayı tespit edildiğinde, "PR.13 Olay İhlal Prosedürü" işletilmeli ve olayın kaynağı belirlenmeli ve mümkün olan en kısa sürede uygun bir yanıt planı uygulanmalıdır.

Olası bir bilgi güvenliği olayı, aşağıdaki durumlarda ortaya çıkabilir:

- Bir güvenlik aracı, bir olayın meydana geldiğine dair bir uyarı verir.
- Sistemde veya ağda anormal bir davranış gözlemlenir.
- Bir kullanıcı, şüpheli bir etkinlik bildirir.

4.8.3. Uygun önlemlerin alınması

Olası bir bilgi güvenliği olayı tespit edildiğinde, uygun bir yanıt planı uygulanmalıdır. Bu plan, olayın ciddiyetine ve doğasına bağlı olarak değişebilir.

Yanıt planı, aşağıdaki bileşenleri içerebilir:

- Olayın kaynağının belirlenmesi
- Olayın doğrulanması
- Gerekli önlemlerin alınması
- Olayın sonuçlarının tespiti ve iyileştirme çalışmaları

Yanıt planı, ilgili personel tarafından düzenli olarak gözden geçirilmeli ve güncellenmelidir.

4.9. Veri Sızıntısı Önleme

Veri sınıflandırması: Veriler, hassasiyet düzeylerine göre sınıflandırılmalıdır. Daha hassas veriler daha sıkı bir şekilde korunmalıdır.

Erişim kontrolü: Veriye erişim, iş gereksinimlerine göre tanımlanmalıdır. Sadece yetkili personel tarafından erişilebilir olmalıdır.

Güçlü kimlik doğrulama: Güçlü kimlik doğrulama yöntemleri kullanılmalıdır. Şifreler düzenli olarak değiştirilmeli ve uzunluğu, karmaşıklığı ve benzersizliği sağlanmalıdır.

Güvenlik duvarı: Güvenlik duvarı kullanılmalı ve güncel tutulmalıdır. Güvenlik duvarı, yetkisiz erişimleri önlemek için ağ trafiğini izlemeli ve filtrelemelidir.

Veri şifreleme: Hassas veriler şifrelenmelidir. Bu, verilerin çalınması durumunda bile korunmasına yardımcı olabilir.

Veri yedekleme: Veriler düzenli olarak yedeklenmelidir. Bu, verilerin sızıntı durumunda geri yüklenebilmesine yardımcı olabilir.

Risk değerlendirmesi: Kuruluş, olası veri sızıntılarına karşı düzenli olarak risk değerlendirmesi yapmalıdır.

4.10. Fikri Mülkiyet Haklarının Korunması

Kurum süreçlerinde üretilen ve/veya Yazılım Geliştirme gibi kurum kaynakları ve altyapıları kullanılarak üretilen bilgiler, ürünler/hizmetler ve eserlerin fikri mülkiyeti kuruma aittir. Kurum ait ürünler/hizmetler ve eserler yazılı sözleşmelere ve izinler olmaksızın başka kurum ve kuruluşlara açıklanmamalı, verilmemeli, kullandırılmamalıdır. Bu ürün/hizmetler ve eserleri, fiziksel veya sayısal yöntem ve araçlarla izinsiz kopyalamak, çoğaltmak, iletmek, yayınlamak ve satmak yasaktır.

4.10.1. Fikri Mülkiyet Hakları Esasları

Diğer kurum ve kişilere ait eser ve ürünlerin doğru kullanılması ve bunların yanlış kullanımdan doğabilecek yasal sorunların engellenmesi amacıyla uygulanacak kurallar ve izlenecek adımlar aşağıda tanımlanmıştır:

- Kurum tarafından temin edilmemiş ve/veya onay verilmemiş yazılımlar kuruluşun bilgi işlem sistemleri üzerinde kullanılmaz. Sistemlerde yapılan güvenlik taramalarında bu husus kontrol edilir.
- Yazılımların lisans takibi Bilgi İşlem Daire Başkanlığı tarafından sağlanır.
- İhtiyaç duyulan yazılımların lisanslarının temin edinilebilmesi için satın alma süreçleri takip edilir.
- Kurum veya çalışan tarafından satın alınmamış/yasal biçimde edinilmemiş basılı yayınlar (kitap dergi, ses ve görüntü kasetleri vb.) BT kaynakları ve diğer ofis araçları (faks, fotokopi vb.) kullanılarak kullanılmaz, depolanmaz, çoğaltılmaz ve paylaşılmaz.
- Sahip olunan yazılım ve ürünler lisansın izin verdiği maksimum kullanıcı sayısını aşmayacak şekilde kullanılır.

4.10.2. Fikri Mülkiyet İhlalleri Durumunda Uygulanacak İşlemler

Kuruma ait Fikri Mülkiyet Haklarının korunması için, ihlal durumlarında Bilgi Güvenliği Olay Yönetim kapsamında değerlendirmede bulunulur ve disiplin süreci işletilir.

4.11. Kriptografik Kontroller

4.11.1. Erzurum Teknik Üniversitesi Bilgi İşlem Dairesi Başkanlığı'nın sahip olduğu veya yeni alınan her türlü SSL sertifikaları Bilgi İşlem Dairesi Başkanlığı tarafından takip edilir.

	HAZIRLAYAN	ONAYLAYAN
ÜNVANI	BGYS YÖNETİM TEMSİLCİSİ (DAİRE BAŞKANI)	GENEL SEKRETER
ADI SOYADI	Dr. Naci BAYRAK	Prof.Dr. Ahmet DUMLU
İMZA		