SAĞLIK BİLİMLERİ ÜNİVERSİTESİ

Hazırlayan	Kontrol eden	Onaylayan

Bilgi İşlem Daire Başkanlığı

Tarih: 2026

İÇİNDEKİLER

Hazırlayan	Kontrol eden	Onaylayan

Hazırlayan	Kontrol eden	Onaylayan

Hazırlayan	Kontrol eden	Onaylayan

Hazırlayan	Kontrol eden	Onaylayan

Hazırlayan	Kontrol eden	Onaylayan

1. BİLGİ GÜVENLİĞİ POLİTİKASI

Sağlık Bilimleri Üniversitesi (SBÜ); eğitim-öğretim, araştırma, sağlık hizmeti sunumu ve idari faaliyetleri kapsamında üretilen, işlenen, saklanan ve iletilen tüm bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı temel bir kurumsal sorumluluk olarak kabul eder. Bu politika, ISO/IEC 27001:2022 standardının gereksinimleri doğrultusunda üniversitemizin tüm kampüslerini (Hamidiye, Gülhane, Selimiye, DETUAM ve diğer kampüsler) ve bu kampüslerde görev yapan personeli, akademisyenleri, öğrencileri, paydaşları, tedarikçileri ile bilgi varlıklarına erişim sağlayan tüm ilgili tarafları kapsar.

SBÜ üst yönetimi, Bilgi Güvenliği Yönetim Sistemi (BGYS) kapsamında;

Üniversitenin misyon, vizyon ve stratejik hedefleriyle uyumlu bilgi güvenliği hedeflerinin belirlenmesi için bir çerçeve oluşturmayı ve bu hedeflerin düzenli aralıklarla gözden geçirilmesini sağlamayı,

Bilgi güvenliği risklerinin sistematik olarak belirlenmesi, analiz edilmesi ve değerlendirilmesi amacıyla risk yönetim metodolojisini kurumumuz, personelimiz, akademisyenlerimiz, öğrencilerimiz, paydaşlarımız ve tedarikçilerimiz için kurmayı ve risklere ilişkin uygun kontrol önlemlerinin alınmasını sağlamayı,

Bilgi İşlem Daire Başkanlığı faaliyetleri kapsamında hizmet kalitesini sürekli iyileştirmeyi,

Bilgi güvenliği risklerini azaltmak için gerekli insan kaynağı, donanım, yazılım, eğitim ve diğer kaynakları tahsis etmeyi ve bu kaynakların devamlılığını sağlamayı,

Bilgi güvenliğinin ihlali durumunda gerekli görülen yaptırımları uygulamayı,

6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) başta olmak üzere bağlı olunan ulusal, uluslararası ve sektörel düzenlemelere, yasal ve ilgili mevzuat gereklerine uymayı, anlaşmalardan doğan yükümlülükleri karşılamayı, iç ve dış paydaşlara yönelik kurumsal sorumluluklarından kaynaklanan bilgi güvenliği gereksinimlerini sağlamayı,

Tüm personelin ve iş ortaklarının bilgi güvenliğinin sağlanmasındaki süreçlere katılımını ve uymasını sağlamak için bilinçlendirme, eğitim ve teşviki düzenli olarak planlamayı ve uygulamayı,

Bilgi güvenliği olaylarının raporlanması, değerlendirilmesi ve müdahale süreçlerinin etkin şekilde işletilmesi için gerekli mekanizmaları tesis etmeyi,

İş sürekliliği yönetimi kapsamında kritik bilgi sistemlerinin kesintisiz hizmet verebilmesi için gerekli planları oluşturmayı ve düzenli olarak test etmeyi,

BGYS'nin verimliliğini iç ve dış denetimlerle kontrol etmeyi, izlemeyi, gözden geçirmeyi ve sistemi sürekli uyumlu kılmayı, sürekli iyileştirmeyi,

BGYS politikası olarak benimser ve taahhüt eder.

2. KABUL EDİLEBİLİR KULLANIM POLİTİKASI

2.1. AMAÇ

Kabul Edilebilir Kullanım Politikasının amacı, SBÜ personelinin Sistem, Bilgi ve Varlıkların Gizlilik, Bütünlük ve Erişebilirlik özelliğini garantilemek için yapması ve uyması gereken iş kurallarını kendilerine iletmektir.

2.2. KAPSAM

Bu politika; SBÜ personeli ile kurum için çalışan yüklenici firmalar ve SBÜ 'nün bilişim etkileşimli kritik bilgi varlıklarını kullanan tüm şahısları kapsamaktadır.

2.3. SORUMLULUKLAR

Tüm personeller

2.4. TANIMLAR

Gizlilik : Bilginin yetkisiz kişiler, varlıklar ya da proseslere kullanılabilir yapılmama ya da açıklanmama özelliği.

Bütünlük : Varlıkların doğruluğunu ve tamlığını koruma özelliği.

Erişebilirlik : Bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanılabilir durumda olmasıdır.

Penetrasyon (Sızma) Testi: Kötü amaçlı bir saldırganın içeriden ya da dışarıdan sistemlere verebileceği zararı önceden görebilmek ve zayıflıklar için tedbir alabilmek amaçlı planlanmış konusunda uzman kişiler tarafından kullanılan araç ve teknikler ile hedef kurum veya kuruma yönelik gerçekleştirilen bir saldırı simülasyonudur.

2.5. İLGİLİ DOKÜMANLAR

Bilgi Güvenliği Politikası

Disiplin Prosedürü

Olay Bildirim Formu

Parola Politikası

2.6. UYGULAMA

SBÜ bünyesinde kullanılan bilişim cihazlarının her türlü uygunsuz kullanımı virüs saldırılarına, ağ sistemlerinin çökmesine, hizmetlerin aksamasına sebep olabilir ve bunlar yasal yaptırımlara dönüşebilir.

SBÜ'nün amacı herhangi kimse üzerinde kısıtlayıcı politikalar üretmek değil aksine açıklık, güven ve bütünlüğe yönelik kültürü yerleştirmektir. SBÜ, bilerek veya bilmeyerek yapılan yasadışı veya zararlı eyleme karşı hem personelleri hem de SBÜ'nün haklarını korumaya adamıştır. Bu sistemler SBÜ'nün ve personellerimiz menfaatleri doğrultusunda kullanılmalıdır.

Güçlü bir güvenlik ancak bütün personellerin içerisine dahil olduğu takım çalışmasıyla oluşturulabilir. Bu itibarla, bütün kullanıcılar günlük aktivitelerini yerine getirebilmesi için bu kuralları iyi bilmeli ve uygulamanın sorumluluğunu taşımalıdır.

Genel Kurallar

SBÜ ortamında tutulan ve iletilen tüm bilgiler; SBÜ'nün malıdır ve SBÜ bu bilgileri izleme ve denetleme hakkına sahiptir.

Hiçbir personel, bilgisayarlarından anti virüs koruma yazılımını devre dışı bırakamaz, kaldıramaz veya silemez.

Kaynağı belli olmayan ve üretici firma tarafından kopya edilmesi yasaklanmış bir bilgisayar yazılımını kopyalamak yasaktır.

SBÜ personeli, kendilerine tahsis edilmiş tüm bilgisayar erişim bilgilerini ve kendisine verilmiş güvenlik cihazlarını korumaktan sorumludur. Erişim bilgileri herhangi birine söylenemez ve bu bilgiler başkaları ile paylaşılamaz.

Hiçbir personel izin almadan kendi bilgisayarından veya başka bir kaynak kullanarak, SBÜ'nün Bilişim Ağını tarayamaz, izleyemez veya dinleyemez.

SBÜ onaylı resmi penetrasyon (sızma) testleri haricinde, kurum bilgisayar sunucuları için içeriden veya dışarıdan port taraması yapılması yasaktır.

Hiçbir personel, kurum içinde kendilerine tahsis edilen bilgisayar yetkilerinin dışına çıkamaz ve bu konuda yetki aşma işlemine girişemez.

SBÜ adına iş yapan Yüklenici Firma personeli; SBÜ'nün izni ve onayı olmadan SBÜ bilgilerini başkaları ile paylaşamaz. SBÜ'nün izni olmadan iç ağ ve Internet üzerinden bilişim ağlarını tarayamaz ve Penetrasyon testleri gerçekleşemez.

Gizli Bilginin Paylaşımı ve Saklanması

Gizli bilgi ve veriler SBÜ içerisinde sadece işi gereği bilmesi gereken personellerle paylaşılmalıdır. Gizli bilgi ve verilerin ifşa edilmesi gereken üçüncü şahısları var ise, sadece yetki verme amacıyla paylaşılmalı ve gizli tutmayı taahhüt etmeleri sağlanır.

Paylaşılan dokümanın gizliliğine göre yüksek korumalı dosya parolası oluşturulmalı, oluşturulan parola ilgili kişilere farklı bir e-posta aracılığı ile ya da telefon ile

paylaşılmalıdır. Parolanın dosyanın gönderildiği e-posta da açıkça belirtilmemesine özen gösterilmelidir.

Gizli bilgi ve verileri içeren dosyalar sadece bu bilgiye ulaşması gereken kişilerin girebileceği erişim yetkisi ile SBÜ'nün dosya sunucusu üzerinde ortak klasörlerde saklanmalıdır. Gizli bilgi içeren dosyalara yapılan erişimlerin log kayıtları alınmalıdır.

Gizli Bilgi veya Hassas Kişisel Bilgi içeren Materyallerin Saklanması, Arşivlenmesi ve İmha Edilmesi

Öğle yemeği ve/veya her çalışma günü sonu gibi masadan uzun süreli uzak olunan zamanlarda, "Gizli Bilgi" veya "Hassas Kişisel Bilgi" içeren tüm materyaller kilitli çekmece ve/veya kilitli ofislerde anahtarı üzerinde bırakılmadan (anahtar güvenli bir yerde tutularak) muhafaza edilmelidir. Masa üzeri, yazıcı yanı, dolap üzeri, toplantı odası gibi açık alanlarda bırakılmamalıdır.

Masa üzeri, yazıcı yanı, toplantı odaları, yemekhane vb. gibi açık/korunmasız bir alanda "Gizli Bilgi" veya "Hassas Kişisel Bilgi" içeren bir doküman görüldüğünde, derhal doküman bulunduğu yerden alınarak bağlı olduğunuz yöneticiye ve/veya İnsan Kaynakları ve/veya Bilgi Teknolojileri görevlilerine iletilmelidir.

"Gizli Bilgi" veya "Hassas Kişisel Bilgi" içeren evrak ve dosyalar işlemleri tamamlandığında Birime ait Arşiv alanında Arşiv Saklama Koşullarına uygun olarak muhafaza edilmelidir. Arşivden alınan evrak ve dosyalar tekrar Arşiv alanına kaldırılmalıdır.

"Gizli Bilgi" veya "Hassas Kişisel Bilgi" 'ler çöp kutusuna ve/veya geri dönüşüm kutusuna atılmamalıdır. Bu tarzda bilgi içeren evrakları uygun bir şekilde imha etmek için kâğıt öğütücü ve/veya kilitli öğütme çöp kutusu kullanılmalıdır. Yasal bekletme sürecine tabi olan hiçbir evrak imha edilmemelidir.

Kurum Bilgisayarı ve Diğer Dijital Aygıtların Kullanımı

Masadan ayrılan tüm zamanlarda bilgisayar ekranı kilitlenmeli ve her çalışma günü sonunda bilgisayar sistemi kapatılmalıdır.

Dizüstü bilgisayar, kişisel dijital yardımcılar, CD, DVD veya USB disk gibi veri saklama aygıtları hassas kişisel bilgi kategorisinde olup, şifrelenerek, kilitli çekmece ve/veya kilitli ofislerde anahtarı üzerinde bırakılmadan (anahtar güvenli bir yerde tutularak) saklanmalıdır.

Bilgisayar ve diğer program parolaları Bilgi Teknolojileri sisteminin önerdiği şekilde belirlenmeli ve önerdiği aralıklarla değiştirilmelidir. Bilgi Teknolojileri dışında bağlı olunan yönetici dâhil kimse ile paylaşılmamalıdır.

Parola belirleme kuralları:

Ad, soyadı, doğum tarihi, telefon numarası gibi kişisel bilgiler parola olarak seçilmemelidir.

Parola Politikasında belirtilen şartlara uygun özellikte oluşturulmalıdır.

Parolalar düzenli aralıklarla ve en az Parola Politikasında belirtilen sürede değiştirilmelidir.

Parola ve erişim bilgileri üçüncü şahısların ulaşabileceği bilgisayar ortamında bir dosyada ve/veya hatırlatma kâğıdı olarak açık ortamda ve/veya anımsatıcı olarak herhangi bir programda saklanmamalıdır.

SBÜ'nün tahsis ettiği yazılımlar ilgili lisans kurallarına uygun bir biçimde kullanılmalı ve lisanslı olmayan yazılımlar illegal bir şekilde kesinlikle kullanılmamalıdır.

Toplantı Odaları & Açık Ofis & Çalışma Alanlarının Kullanımı

Toplantı sonrasında "Gizli Bilgi" veya "Hassas Kişisel Bilgiler" toplantı odasında bırakılmamalıdır. Toplantı esnasında kullanılan yazı tahtasındaki bilgiler uygun şekilde imha edilmelidir.

Evrak, dosya, numune ürün vb. materyaller ve kişisel eşyalar açık ofis ortamının çalışma koşulunu olumsuz etkilemeyecek şekilde çalışma alanınızda dolap ve çekmece gibi güvenilir kilitli alanlarda anahtarı üzerinde bırakılmadan muhafaza edilmelidir.

Temizlik personelinin görevini yerine getirmesini engellememesi açısından çalışma masası yan tarafı ya da altı, dolap üzeri gibi açık ofis ortamındaki ortak alanları kullanmamaya özen gösterilmelidir.

SBÜ dışından gelen ziyaretçi ve merkez ofis de görev almayan personellerin ziyaretçi kartları verilerek gidecekleri yere ilgili birimde personel bir kişi ve/veya Güvenlik Görevlisi eşliğinde ulaşması sağlanır.

Kurum Dışında Kuruma ait Bilgi, Evrak, Bilgisayar ve Dijital Araçların Kullanımı

"Gizli Bilgi" veya "Hassas Kişisel Bilgi" içeren evrak, dosya, Kurum Bilgisayarı ve diğer dijital aygıtlar kurum dışındaki ortamlarda korumasız biçimde açık alanda bırakılmamalı, güvenilir bir biçimde muhafaza edilmelidir. Özellikle bilgisayarların araç içinde bırakılması gereken durumlarda mutlaka kapalı bagaj içinde olmalıdır.

"Gizli Bilgi" veya "Hassas Kişisel Bilgilerin" imhası için kurum içerisinde kâğıt öğütücü kullanılmalıdır.

Kurum dışında açık ortamda yapılan toplantı, görüşme ve/veya çalışma hallerinde yüksek sesle konuşmayarak duyulmamasına ve başkalarının bilgileri görmemesine özen gösterilmelidir.

Bilgi Güvenliği Olay Bildirimi

Tüm personeller, cihazlarda olağandışı bir şey meydana gelmesi, veri dosyalarında olağandışı değişiklikler, ihlaller, şüpheli durumlar oluşması halinde durumu derhal yöneticisine veya Bilgi Teknolojileri Yardım Masası(Bilgi İşlem Daire Başkanlığı)'na (bilgi.guvenligi@sbu.edu.tr) bildirmekle yükümlüdür.

Bilgi Güvenliği Politikasına göre bilgi güvenliği ihlali gerçekleştiği düşünülen olaylarda ise Bilgi Teknolojileri Birimine e-posta yolu ile "Olay Bildirim Formu" nu doldurularak yazılı bir şekilde bildirilmelidir.

Bilgi Teknolojileri Biriminin bilgi güvenliği ihlalini tespit etmesi halinde "Disiplin Prosedürü" ne göre işlem yapılacaktır.

3. ERİŞİM POLİTİKASI

3.1. AMAÇ

Bu politikanın amacı, SBÜ bünyesinde bulunan Bilgi Teknolojileri sistemlerini kullanan kullanıcıların ve kurum sistemlerine dışarıdan bağlantı sağlayacak kullanıcıların kabul edilebilir seviyede fiziki ve dijital erişimlerinin nasıl olması gerektiğini düzenlemek, hassas ve kritik bilgi içeren binalara, odalara, alanlara veya tesislere fiziksel erişim güvenliğini sağlamak ve Kişisel Verilerin Korunması Kanunu'nun 12. Maddesi gereğince alınması gereken tedbirleri almaktır.

3.2. KAPSAM

Bu politikanın kapsamı, SBÜ tarafından sahip olunan veya işletilen tüm Bilgi Teknolojisi kaynakları için geçerlidir. SBÜ Bilgi Teknolojileri kaynaklarında (e-posta, mesajlar ve dosyalar dahil) iletilen veya depolanan, özellikle diğer tarafların mülkiyeti olarak tanımlanmayan tüm bilgiler SBÜ'nün mülkiyetindedir. Bilgi Teknolojileri kaynaklarının tüm kullanıcıları (SBÜ personelleri, yüklenicileri, satıcıları veya diğerleri) bu politikaya uymaktan sorumludur.

3.3. SORUMLULUKLAR

Bilgi İşlem Dairesi Yetkilisi

Bilgi İşlem Dairesi Personeli

İdari İşler Dairesi

3.4. TANIMLAR

EBYS: Elektronik Belge Yönetim Sistemi

SSL VPN (Secure Sockets Layer Virtual Private Network): SSL veya TLS protokolleri üzerinden güvenli erişim sağlayan sanal özel ağ teknolojisidir. SSL VPN bağlantısı uçtan uca şifrelenerek, uç nokta cihazları (bilgisayar, telefon, tablet vb.) ve kurumun veri kaynakları arasında taşınan verinin internet üzerinden taşınmasını sağlar. Bu sayede personeller, kurum veri kaynaklarına (ERP yazılımları, veri tabanları, firmaya özel uygulamalar vb.) kurum ağı dışından güvenli şekilde bağlanırlar.

VPN: Sanal Özel Ağ

3.5. İLGİLİ DOKÜMANLAR

Disiplin Prosedürü

Zimmet Teslim Formu

Parola Politikası

Hesap Teslim Formu

3.6. UYGULAMA

Erişim politikası, SBÜ için genel bilgi güvenliği politikasının bir parçası olarak düşünülebilir. Erişim kontrol prosedürleri, genel olarak güvenlik programı ve gerektiğinde belirli bir bilgi sistemi için geliştirilebilir. Kurumsal risk yönetimi stratejisi, erişim politikasının geliştirilmesinde kilit bir faktördür.

Kullanıcı Erişim Yönetimi

Yetkili kullanıcı erişimini temin etmek, sistem ve hizmetlere yetkisiz erişimi engellemek için dikkat edilmesi gereken hususlar aşağıda belirtilmiştir.

Hazırlayan	Kontrol eden	Onaylayan

Genel Kurallar

Kurum bünyesinde bilgi güvenliği gereklilikleri, iş gereksinimlerine göre açıkça belirtilmeli ve Kurum bilgi güvenliği ile ilgili standartları dikkate almalıdır.

SBÜ'de kullanılan Bilgi Sistemleri ve hizmetler için erişim kontrolleri planlanırken aşağıdaki ilkeler göz önünde bulundurulmalıdır.

Genel İlkeler;

Bilgi Güvenliği: Bilgi güvenliği sistemleri tek bir noktadan sağlanmamalı, kontroller birden çok kontrole bağlı olmalı, iki adımlı kimlik doğrulama ile derinlemesine bir güvenlik sağlanır.

Yetkide İstisna: Kullanıcıların sistemlere erişimleri zorunlu değil istisna olmalıdır. Yetkisi olması durumunda erişebilmelidir.

Gerektiği Kadar Bilme: Erişim yetkisi olan kullanıcıların yetkileri belirli periyodlarla gözden geçirilmeli ve yetkisinin dışında harici bir yetkiye sahip olmamalıdır.

Görevler Ayrılığı: Kullanıcıların sahip olacağı yetkilerin neler olacağı birim yöneticisi tarafından belirlenmelidir.

SBÜ Personelleri veya SBÜ dışı kişilerin erişim sağladığı tüm erişim kayıtları (Firewall, sunucu erişim, veritabanı, v.b. loglar) inkâr edilemez şekilde ve değiştirilemeyeceğinin garanti altına alınması koşulu ile saklanmalıdır. İlgili erişim kayıtları yetkili kişiler haricinde incelenemez ve erişilemez şekilde tutulmalıdır. Erişim kayıtları, "Saklama ve İmha Politikası" nda belirtilen sürelerde saklanmalıdır.

Kullanıcı Oluşturma

Yeni başlayan personelin Kurum ağına, sistemlerine ve uygulamalarına erişim sağlayabilmesi için Bilgi Teknolojileri Birimi tarafından kullanıcı hesabı ve yetkileri oluşturulur. Kullanıcıya parolaları sözlü olarak iletir. Bilgi Teknolojileri Birimi tarafından Active Directory ve diğer uygulamalar için oluşturulan parolalar "Parola Politikasına" göre oluşturulur.

Yetkili Kullanıcı Oluşturma

SBÜ bünyesinde kullanılan Bilgisayar Sunucu Sistemlerine Yönetici (Administrator) düzeyindeki izinlere erişim, yalnızca Bilgi Teknolojileri Birimi tarafından sağlanmaktadır. Personellerin yönetici (Admin) erişim hakkı bulunmamaktadır. Sadece Teknik Servis personelinden bazılarına servis için kullanacakları programları yükleyebilmeleri maksadıyla local admin hakkı verilir. Çeşitli yazılımlarla hangi programları yükleyip kaldırdıklarının takibi yapılmaktadır.

Kullanıcılara Ait Gizli Kimlik Doğrulama Bilgilerinin Yönetimi

SBÜ bilişim sistemlerinde, kimlik doğrulama Active Directory ve Parola Politikası kullanılarak yapılmaktadır. Her kullanıcı SBÜ'nün sistemlerine belirlenen kullanıcı adı ve parolasıyla girmektedir. Kullanıcıların SBÜ içerisinde kendilerine tahsis edilen kullanıcı adı ve parolaları paylaşmayacaklarına dair taahhüt iş sözleşmeleri içerisindeki gizlilik maddesi ile alınmaktadır.

SBÜ Dışı Kullanıcı Oluşturma

Kurum dışından bakım ve destek hizmeti alınan uygulamalar, sunucular ve ağ cihazları için Bilgi Teknolojileri Birimi tarafından kurum dışı kullanıcı oluşturulur. Bağlantı yapılacak uygulamalar ve Sunucular üzerinde ilgili kullanıcıya göre kullanıcı hesabı ve yetkisi oluşturulur. Kurum dışından sistemlere bağlantılar SSL VPN ve Bilgi İşlem Dairesi Personelinin bilgisayarı üzerinden olmak üzere iki şekilde gerçekleştirilir. SSL VPN ile bağlantılarda; Firewall üzerinden gerekli bilgi güvenliği tanımlamaları yapılarak, SSL VPN ile kurum dışından bağlanacak kişilere, bağlanacağı kendi uygulama sunucusuna

yönlendirme yapılarak erişim yetkisine göre bağlantı gerçekleştirmesi sağlanır. "Parola Politikası" na uygun VPN si oluşturularak ilgili kişi ile paylaşılır. Bilgi İşlem Dairesi Personelinin bilgisayarı üzerinden TeamViewer bağlantı yapılması sağlanır. Bağlantı esnasında yapılan işlemlerin izlenmesi sağlanır. Ayrıcalıklı bir kullanıcı hesabı ile oluşturulmuşsa yapılacak işlemler biter bitmez devre dışı bırakılır. SBÜ dışı kullanıcıların dışarıdan erişim sağlayabilmeleri için, SSL VPN ve SMS/Mobil uygulama vb. destekli iki faktörlü doğrulama ile bağlanmaları sağlanmaktadır.

Danışmanlar, hizmet alınan firma personelleri vb. SBÜ dışı kişilerin bağlantısı yapılmadan önce her seferinde Bilgi Teknolojileri Birimi tarafından e-posta veya telefon ile irtibata geçilmeli ve faaliyetin kaydı tutulmalıdır. Bunun için "Uzaktan Erişim Kayıt Formu" doldurulmalıdır ve ayrıca Oturum Kaydetme Yazılımı (Session Recording) ile işlemler kayıt altına alınmalıdır.

Test Kullanıcısı Oluşturma

Oluşturulan test kullanıcılarının 6 ayda bir kontrol sağlanarak silinmesi veya pasife alınması sağlanır.

Kullanıcı Askıya Alma, Silme ve Gözden Geçirme (AD)

Kullanıcı askıya alma, silme ve gözden geçirme işlemleri Active Directory ve kullanılan uygulamalar üzerinden yapılır.

Sistem yönetimi hesapları (administrator), yalnızca sistem yönetimi görevlerini gerçekleştirmek için Bilgi Teknolojileri Birimi tarafından kullanılır.

Bilgi Teknolojileri Birimi tarafından 6 ayda bir yetki ve hesap kontrolü yapılır.

Gözden geçirme işlemleri aşağıdaki kontroller ile yapılır;

• Erişimi olmaması gereken kullanıcıların tespiti

• Rolün gerektirdiğinden daha fazla erişime sahip kullanıcıların tespiti

• Yanlış rollere sahip kullanıcıların tespiti

• Bu politikaya uymayan diğer konuların tespiti

Bu inceleme sonuçları ayrıca yazılı olarak raporlanmalıdır.

Fiziksel Erişim

Bina Erişimi

SBÜ binasının bulunduğu alana erişimler erişim kontrollü olarak yapılmakta ve sınırları belirlenerek dış etkenlere karşı güvenli koruma alanı sağlanmaktadır. SBÜ binasının ana giriş kapıları güvenlik görevlileri gözetiminde tutulur ve kamera sistemi ile izlenir. Mahremiyet gerektiren alanlar ise hiçbir suretle kamera ile izlenmez. Gerekiyorsa halka açık alanları görmeyecek şekilde kamera açıları değiştirilir. Güvenlik personeli bilgi güvenliği politikalarına uymakla yükümlüdür.

Birim Odaları Erişimi

Kişisel veri işlenen ve bulundurulan odalar kullanılmadıkları zaman kilitli bulundurulur.

Koridorlar ve hassas bilgi içeren odalar güvenlik kameraları ile izlenmeli ve kontrol edilir.

Kritik odaları kilitli bulundurulur ve erişimler sadece yetkili personel tarafından sağlanır.

Kullanıcılar masaları başında olmadıklarında ve çalışma ortamının denetimsiz kaldığı durumlarda hassas bilgi içeren basılı bilgileri kilitli ortamlarda bulundurur.

Sistem Odası Erişimi

Sistem odasına erişim güvenliği için kapısı kilitli bulundurulur.

Sistem odasının içerisi ve dışarısı kamera sistemi ile izlenmeli ve kontrol edilir.

Sistem odaları yetkisiz personelin bilerek veya kaza ile erişiminin engellenmesi amacıyla her zaman kilitli tutulur.

Sistem odasına girmeye yetkili olmayan ama bakım/onarım, danışmanlık vb. gibi amaçlarla sistem odasında çalışma ihtiyacı olan kişilerin; uygun şartlar altında, gerekli önlemler alındıktan sonra ve ancak kurum personeli bir kişinin gözetiminde çalışması sağlanır.

Sistem odasında bulunan sunuculara ve bilgi içeren her türlü ekipmanlara fiziksel erişim, kullanıcısı başında bulunduğu zaman zarfında izin verilir ve kontrol altında tutulur.

İşten ayrılan Bilgi İşlem Dairesi Personeline ait yetkiler kaldırılır.

Sistem odası özellikle yangın ve sel baskını gibi doğal afetlere karşı korumalı olmalıdır.

Ağlara ve Ağ Hizmetlerine Erişim

SBÜ personelleri, kendilerine tahsis edilmiş tüm bilgisayar erişim bilgilerini ve kendisine verilmiş güvenlik cihazlarını korumaktan sorumludur. Erişim bilgileri herhangi birine söylenemez ve bu bilgiler başkaları ile paylaşılamaz.

Ağlara İçeriden Erişim

SBÜ içerisinde kullanılan Bilgi Sistemlerine erişim güvenliğini sağlamak ve kontrol etmek için domain yapısı kullanılmaktadır. Kullanıcılar Active Directory üzerinde tanımlı kullanıcı hesapları ve parolaları ile sunucu ve uygulamaların bulunduğu sisteme ve izin verilen ağlara yetkileri dahilinde erişim sağlarlar.

SBÜ ağı çoklu VLAN yapısı ile birimler, sunucular, kameralar ve kablosuz ağlar ile ayrılmıştır. Bilgi Teknolojileri Birimi tarafından VLAN ayrımı sürekli gözden geçirilir ve gerekli olması durumunda yeni VLAN ayrımı yapılır.

Ağlara Dışarıdan Erişim

SBÜ ağına dışarıdan erişim SSL VPN üzerinden Firewall ile SMS kullanılarak iki adımlı kimlik doğrulama ile yapılmaktadır. Uzaktan Erişim Politikasında belirtilen kurallara göre erişim sağlanır.

Kablosuz Ağ Erişimi

SBÜ içerisinde kullanılan kablosuz ağlar, WPA2 şifrelemesi kullanılarak ve farklı bir fiziksel ağ ile LAN'dan ayrılarak 5651 loglaması yapan cihaz üzerinden internete çıkış yapmaktadır.

Wireless ağlarında WPA2 şifreleme metodu kullanılmaktadır. Kullanıcılar misafir ağına giriş yaparken ortak belirlenen birinci parola ve SMS ile cep telefonuna gelen ikinci parolayı girerek misafir ağına giriş yaparlar.

Ziyaretçilerin interneti kullanabilmesi için kablosuz ağlar ayrı bir fiziksel ağ ile misafir ağı olarak ayrılır. Misafir kablosuz ağı 5651 loglaması yapılarak güvence altına alınır.

Kablosuz ağ erişimi özellikle 5651 sayılı kanuna uygun bir şekilde ve 6698 sayılı kanunun 4. Maddesindeki ilkelere uygun bir şekilde kullanıcı erişimleri loglanmaktadır.

Kurum Dışı Kişilerin Uzaktan Erişimi

SBÜ ağına dışarıdan erişim SSL VPN üzerinden Firewall ile SMS kullanılarak iki adımlı kimlik doğrulama ile yapılmaktadır. "Uzaktan Erişim Politikası"nda belirtilen kurallara göre erişim sağlanır.

Ortak Paylaşım Dizinlerine Erişim

Kullanıcılar SBÜ bünyesinde kullanılan dosya sunucusuna Active Directory üzerinde tanımlanmış kullanıcı hesabı ve yetkilerine göre erişir.

Dosya sunucusu üzerinde organizasyon yapısına göre birimlere ayrılmış ve sadece o birimde tanımlı kullanıcıların yetkilerine göre erişebilecekleri klasör yapısı oluşturulur. Kullanıcılar kendi birim klasörlerine yetkisi dahilinde erişim sağlar. Yetkisiz kullanıcılar yetkisi olmayan klasörlere erişemez.

Klasörler içerisinde kişisel verilerin bulunup bulunmadığı, bulunması gerekiyorsa gerekli tedbirlerin alındığı kontrol edilir.

Özel nitelikli kişisel veriler, Active Directory üzerinde tanımlanmış kullanıcı yetkileri dahilinde kurum Dosya Sunucusu üzerinden paylaştırılan birimlere ait klasörler içinde kullanıcılar için tanımlanmış klasörlerde tutulmaktadır. Özel nitelikli kişisel verilerin mutlak suretle şifreli olarak tutulması gerekir.

Her 6 ayda bir dosya sunucusunda klasörler içerisinde bulunan kişisel veriler kontrol edilmeli ve ortak paylaşımda bulunması gerekmeyen veriler, "Saklama ve İmha Politikası"nda belirtildiği gibi yok edilir.

Uygulamalara Erişim

Personelin ilk işe girişinde ilgili birim yöneticisi tarafından personelin kullanması gereken uygulamalar ile ilgili yetkiler belirlendikten sonra uygulamalar ile ilgili kullanıcı adı, parola ve yetkilerin tanımlanması için Bilgi Teknolojileri Birimi'ne EBYS üzerinden talepte bulunulur.

Kullanıcılar uygulamalara kendilerine verilen kullanıcı adı ve parolaları ile yetkileri dahilinde giriş yapar ve kullanır.

SBÜ bünyesinde kullanılan uygulamaların her biri için, Bilgi Teknolojileri Birimi sorumludur. Uygulamalar ile ilgili destek gerekirse Bilgi Teknolojileri Birimi ilgili firmayla bağlantı sağlar.

Uygulamalar ile ilgili dikkat edilmesi gereken hususlar aşağıda belirtilmiştir;

Uygulamalara erişim sadece kullanıcı adı ve parolası olan tanımlı personeller tarafından sağlanır.

Kurulum ile gelen ön tanımlı tüm hesaplar kaldırılır ve ön tanımlı gelen parolalar "Parola Politikası" kapsamında tercih edilen yöntem ile değiştirilir.

Kullanılan uygulamalar içerisinde bulunan Kişisel Verilerin kontrollü erişilebilir olması ve kişisel verilerin mümkün olduğunca maskeli gözükmesi sağlanır.

Uygulamaların güncel versiyonları kontrol edilir ve güncel olması sağlanır.

Uygulamaya erişim sağlayan kullanıcıların hesaplarının Envanter Yazılım Uygulaması içerisindeki "Zimmet Teslim Formu" ile teslim edilir ve her 6 ayda bir yetki kontrolleri ile yetkisiz erişim yapan kullanıcı olup olmadığı kontrol edilir.

Kullanılan uygulamaların yedeklerinin alındığından emin olunur ve alınan yedeklerin şifreli olması sağlanır.

Bulut Sistemlere Erişim

SBÜ'de bulut sistemi olarak Office 365 hizmeti kullanılmaktadır. Office 365 yönetim portalına erişimler sadece Bilgi Teknolojileri personelleri tarafından yapılmakta ve admin rolü ile erişim sağlanmaktadır.

SBÜ'nün kullandığı bulut sistemlerine erişim ilgili bulut sistemlerinin yönetim portalı üzerinden Bilgi İşlem Dairesi Yetkilisi yönetiminde ve kontrolünde sağlanır. Bulut sistemini kullanacak personellere gerekli yetkiler Bilgi İşlem Dairesi Yetkilisi tarafından verilir.

Bulut servis sağlayıcılarının seçiminde Türkiye dışında tutulan veriler için Veri Koruma Politikası kapsamına uygun hareket edilmelidir. Bulut sistemlere erişimde aşağıdaki hususlara dikkat edilir;

Bulut hizmetine erişim hakları Bilgi İşlem Dairesi Yetkilisi kontrolünde yetki matrisi ve yetki kontrolü ile sağlanır.

Kullanıcı hesapları için iki faktörlü doğrulama yapılması sağlanır.

Kullanıcı parolaları için "Parola Politikası" kapsamında belirtilen politikanın uygulanması sağlanır.

İnternet Erişimi

SBÜ internetini kullanan personel, öğrenci, akademisyen ziyaretçi, tedarikçi, danışman gibi üçüncü tarafların güvenli internet erişimi için uyması gereken kurallar aşağıdaki gibidir;

Bütün kullanıcılar ve Sistem yöneticileri aşağıdaki internet erişim ve kullanım yönteminden dışarıya çıkmamalıdır.

İnternet kullanımı;

SBÜ personellerinin interneti sorumlu ve verimli kullanmaları beklenmektedir. İnternet erişimi yalnızca işle ilgili faaliyetlerle sınırlıdır ve kişisel kullanıma izin verilmez.

İşle ilgili faaliyetler, internet üzerinden bulunabilecek ve bir personelin rolüne yardımcı olacak araştırma ve eğitim amaçlarını içerebilir.

SBÜ bilgisayar sistemleri tarafından oluşturulan, iletilen ve/veya alınan tüm İnternet verilerinin SBÜ'ye ait olduğu kabul edilir ve resmi verilerinin bir parçası olarak kabul edilir. Bu nedenle, yasal nedenlerle veya diğer uygun üçüncü taraflara ifşaya tabidir.

İnternete erişmek için kullanılan ekipman, hizmetler ve teknoloji SBÜ'nün mülkiyetindedir ve SBÜ, İnternet trafiğini izleme ve çevrimiçi bağlantıları aracılığıyla oluşturulan, gönderilen veya alınan verileri izleme ve bunlara erişme hakkını saklı tutar.

Tüm web sitesi ziyaretleri ve indirilen dosyalar, iş için zararlı ve/veya iş ile ilgili olmadıkları düşünülürse SBÜ tarafından izlenebilir ve/veya engellenebilir.

Anlık mesajlaşma teknolojisi gibi yazılımların yüklenmesi kesinlikle yasaktır.

Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemeli ve dosya indirme yapılmamalıdır.

Üçüncü şahısların SBÜ internetini kullanmaları birim yöneticilerinin izni ve bu konudaki kurallar dahilinde gerçekleştirilebilecektir.

Personeller tarafından kabul edilemez internet kullanımı aşağıdakileri içerir ancak bunlarla sınırlı değildir:

İnternette ayrımcı, taciz edici veya tehdit edici mesajlar veya resimler göndermek veya yayınlamak

Bilgisayarları herhangi bir şekilde dolandırıcılık ve/veya yazılım, film veya müzik korsanlığı yapmak için kullanmak

Yetkisiz olarak başka birinin parolasını çalmak, kullanmak veya ifşa etmek

Telif hakkıyla korunan veya yetkisiz yazılım ve elektronik dosyaların indirilmesi, kopyalanması veya korsan olarak kullanılması

Gizli materyalleri, ticari sırları veya özel bilgileri kuruluş dışında paylaşmak

Yetkisiz web sitelerine girmek

SBÜ ağına kötü amaçlı yazılım sokmak ve/veya kuruluşun elektronik iletişim sistemlerinin güvenliğini tehlikeye atmak

SBÜ'nün görüşlerini temsil eden kişisel görüşleri aktarmak

Müstehcen, saldırgan veya yasa dışı materyal indirmek veya yüklemek.

Gizli bilgileri yetkisiz alıcılara göndermek.

Film, müzik ve diğer telif hakkıyla korunan materyal ve yazılımları indirmek veya yüklemek.

SBÜ ağının ve bilgisayarlarının güvenliğini tehlikeye atabilecek potansiyel olarak tehlikeli web sitelerini ziyaret etmek.

Bilgisayar korsanlığı, dolandırıcılık, yasa dışı mal alıp satma ve daha fazlası gibi yetkisiz veya yasa dışı eylemler gerçekleştirmek.

Bu belgede belirtilen tüm hüküm ve koşullar, SBÜ ağının ve İnternet bağlantısının tüm kullanıcıları için geçerlidir. Bu kuralları ihlal eden herhangi bir kullanıcı, kurum tarafından uygun görülen disiplin cezalarına tabidir.

Yaptırım

Bu politikaya uygun olarak çalışmayan tüm personel hakkında "Disiplin Prosedürü" hükümleri uygulanır.

4. UZAKTAN ERİŞİM POLİTİKASI

4.1. AMAÇ

Bu politikanın amacı, SBÜ ağına uzaktan erişimlerde dikkat edilecek kuralları ve gereksinimleri tanımlamaktır. Bu kurallar ve gereksinimler, SBÜ kaynaklarının yetkisiz kullanımından kaynaklanabilecek zararlardan SBÜ'nün olası zararını en aza indirecek şekilde tasarlanmıştır. Zararlar, hassas veya kuruma ait gizli verilerin, fikri mülkiyetin, kamu imajının zedelenmesi, kritik SBÜ dahili sistemlerinin zarar görmesi ve bu kayıpların bir sonucu olarak maruz kalınan para cezaları veya diğer mali yükümlülükleri içerir.

4.2. KAPSAM

Bu politika SBÜ'nün bütün personelini, sözleşmelileri veya SBÜ adına personelleri ve SBÜ'nün bilgisayar ağına uzaktan erişen bütün kişi ve firmaları kapsamaktadır.

4.3. SORUMLULUKLAR

Bilgi İşlem Dairesi Başkanlığı

Bilgi İşlem Dairesi Personeli

Uzak bağlantı yapan personel

Kurum dışı uzak bağlantı yapan firmalar

4.4. TANIMLAR

SSL VPN (Secure Sockets Layer Virtual Private Network): SSL veya TLS protokolleri üzerinden güvenli erişim sağlayan sanal özel ağ teknolojisidir. SSL VPN bağlantısı uçtan uca şifrelenerek, uç nokta cihazları (bilgisayar, telefon, tablet vb.) ve kurum veri kaynakları arasında taşınan verinin internet üzerinden taşınmasını sağlar. Bu sayede personeller, kurum veri kaynaklarına (ERP yazılımları, veri tabanları, kurum özel uygulamalar vb.) kurum ağı dışından güvenli şekilde bağlanırlar.

VPN: Sanal Özel Ağ

4.5. İLGİLİ DOKÜMANLAR

Uzaktan Erişim Kayıt Formu

Parola Politikası

4.6. UYGULAMA

Gereklilikler

SBÜ'nün bilgisayar ağına uzaktan erişim tek yönlü şifreleme algoritması veya güçlü bir passphrase ile yapılır.

Internet üzerinden SBÜ'ye uzaktan erişim ile herhangi bir yerdeki bilgisayar ağına erişen kişi SSL VPN teknolojisini kullanılır.

Kurum sistemlerine güvenli uzaktan erişim şifreleme ve güçlü parolalar ile sıkı bir şekilde kontrol edilir. Parolalar Parola Politikasına uygun olarak verilmelidir.

Kullanıcılar kurum ağına uzaktan erişimlerde iki faktörlü kimlik doğrulaması ve SSL VPN bağlantısı yaparak erişim sağlanır.

Uzaktan erişilen bilgisayar veya sunucu mutlaka statik IP ye sahip olmalı ve bu IP kurum güvenlik duvarında tanımlanmış olmalıdır.

VPN bağlantı izni olan yetkili kullanıcılar, oturum açma bilgilerini ve parolalarını aile üyeleri dahil kimseyle paylaşamazlar.

VPN bağlantı izni olan yetkili kullanıcılar, SBÜ'nün ağına uzaktan bağlanmak için SBÜ'ye ait bir bilgisayarı kullanırken, kişisel ağlar dışında, uzak sunucunun aynı anda başka bir ağa bağlı olmamasını sağlamalıdır.

SBÜ işini yürütmek için uzak bağlantı izni ve yetkileri personelin bağlı bulunduğu birim yöneticisi tarafından onaylanmalı ve Bilgi Teknolojileri Birimi 'ne talepte bulunulmalıdır.

Uzaktan erişim teknolojileri aracılığıyla SBÜ dahili ağlarına bağlanan tüm kullanıcı bilgisayarları, en güncel anti-virüs yazılımını kullanmalıdır, buna kurum dışından bağlanacak firmaların bilgisayarları da dahildir. Üçüncü şahıs bağlantıları, gizlilik anlaşmasında belirtilen gereksinimlere uygun olmalıdır.

SBÜ ile uzaktan bağlantı sağlayacak firma ile hassas veriye erişim hakkında gizlilik anlaşması imzalamalıdır.

Uzaktan erişim sağlayacak firmalar için bağlantıdan önce Uzaktan Erişim Kayıt Formu doldurulmalıdır.

Uzaktan erişecek firmaların bağlanacakları uygulama veya sunuculara erişim yetkileri ve rolleri Bilgi İşlem Dairesi Personeli tarafından verilmeli ve işlem bitince açılan hesaplar pasife alınmalıdır.

SBÜ ağlarına uzaktan erişim yöntemi ile dışardan bağlanan firmalar gerekli bilgi güvenliği tedbirlerini almalıdır. (Firewall, Antivirus vb.)

SBÜ Bilgi Teknolojileri Birimi tarafından 6 Ayda bir periyodik olarak kullanıcı hesapları kontrol edilmeli ve gereksiz kullanıcı hesapları kaldırılmalıdır.

Uzaktan erişim sağlayacak firmanın sadece belli zaman aralıklarında veya istek yapılan durumlarda uzaktan erişimine izin verilebilir.

5. KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI

5.1. AMAÇ

SBÜ'nün bilgi sistemlerine erişimde kimlik doğrulaması ve yetkilendirme politikalarını tanımlamaktır.

5.2. KAPSAM

SBÜ bilgi sistemlerine erişen firma personeli ile kurum dışı kullanıcılar bu politika kapsamı altındadır.

5.3. SORUMLULUKLAR

Bilgi İşlem Dairesi Yetkilisi

Bilgi Teknolojileri Personeli

5.4. TANIMLAR

SSL VPN (Secure Sockets Layer Virtual Private Network): SSL veya TLS protokolleri üzerinden güvenli erişim sağlayan sanal özel ağ teknolojisidir. SSL VPN bağlantısı uçtan uca şifrelenerek, uç nokta cihazları (bilgisayar, telefon, tablet vb.) ve SBÜ'nün veri kaynakları arasında taşınan verinin internet üzerinden taşınmasını sağlar. Bu sayede personeller, kurum veri kaynaklarına (ERP yazılımları, veri tabanları, kuruma özel uygulamalar vb.) SBÜ ağı dışından güvenli şekilde bağlanırlar.

VPN: Sanal Özel Ağ

5.5. İLGİLİ DOKÜMANLAR

Harici bir doküman belirtilmediği için eklenmemiştir.

5.6. UYGULAMA

Kimlik doğrulama, bir sistem veya uygulamanın, bir kişinin veya cihazın gerçekten kim veya ne olduğunu iddia ettiğini ve talep edilen kaynağa erişime izin verildiğini doğrulama sürecidir. Güçlü kimlik SBÜ protokolleri, hem kişisel hem de SBÜ bilgilerinin korunmasına ve SBÜ kaynaklarının kötüye kullanılmasının önlenmesine yardımcı olur.

SBÜ'de kullanılan Bilgi Sistemleri ve hizmetler için erişim kontrolleri planlanırken aşağıdaki ilkeler göz önünde bulundurulmalıdır.

Genel İlkeler;

Bilgi Güvenliği: Bilgi güvenliği sistemleri tek bir noktadan sağlanmamalı, kontroller birden çok kontrole bağlı olmalı ve derinlemesine bir güvenlik sağlanır.

Yetkide İstisna: Kullanıcıların sistemlere erişimleri zorunlu değil istisna olmalıdır. Yetkisi olması durumunda erişebilmelidir.

Gerektiği Kadar Bilme: Erişim yetkisi olan kullanıcıların yetkileri belirli periyodlarla gözden geçirilmeli ve yetkisinin dışında harici bir yetkiye sahip olmamalıdır.

Görevler Ayrılığı: Kullanıcıların sahip olacağı yetkilerin neler olacağı birim yöneticisi tarafından belirlenmelidir.

SBÜ sistemlerine tüm kullanıcılar Windows AD (Active Directory) domain yapısı üzerinden erişim kontrolü sağlanarak erişir.

Tüm kullanıcıların, mevcut oturumları bittiğinde veya iş bilgisayarlarından uzakta olmaları beklendiğinde oturumlarını kapatmaları veya sistemlerini kilitlemeleri gerekir.

SBÜ sistemlerine kurum dışından uzaktan erişim ile erişecek kullanıcılar SSL VPN ile bağlantı sağlamalı ve iki faktörlü kimlik doğrulama ile erişim sağlamalıdır.

Kullanıcılar, kendilerine uygun yetki verilmeyen SBÜ bilgi sistemlerine veya veri tabanlarına erişmeye çalışmamalıdır.

SBÜ'nün uyması gereken bazı düzenlemeler ve sözleşme yükümlülükleri, zorunlu erişim ve kimlik doğrulama yönetimi gereksinimlerine sahiptir. Kapsamlı olmayan bir dizi gereksinim, parola süresinin dolmasını, başarısız denemelerden sonra kilitlemeyi ve bir süre işlem yapılmadığında otomatik olarak oturumu kapatmayı içerebilir.

Özellikle uygulama veya sistem yöneticisi hesapları gibi ayrıcalığa sahip hesaplarda, makul olduğunda, bu hesaplar için iki faktörlü kimlik doğrulama kullanılmalıdır.

Kullanıcılar ve sistemler için oluşturulacak parolalar için Parola Politikası'na uyulmalıdır.

Erişim kontrolleri, maksimum oturum açma denemesi sayısı ve bir kilitleme süresi dahil olmak üzere hesap kilitleme özelliklerini içermelidir.

SBÜ bünyesindeki bilgisayar sistemlerinde kullanılan tüm işletim sistemleri, uygulama yazılımları, veri tabanları, paket programlar ve oturum açılarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkileri Bilgi Teknolojileri Birimi tarafından belirlenerek, kontrol altında tutulmalıdır.

Bilgi Teknolojileri Birimi tarafından kullanıcı erişim ve yetkileri 6 ayda bir AD ve uygulamalar üzerinden kontrol edilerek güncelliği sağlanır.

SBÜ tarafından personelin kullanımına tahsis edilen bilgisayarların güvenliğinden kendileri sorumludur.

Sistemler başarılı ve başarısız erişim logları düzenli olarak tutulmalı, tekrarlanan başarısız log-on girişimleri incelenmelidir.

Kullanıcılar kendilerine verilen kullanıcı hesaplarını ve parolalarını gizlemeli ve kimseyle paylaşmamalıdır.

Bilgi Teknolojileri Birimi tarafından kurum sistemlerine oturum açan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve yetki ihlalleri kontrol edilmelidir.

SBÜ'deki her bir bilgisayar kullanıcısına ayrı bir kullanıcı hesabı açılmalı ve sunuculara, uygulamalara ve sistemlere erişimleri izlenmelidir.

Personelin kullanıcı adı kendi adı.soyadı olarak oluşturulur. Şifresini ilk oluşturmak için 7889'a "sbusifre" yazıp kısa mesaj (SMS) gönderir ve gelen parolayı girerek erişim sağlar.

6. TEMİZ MASA TEMİZ EKRAN POLİTİKASI

6.1. AMAÇ

SBÜ personellerinin mesai saatleri içi veya dışında kendilerine görevleri gereği paylaşılmış olan bilgilerin yetkisiz erişimler veya uygunsuz kullanımı sonucunda başına gelebilecek riskleri ortadan kaldırmak.

6.2. KAPSAM

Çalışma masalarını, bilgisayar ekranlarını, yazıcıları, basılı dokümanlar, belgeler ve kayıtları kapsar.

6.3. SORUMLULUKLAR

Tüm personeller

Bilgi İşlem Dairesi Yetkilisi

Bilgi İşlem Dairesi Personeli

6.4. TANIMLAR

Harici bir tanım belirtilmediği için eklenmemiştir.

6.5. İLGİLİ DOKÜMANLAR

Harici bir doküman belirtilmediği için eklenmemiştir.

6.6. UYGULAMA

Kullanıcılar çalışma masaları üzerinde bulunan "gizli ya da çok gizli" bilgiler içeren basılı evrakları işlemin bitmesini takiben kilitli dolaplarda muhafaza edeceklerdir.

Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler kağıt öğütücü, disk/disket kıyıcı, yakma vb. metotlarla imha edilecektir.

Ortak kullanılan yazıcılar üzerinde herhangi bir doküman bırakılmayacaktır.

Kullanıcı bilgisayarlarında ekranlarında hiçbir etkinlik olmadığı takdirde 10 dakika içerisinde parola korumalı ekran koruyucu devreye girmelidir.

Personelin çalıştığı oda içerisinde kilitli dolap bulunmuyorsa oda kapısı boş zamanlarda kilitlenmeli ve anahtar ilgili personel tarafından muhafaza edilmelidir.

Hazırlayan	Kontrol eden	Onaylayan

Masa çekmecelerinin anahtarları, ev ve araba gibi özel anahtarlar, kasa anahtarları masa üzerinde bırakılmamalıdır.

Duvar tahtalarına/beyaz tahtaya yazılan hassas bilgiler silinmelidir.

SBÜ bünyesinde kullanılan toplantı salonlarında "gizli ve kritik bilgi" içeren dokümanları toplantı sonrasında ilgili salonlarda bırakmamalı ve salonlardaki tahtalara alınmış notlar silinmelidir.

Danışman/Sekreter alanı her zaman mümkün olduğunca açık tutulmalıdır. Ziyaretçilerin ulaşabileceği veya görebileceği masalarda kişisel olarak tanımlanabilecek hiçbir bilgi tutulmamalıdır.

Parolalar, bir bilgisayarın üzerine veya altına yapıştırılan yapışkan notlarda bırakılmamalı ve erişilebilir bir yere yazılmamalıdır.

Bilgisayar ekranları yetkisiz kişilerin görüşlerinden uzak bir açıda olmalıdır.

SBÜ'ye ait yürütülen iş ve işlemlerde SBÜ e-posta @sbu.edu.tr adresi kullanılmalıdır. Bunun haricinde şahsi e-posta adresleri kesinlikle kullanılmamalıdır.

Kullanıcılar, bilgisayarlarının yanından ayrılırken kapatmalı veya kilitlemelidir (Windows; Windows + L, MAC; kntrl+cmd+Q).

Personellerin bu politikaya sürekli uyumunu sağlamak için düzenli ve devam eden Temiz Masa Temiz Ekran denetimleri yapılır.

7. E-POSTA KULLANIM POLİTİKASI

7.1. AMAÇ

Bu politikanın amacı SBÜ e-posta altyapısına yönelik kuralları ortaya koymaktır. SBÜ'de oluşturulan e-postalar resmi bir kimlik taşımaktadırlar. E-posta SBÜ'nün en önemli iletişim kanallarından biridir. Bunun yanı sıra e-posta basitliği ve hızı nedeni ile yanlış kullanıma veya gereğinden fazla kullanıma açık bir kanaldır.

7.2. KAPSAM

Bu politika SBÜ'de oluşturulan e-postaların doğru kullanımını içermektedir ve bütün personeli kapsamaktadır.

7.3. SORUMLULUKLAR

SBÜ Personeli

7.4. TANIMLAR

Harici bir tanım belirtilmediği için eklenmemiştir.

7.5. İLGİLİ DOKÜMANLAR

Harici bir doküman belirtilmediği için eklenmemiştir.

7.6. UYGULAMA

"Bilgi Güvenliği Prosedürü"nde e-posta kullanımı maddesinde belirtilen hususlar ile aşağıdaki kurallar çerçevesinde e-posta kullanım çerçevesi belirtilmiştir.

Yasaklanmış Kullanım

SBÜ e-posta alt yapısı kullanılarak herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren (taciz, suistimal vb.) mesajların gönderilmesi kesinlikle yasaktır. Bu tür mesajların varlığında ilgili birim yöneticisi derhal bilgilendirilmeli ve zararlı içeriğe sahip mesaj silinmelidir.

Mesaj gönderilirken mesajı ve mesaj içeriğini almaya yetkin kişi dışında başkalarına ulaşmaması için son derece dikkat edilmelidir.

E-posta şeklinde gelen spam, sahte e-posta, zincir mesajlar ve içerikleri derhal silinmelidir ve bu tür zararlı e-postalara asla yanıt yazılmamalıdır.

SBÜ e-posta adresleri kişisel amaçla kurum dışı e-posta listelerine üye olmak için kullanılmamalıdır.

Doğrudan veya dolaylı olarak kullanıcı adını ve parolasını isteyen herhangi bir e-posta, sahte bir e-posta olarak ele alınmalı, asla yanıtlanmamalı ve derhal silinmelidir.

SBÜ personelleri kişisel e-posta adreslerini kullanarak rahatsız edici içeriğe sahip (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) mesajlar gönderemez.

Kişisel Kullanım

SBÜ'de personeller e-posta adreslerini kişisel amaçları için uygun ölçüde kullanmalıdır.

Kurumsal e-posta hesaplarına yalnızca hesabın yetkili sahibi erişebilir. Parolaların ve kullanıcı hesaplarının gizliliği korunmalıdır. Personeller, e-posta hesaplarının yetkisiz şahıslar tarafından görülmesi ve okunmasını engellemek ve erişimlere karşı korumakla yükümlüdür.

Ağın bütünlüğü için tehlikeli olan ve kaynağı belli olmayan dosyalara erişilmemeli ve kesinlikle silinmelidir.

Kurumsal mesajlar düzenli olarak personeller tarafından kontrol edilmeli ve zamanında yanıtlanmalıdır.

Birim yöneticileri, SBÜ personellerinin SBÜ'den ayrılması (iş değiştirme, emekli olma vb.) durumunda onların SBÜ e-posta adreslerine ilişkin değişiklik durumunu Bilgi Teknolojileri Birimi'ne bildirmekle yükümlüdür.

İzleme

SBÜ personellerinin gönderdikleri, aldıkları veya sakladıkları e-postalar Bilgi Teknolojileri Birimi'nde yetkili kişiler tarafından önceden haber verilmeksizin e-posta mesajlarını denetleyebilirler.

E-Posta Yönetimi

SBÜ, e-postaların SBÜ bünyesinde güvenli ve başarılı bir şekilde iletilmesi için gerekli yönetim ve altyapıyı sağlamakla sorumludur.

E- Posta Virüs Koruma

E-posta ile gelen ek virüs veya diğer zararlı kodlar bulaşmış ise bir kullanıcıya zarar verebilir. Kullanıcılar virüs bulaşmış olduğundan şüphelendikleri e-postaları bilgisayarlarında bulunan anti-virüs yazılımı ile temizlemeli ve Bilgi Teknolojileri Birimi'ne haber vermelidir.

8. ANTİVİRÜS POLİTİKASI

8.1. AMAÇ

Bu politikanın amacı SBÜ'nün bilişim ortamlarındaki Virüs, Solucan, Truva Atı ve diğer zararlı kodlara ve saldırılara karşı alınacak tedbirleri tanımlamaktadır.

8.2. KAPSAM

Bu politika SBÜ'deki bütün bilgisayarları ve kritik bilgi sistemlerini kapsamaktadır.

Hazırlayan	Kontrol eden	Onaylayan

8.3. SORUMLULUK

Bilgi İşlem Dairesi Yetkilisi

Bilgi İşlem Dairesi Personeli

Tüm Personel

8.4. TANIMLAR

SSL VPN (Secure Sockets Layer Virtual Private Network): SSL veya TLS protokolleri üzerinden güvenli erişim sağlayan sanal özel ağ teknolojisidir. SSL VPN bağlantısı uçtan uca şifrelenerek, uç nokta cihazları (bilgisayar, telefon, tablet vb.) ve SBÜ'nün veri kaynakları arasında taşınan verinin internet üzerinden taşınmasını sağlar. Bu sayede personeller, SBÜ veri kaynaklarına (ERP yazılımları, veri tabanları, kuruma özel uygulamalar vb.) SBÜ ağı dışından güvenli şekilde bağlanırlar.

VPN: Sanal Özel Ağ

8.5. İLGİLİ DOKÜMANLAR

Harici bir doküman belirtilmediği için eklenmemiştir.

8.6. UYGULAMA

Virüslerden, zararlı yazılımlardan, zararlı kodlardan, vb. korunmak için uyulması gereken kurallar aşağıdakilerle sınırlı kalmamak üzere gerekli güvenlik önlemleri alınmalıdır.

SBÜ Bilgi Teknolojileri Birimi tarafından onaylanmış en son antivirüs yazılımları tüm bilgisayarlara kurulmalıdır.

Kullanıcılar bilinmeyen ve şüpheli bir kaynaktan gelen e-posta mesaj ve eklerini açmamalıdır.

Bilgi Teknolojileri Birimi tarafından kullanıcılara iş süreçlerinde kullanılmak üzere verilmiş olan tüm harici disk ve USB bellekler her defasında kullanıcılar tarafından kullanılmadan önce virüs taraması yapılır.

Kullanıcılar tarafından tüm e-posta ve ekleri açılmadan önce antivirüs taramasından geçirilmelidir.

Internet üzerinden kaynağı belli olmayan web sitesinden yazılım yüklemesi yapılmamalıdır.

SBÜ dışı üçüncü taraf kişiler kurum ağına SSL VPN teknolojisi ile bağlanabilir.

SBÜ personeli, e-posta veya başka yollarla kendilerinden istenen parola, kullanıcı kimlik veya gizli bilgileri iletmeyecek ve böyle durumlar olursa bunu Bilgi İşlem Dairesi ekibine hemen bildirecektir.

Kullanıcı bilgisayarlarına ve sunuculara yüklenen antivirüs yazılımı merkezi olarak yönetilmeli ve SBÜ antivirüs sunucusundan otomatik olarak yüklenmeli ve ilgili sunuculara dağıtımı yapılır.

Bilgi Teknolojileri Birimi Birimi tarafından kurulmuş olan antivirüs ve/ya SPAM koruma yazılımlarını kullanıcılar bilgisayarlarından devre dışı bırakamaz veya kaldıramaz.

SBÜ bilişim ağına etkileşimli olarak bağlanacak herhangi bir bilgisayar sisteminin virüs, truva atı, solucan veya diğer zararlı kodlardan muaf olduğu tespit edildikten sonra bağlantısı gerçekleştirilecektir.

SBÜ ağı ve önemli sunucu bileşenleri için Ağ ve Sunucu Saldırı Tespit sistemleri devreye alınacaktır.

9. PAROLA POLİTİKASI

9.1. AMAÇ

Bu politikanın amacı güçlü bir parola oluşturulması, oluşturulan parolanın korunması ve bu parolanın değiştirilme sıklığı hakkında standart oluşturmaktır.

9.2. KAPSAM

Bu politika kullanıcı hesabı olan (Bilgisayar ağına erişen ve parola gerektiren kişiler) bütün kullanıcıları ve tüm SBÜ kayıtlarında bulunan kişisel verilerin şifrelenmesi ile ilgili esasları kapsamaktadır.

9.3. SORUMLULUK

Bilgi İşlem Dairesi Yetkilisi

Bilgi İşlem Dairesi Personeli

Tüm personeller

9.4. TANIMLAR

Passphrase: Bir bilgisayar sistemi için erişim anahtarı olarak kullanılan sözcük ve karakter kombinasyonu (uzunluğu standart bir paroladan daha fazla güvenlik sağlar)

9.5. İLGİLİ DOKÜMANLAR

Harici bir doküman belirtilmediği için eklenmemiştir.

9.6. UYGULAMA

1 Genel

Sunucuların ve ağ cihazlarının yönetimi için kullanılan parolalar en az yılda bir değiştirilir.

Bütün kullanıcı parolaları en az 180 günde bir değiştirilir.

Sunucular ve ağ cihazları için farklı parolalar kullanılır.

Kullanıcılara parolalarını kâğıtlara ya da Word, Excel gibi dokümanlara kaydetmemesi ve SBÜ içi veya SBÜ dışından kişilerle paylaşmaması, konusunda belirli periyodlarda bilgi güvenliği ve farkındalık eğitimleri düzenlenir.

Parolalar hiçbir şekilde e-posta içerisinde veya ek olarak karşı tarafa iletilmez.

SBÜ dışından harici kişiler için açılan kullanıcı hesaplarının parolaları en az 10 karakterde SBÜ'nün parola politikasına uygun ve güçlü bir parolaya sahip olmalıdır.

Bir kullanıcı adı ve parolası birden çok bilgisayarda kullanılmaz.

Özel nitelikli kişisel verilerin aktarılması durumunda mutlak suretle şifreli gönderim sağlanır. Gönderim sağlanacak platformda şifreleme sağlanmıyorsa, aktarımı sağlanacak özel nitelikli kişisel verinin kendisinin şifrelenmesi ve parolanın başka bir platformdan aktarım sağlanacak kişiyle paylaşılması sağlanır.

2. Ana Noktalar

A. Genel Parola Oluşturma Kuralları

SBÜ içerisinde parolalar uygulamalara veya sistemlere oturum açmak için değişik amaçlar için kullanılmaktadır. Bunlardan bazıları: Kullanıcı hesap parolaları, e-posta erişim parolaları, ekran koruma parolaları, yönlendirici erişim parolaları vs. bütün kullanıcılar güçlü bir parola seçimi hakkında özen göstermelidir.

Zayıf Parolalar aşağıdaki karakteristiklere sahiptir:

Parolalar sekiz karakterden daha az karaktere sahiptir.

Parolalar sözlükte bulunan bir kelimeye sahiptir.

Parolalar aşağıdaki gibi ortak değere sahiptir.

Ailesinin, arkadaşının sahip olduğu bir hayvanın veya bir sanatçının ismine sahiptir.

Bilgisayar terminolojisi ve isimleri, komutlar, donanım veya yazılım gibi

“bilişim” , “Ankara” , “İstanbul” gibi

AaaBb, qwerty ,qazwsx, 123321 gibi sıralı harf veya rakamlar

Güçlü Parolalar aşağıdaki karakteristiklere sahiptir:

Küçük ve büyük karakterlere sahiptir. (A-Z , a-z)

Hem dijit hem de noktalama karakterleri ve ayrıca harflere sahiptir. (0-9,!,@,&=(,}?,\)

En az 10 alfanumerik karaktere sahiptir.

Herhangi bir dildeki argo lehçe veya teknik bir kelime olmamalıdır.

Parolalar herhangi bir yere yazılmamalı veya elektronik ortamda tutulmamalıdır.

B. Parola Koruma Standartları

SBÜ bünyesinde kullanılan parolaları SBÜ dışında herhangi bir şekilde kullanmayınız. Kimse ile paylaşmayınız. İlgili parolalar SBÜ’ye ait gizli bilgiler olarak düşünülmelidir. Değişik sistemler için farklı şifreleme kullanın.

Aşağıdakiler yapılmayacaklar listesidir.

Herhangi bir kişiye telefonda parola vermek,

E-posta mesajlarında parola belirtmek,

Üst yöneticinize parolaları söylemek,

Başkaları önünde parolalar hakkında konuşmak,

Aile isimlerini parola olarak kullanmak,

Parolaları işten uzakta olduğunuzda iş arkadaşlarınıza bildirmek,

Uygulamalardaki "parola hatırlatma "özelliklerini seçmeyiniz.

Parolalar en az 180 günde bir değiştirilmelidir.

Parolaların değiştirilip değiştirilmediği yapılan testler ile takip edilir.

C. Uygulama Geliştirme Standartları

Uygulama geliştiricileri programlarındaki aşağıdaki güvenlik özelliklerinin sağlandığından emin olmalıdırlar.

Bireylerin (grupların değil) kimlik doğrulaması işlemini destekleyebilmelidir.

Parolaları text olarak veya kolay anlaşılabilir formda saklamamalıdır.

Kural yönetim sistemini desteklemelidir.

D. Uzaktan Erişen Kullanıcılar İçin Parola Kullanımı

SBÜ'nün bilgisayar ağına uzaktan erişim tek yönlü şifreleme algoritması veya güçlü bir passphrase ile yapılacaktır.

E. Passphrase

Bir passphrase standart parolalardan daha uzun karakter dizisine sahiptir. (genellikle 4'ten 16'ya kadar karaktere sahiptir.), dijital imzaların (bir mesajı gönderen kişinin gerçekten o kişi olduğunu kanıtlayan kodlanmış bir imza), mesajların kodlanması veya çözülmesinde kullanılır.

Passphrase'ler parolalar gibi değildir. Passphrase parolalardan daha uzundur, dolayısı ile daha güvenlidir.

Passphrase'ler tipik olarak birçok kelimeden ibarettir. Bundan dolayı Passphrase'ler "sözlük" saldırılarına karşı daha güvenlidir.

İyi bir passphrase büyük ve küçük harf ve rakamlardan oluşan kombinasyona sahiptir.
Örnek bir passphrase:

"?*@105incicaddedekiTrafik*&#!#Bugun"

Şifreleme için geçerli olan bütün kurallar Passphrase'ler içinde geçerlidir.

10. TAŞINABİLİR MOBİL CİHAZ POLİTİKASI

10.1. AMAÇ

Bu politikanın amacı SBÜ'ye ait bilgi içeren taşınabilir ve mobil cihazların kullanımı ile ilgili kuralları belirlemektir.

10.2. KAPSAM

SBÜ tarafından mobil cihaz verilen tüm personelleri kapsamaktadır.

10.3. SORUMLULUK

SBÜ mobil cihaz verilen tüm personel

Bilgi İşlem Dairesi Yetkilisi

Bilgi Teknolojileri Personeli

10.4. TANIMLAR

Harici bir tanım belirtilmediği için eklenmemiştir.

10.5. İLGİLİ DOKÜMANLAR

Disiplin Prosedürü

Zimmet Formu

10.6. UYGULAMA

SBÜ bünyesinde personellere verilen taşınabilir mobil cihazlar için aşağıdaki hususlara dikkat edilmelidir;

SBÜ tarafından işi ile ilgili kullanması için personele verilen akıllı telefon, telefon hattı, bilgisayar, tablet, laptop gibi mobil cihazlar "Zimmet Formu" ile zimmetlenerek kayıt altına alınır.

Her personel kendisine zimmetlenen cihazın güvenliğinden ve amacına uygun kullanımından sorumludur.

SBÜ tarafından verilen mobil cihazlar üzerine herhangi bir yazılım veya kişisel veri (aile fotoğrafları vs.) yüklenmemelidir.

Cihazlar, mümkün olduğunca hasar görmesini önleyecek şekilde korunaklı olarak taşınmalıdır.

Mobil cihazın işletim sistemi sürümüne (cihazın root erişimi/jailbreak'li olup olmadığı dahil), satıcı/marka, model veya mobil cihaz yönetimi yazılımı istemci sürümüne (varsa) dayalı olarak kurumsal hizmetlere erişimi sınırlanır veya engellenir.

SBÜ tarafından personele verilen SBÜ hattı üzerinden yapılan tüm görüşmelerden personel sorumludur.

Halka açık yerlerde, toplantı odalarında ve diğer korunmasız alanlarda mobil cihazlar kullanılırken dikkatli olunmalı gözetimsiz bırakılmamalıdır.

Bir mobil cihazın kaybolması veya çalınması durumunda, kullanıcının olayı derhal Bilgi Teknolojileri Birimine bildirmesi gerekir. Cihaz, tüm verilerden uzaktan silinecek ve Bilgi İşlem Dairesi Personeli dışında herhangi birinin erişimini önlemek için kilitlenecektir. Cihaz kurtarılırsa, yeniden kullanım için Bilgi Teknolojileri Birimine gönderilebilir. Uzaktan silme, SBÜ işi veya kişisel ile ilgili olsun, cihazdaki tüm verileri yok edecektir. Kullanıcının, nadiren bir güvenlik ihlali durumunda kişisel verilerin silinebileceğini, cihazı kurumsal kaynaklara bağlamadan önce kabul eder.

SBÜ tarafından personele verilen akıllı telefon, telefon ve/veya telefon/data hattı bir başkasına devir veya teslim edilemez.

SBÜ tarafından personele tahsis edilen telefona ait parola, PUK ve PIN gibi bilgilerin gizliliğinden ve yapılan işlemlerden personel kendisi sorumludur.

SBÜ tarafından personele verilen telefon ve/veya telefon hattı kurum işlemleri dışında personelin kendi şahsi işlemleri için kullanılamaz.

Kusur sebebiyle oluşacak hasarların garanti kapsamına girmemesi durumunda telefonda oluşacak hasardan personel sorumludur.

SBÜ'yü belirten etiket veya seri numarası gibi tanımlayıcı işaretler cihaz üzerinden kaldırılmamalıdır.

Cihaz ekranının kısa bir süre kullanılmadığında kilitlendiğinden ve kilidini açmak için bir erişim kodu veya parola gerektirdiğinden emin olunmalıdır. Kullanılan parolalar güçlü ve tahmin edilmesi zor olmalıdır.

Cihaza SBÜ tarafından antivirüs yazılımı yüklenmeli ve düzenli olarak güncellenmesi sağlanır.

Taşınabilir bilgisayarlar admin yetkisi sınırlandırılarak yalnızca user yetkilendirmesi ile ilgili kişiye teslim edilir.

SBÜ'ye ait bilgisayar, telefon, mobil cihaz ve taşınabilir belleklere, siyasi içerikli bilgiler, ırkçılık, şiddet, pornografi veya erotizm içeren resim, film veya müzik kopyalanamaz ve dışarıdan herhangi bir yazılım cihaz içerisinde bulundurulamaz.

SBÜ bilgisayarları ve telefonları üzerinden SBÜ dışı ve SBÜ içi kişilerle SBÜ itibarını zedeleyecek ve yasa dışı olan iletişim kurulamaz.

Bilgisayarlar ve mobil cihazlar üzerindeki antivirüs programları hiçbir nedenle devre dışı bırakılamaz.

Telefon ve mobil cihazlara erişim kontrolü olarak mutlaka parola kullanın.

Taşınabilir bilgisayarlar üzerinde yapılan çalışmalar ve oluşturulan dosyalar mutlaka ağ üzerinde kurumun dosya sunucusuna kaydedilir.

Mobil cihazlarda hassas ve gizli bilgileri mümkün olduğunca bulundurulmamalıdır.

Mobil cihazlarda bulunan verilerin yedekleri alınır ve güncel bir kopyası kurumun dosya sunucusu üzerinde ilgili alanlarda saklanır.

SBÜ verilerini depolamak veya bunlara erişmek için kullanılan tüm mobil cihazlar, SBÜ Bilgi Teknolojileri Biriminin kimlik doğrulama gereksinimlerine uymalıdır. Ayrıca, herhangi bir kurumsal veri taşıyan cihazın kurum ağına bağlanabilmesi için tüm donanım güvenlik yapılandırmalarının SBÜ Bilgi Teknolojileri Birimi tarafından önceden onaylanması gerekir.

SBÜ tarafından yeterli önlemler alınarak ve personelin özel hayatına saygı hakkı korunarak, orantılı olmak kaydıyla personelin e-posta aktivitelerinin izlenmesi gibi tedbirlere başvurulabilecektir.

Yaptırım

Bu politikaya uygun olarak çalışmayan tüm personel hakkında Disiplin Prosedürü hükümleri uygulanır.

11. FİZİKSEL GÜVENLİK POLİTİKASI

11.1. AMAÇ

Bu politika, SBÜ'nin hassas, gizli ve kritik kurumsal ve kişisel verilerin korunması amacıyla sistem odasına, kurumsal bilgilerin ve kişisel verilerin bulundurulduğu sistemlerin yer aldığı tüm çalışma alanlarına ve SBÜ binalarına yetkisiz girişlerin yapılmasını önlemek amacıyla kurallar çerçevesi oluşturmaktır.

11.2. KAPSAM

SBÜ binalarında yer alan bilgi varlıklarının bulunduğu fiziksel alanları ve çevresel güvenlik konularını, tüm personeller, sözleşmeli personeller, tedarikçiler, üçüncü kişileri ve diğer tüm ziyaretçiler için geçerlidir.

11.3. SORUMLULUK

Bilgi İşlem Dairesi Yetkilisi

İdari İşler Dairesi

11.4. TANIMLAR

Harici bir tanım olmadığı için eklenmemiştir.

11.5. İLGİLİ DOKÜMANLAR

Fiziksel ve Çevresel Güvenlik Prosedürü

Erişim Politikası

11.6. UYGULAMA

Fiziksel güvenlik kontrolleri, aşağıdakilerle sınırlı kalmamak koşulu ile "Fiziksel ve Çevresel Güvenlik Prosedürü" ve "Erişim Politikası"nda belirtilen güvenlik önlemlerine dikkate alınarak uygulanır:

SBÜ binası dış ve çevresel tehditlere karşı CCTV güvenlik kameraları ile izlenir ve güvenlik personeli tarafından korunur.

Sunucu odalarına/alanlarına fiziksel erişim tamamen kontrol edilir ve sunucular sunucu kabinetlerinde kilit altında tutulur.

Sunuculara erişim, yalnızca belirlenmiş Bilgi İşlem Dairesi personeli ile sınırlandırılır. Bunların dışında herhangi bir kişi tarafından geliştirme alanından sunucular üzerinde çalışmak istenirse, sunuculara yalnızca Kısıtlı Kullanıcı Hesabı ile Uzak Masaüstü Bağlantısı üzerinden bağlanılır.

Kritik yedekleme ortamı yanmaz bir kasada tesis dışında bulunan konumda tutulur.

Yetkisiz fiziksel erişimi, hasarı ve müdahaleyi önlemek için bilgi sistemleri içeren alanları korumak için güvenlik çevreleri geliştirilir.

Bilgi sistemlerinin bulunduğu tesislere yetkili erişimi olan personelin listesi, uygun yetkilendirme bilgileriyle birlikte muhafaza edilir. Erişim listesi ve yetkilendirme bilgileri, periyodik olarak yetkili personel tarafından gözden geçirilir ve onaylanır.

Bilgi sistemlerinin bulunduğu tesislere tüm fiziksel erişim noktaları (belirlenmiş giriş/çıkış noktaları dahil) kontrol edilir ve erişim yetkisinin doğrulanmasından sonra kişilere erişim sağlanır.

Fiziksel güvenlik olaylarını tespit etmek ve bunlara müdahale etmek için bilgi sistemlerine fiziksel erişimler izlenir.

Yangın, sel, deprem, patlama, sivil kargaşa ve diğer doğal ve insan kaynaklı afetlerden kaynaklanan hasarlara karşı fiziksel koruma tasarlanır ve uygulanır.

Bilgi sistemleri ve bileşenleri, fiziksel ve çevresel tehlikelerden kaynaklanan riskleri ve yetkisiz erişim fırsatlarını en aza indirecek şekilde tesis içinde konumlandırılır.

Bilgi sistemleri, elektrik kesintilerinden ve destekleyici tesislerdeki bir arızanın neden olduğu diğer kesintilerden korunur.

Veri taşıyan veya bilgi hizmetlerini destekleyen güç ve telekomünikasyon kabloları, kesintiye veya hasara karşı korunur.

Bilgi sistemlerine fiziksel erişim kontrolü, kurum binasına fiziksel erişim kontrolünden bağımsızdır. Bu kontrol, daha yüksek etki düzeyine sahip sunucu odaları veya bilgi sistemleri için geçerlidir.

Uygun müdahale eylemlerini başlatmak ve olası izinsiz girişleri tanımak için otomatik mekanizmalar kullanılır.

Hazırlayan	Kontrol eden	Onaylayan

Üçüncü kişilerin sistem odasına fiziksel erişimine izin verilmeden önce kimliklerinin doğrulanması yapılır.

Ziyaretçilere görevlendirilen personel eşlik eder ve gerektiğinde faaliyetleri izlenir.

Sistem personeli, en son anti-virüs tanımı, en son yamalar ve güncellemeler ve ağa zarar verebilecek her türlü güvenlik açığı için ziyaretçilerin dizüstü bilgisayarlarını inceler.

Resmi iş için harici ağa bağlanması gereken herhangi bir kullanıcı, Bilgi İşlem Dairesi Müdürü 'nden resmi bir onay aldıktan sonra bağlantı yapabilir.

Hem ziyaretçiler hem de yetkili kişiler tarafından yapılan tüm fiziksel erişimlerin kaydı tutulur.

Ziyaretçilerin kuruma girişi ve/veya kurye teslimatları yetkili görevliler gözetiminde yapılır.

Kullanılmadıkları durumlarda çalışma alanları kilitli ve kontrol altında tutulur.

Yetkisiz kişilerin güvenli alanlara, fotoğraf, video, ses vb. kayıt cihazları ile girmesi yasaktır.

12. KRİPTOGRAFİK KONTROLLER POLİTİKASI

12.1. AMAÇ

Bu politika, kriptografik kontrollerin kullanımı için pratik yönergeler içerir.

Hazırlayan	Kontrol eden	Onaylayan

12.2. KAPSAM

SBÜ BGYS kapsamı dahilinde Bilişim alt yapısında işlenen kişisel veriler, gizli ve hassas verilerin kurum içinde dolaşımını kapsar.

12.3. SORUMLULUK

Bilgi İşlem Dairesi Yetkilisi

Bilgi İşlem Dairesi Personeli

12.4. TANIMLAR

Kriptografi: Verileri yalnızca amaçlananların okuyabileceği ve işleyebileceği bir biçimde depolama ve iletme yöntemi.

Şifreleme: Verileri düz metinden, şifreli metin olarak bilinen yetkisiz taraflarca okunamayacak bir forma dönüştürme işlemi.

Anahtar: Şifreleme ve parola çözme sürecini kontrol eden giriş. Kriptografide kullanılan hem gizli hem de açık anahtarlar vardır.

Dijital Sertifika: Elektronik işlemler yapılırken sertifika sahibinin kimliğini doğrulamak için kullanılan elektronik belge. SSL sertifikaları, İnternet'teki bir sunucu hakkındaki verileri ve ayrıca sahiplik makamının genel şifreleme anahtarını tanımlayan yaygın bir örnektir.

Dijital İmza Sertifikası: Bir mesajı gönderenin veya bir belgenin sahibinin gerçek olduğunu ve mesajın veya belgenin bütünlüğünün bozulmadığını kanıtlayan bir tür dijital sertifika. Dijital imza sertifikası, asimetrik şifreleme kullanır ve birinin el yazısı imzasının veya bilgisayar tarafından oluşturulan el yazısı imzasının (diğer adıyla elektronik imza) taranmış bir sürümü değildir.

SSH Anahtarları: SSH sunucularının kimliğini doğrulamak ve güvenli bir ağ bağlantısı kurmak için kullanılan genel/özel anahtar çifti.

S/MIME: e-postalarınızı şifrelemenizi sağlayan bir teknolojidir. S/MIME, e-postalarınızı istenmeyen erişimden korumak için asimetrik şifrelemeye dayanmaktadır.

Hazırlayan	Kontrol eden	Onaylayan

Gizlilik: Saklanan veya iletilen hassas veya kritik bilgileri korumak için bilgilerin şifrelenmesi

Bütünlük: Saklanan veya iletilen hassas veya kritik bilgilerin gerçekliğini veya bütünlüğünü doğrulamak için dijital imza sertifikaları veya mesaj doğrulama kodlarının kullanılması

İnkâr Edilemezlik: Bir olayın veya eylemin meydana geldiğine dair kanıt sağlamak için kriptografik tekniklerin kullanılması

Kimlik Doğrulama: Sistem kullanıcıları, varlıklar ve kaynaklarla erişim talep eden veya bunlarla işlem yapan kullanıcıların ve diğer sistem varlıklarının kimliğini doğrulamak için kriptografik teknikler kullanılması

12.5. İLGİLİ DOKÜMANLAR

Bilgi Güvenliği İhlal Olay Yönetimi Prosedürü

Olay Bildirim Formu

12.6. UYGULAMA

Şifreleme, verileri yetkisiz kişilerce okunamaz ve erişilemez hale getirmek için dönüştürerek çalışır. Şifrelenmiş verileri okumanın tek yolu bir parola çözme anahtarı kullanmaktır. SBÜ, şifrelemeyi şu amaçlar için kullanır:

Bilgi ve verilerin saklanırken güvenliğini sağlamak

İşlenmiş ve kullanılan veriler

Kullanıcı kimlik bilgilerini (parolalar/oturum açmalar) korumak

Güvenli iletişim ve bağlantıları etkinleştirmek

Doğrulama, kimlik doğrulama, tanımlama ve doğrulamayı etkinleştirmek

Bilgi Teknolojileri sistemleri ve cihazlar arasında güvenli geçici internet/ağ bağlantıları

12.7. MASAÜSTÜ VE DİZÜSTÜ BİLGİSAYARLAR

Masaüstleri ve dizüstü bilgisayarlar, SBÜ genelinde en yaygın kullanılan bilgi işlem cihazlarıdır. SBÜ'nün bu cihazlarda hiçbir verinin saklanmaması politikasına rağmen, Kullanıcılar tarafından bilerek veya bilmeyerek verilerin saklanmasına neden olabilecek durum ve olaylar olmaya devam etmektedir. Dizüstü bilgisayarların taşınabilir doğası, hırsızlık ve/veya kayıp riskini artırır, ancak daha da önemlisi, verilerin kaybolması veya ifşa edilmesi riskini artırır.

Bu riskleri ele almanın en etkili ve uygun yolu, aşağıdaki yöntemleri kullanarak bu cihazları şifreleme ile korumaktır:

Masaüstü ve dizüstü bilgisayarlara yüklenen işletim sistemi görüntüleri, 128 bit anahtarlı simetrik anahtar şifrelemesi kullanılarak minimum AES 128 bit (Gelişmiş Şifreleme Standardı) ile yapılandırılır.

Masaüstü ve dizüstü bilgisayarlarda kullanılan şifreleme, rastgele bir şifreleme anahtarının oluşturulmasına ve ilgili anahtarın SBÜ Aktif Dizininde (AD) saklanmasına izin vermelidir.

Masaüstü ve dizüstü bilgisayarlar için şifreleme oluşturma işlemi sırasında, ana kartta Güvenilir Platform Modülü (TPM) yongası olduğu doğrulanır. TPM yongası mevcutsa, şifreleme oluşturma işlemi için TPM işlevi etkinleştirilir ve buna göre şifreleme işlemi başlatılır:

TPM yongası tarafından rastgele bir anahtar oluşturulur

Şifreleme anahtarları Active Directory 'ye geri yazılır.

SBÜ'nün bilgisayar ağı kullanılamaz hale gelirse (AD 'de saklanan anahtarlar) için düzeltme teknikleri mevcuttur. Bilgisayarların tanımlanması ve yöntemlerin kullanılmasını sağlamak için AD 'de bu bilgisayarlar için şifreleme anahtarlarının depolanması başlatılır.

Bir masaüstü veya dizüstü bilgisayarda yerleşik bir TPM yongası yoksa şifreleme anahtarının oluşturulabileceği bir USB anahtarı kullanılarak yapının şifreleme işlemine devam etmesine izin verilir.

Şifreleme anahtarlarının AD 'ye hemen yazılması mümkün değilse, işlemin ardından uygun şekilde saklanması gereken anahtarın

ortamına yazılmasına izin verilir.

Tüm masaüstü ve dizüstü bilgisayarlar en son güvenlik ve işletim sistemi yamalarıyla güncellenir, çünkü bu güncellemeler şifreleme yazılımında keşfedilen kusurlara veya güvenlik açıklarına yönelik güvenlik yamalarını içerebilir.

12.8. MOBİL CİHAZLAR VE TAŞINABİLİR DEPOLAMA ORTAMLARI

Mobil Cihazlar ve Taşınabilir depolama ortamları için aşağıdaki önlemler alınmıştır:

Mobil cihazlar

SBÜ tarafından sağlanan tüm cep telefonları, en az altı karakter içeren bir pin kodu kilidinin kullanımını zorunlu kılacak şekilde yapılandırılır. Bir cep telefonunun güvenliğini sağlamak için tek başına bir PIN kullanılması şifreleme teşkil etmese de, mobil cihaz şifrelemesini desteklemede hayati bir rol oynar.

Kullanıma yetkili ve kişisel olarak tanımlanabilir verileri işleyebilen ve SBÜ tarafından yönetilen mobil uygulamalar, verileri korumak için şifreleme kullanmalıdır.

SBÜ tarafından kullanılması uygun görülen Uygulamalar, internet veya herhangi bir belirtilmemiş ağ bağlantısı üzerinden iletişim kurarken TLS/HTTPS gibi güvenli şifreli iletişim protokollerini kullanır.

Bilgi Transferi ve Taşınabilir Depolama Ortamı

Bilgi Transferi için SBÜ gerektiğinde, şifreli USB bellekleri sağlar. Bu depolama aygıtları yalnızca verilerin geçici olarak depolanması içindir. SBÜ, aşağıdaki koşullar altında USB belleklerin (ve benzer depolama cihazlarının) kullanımına izin verir:

Kullanıcılar, taşınabilir cihaza erişmek için bir parola belirler.

Taşınabilir cihazların parolası, SBÜ'nün parola politikasına uygun olarak belirlenir.

Şifreli USB belleklerde (veya benzer depolama cihazlarında) saklanan SBÜ verileri, mümkün olan en kısa sürede SBÜ'nün bilgisayar ağındaki uygun ve güvenli bir alana aktarılmalıdır. USB belleklerde veya taşınabilir cihazlarda BIRAKILMAMALIDIR.

Cihazlara verilen parolalar bölüm yöneticileri tarafından bilinmelidir. Böylece bir kişinin SBÜ'den ayrılması durumunda SBÜ'nün verilerine erişim sağlanabilir.

Diğer taşınabilir USB aygıtları arasında cep telefonları, kameralar vb. bulunur. Bu diğer aygıtlar SBÜ verilerini depolamak için kullanılmamalıdır.

Kişisel USB bellekler veya harici diskler SBÜ ağına BAĞLANMAMALI ve SBÜ verilerini depolamak için KULLANILMAMALIDIR.

İnternet

SBÜ kurum işleri için interneti kullanırken bağlantıları şifreleyerek, parolaları ve verileri korumaya yardımcı olan, HTTPS siteleri kullanılmalıdır.

E-Posta

Özel nitelikli kişisel veriler, kişisel veriler, hassas veriler, çok gizli ve gizli olarak nitelendirilen veriler e-posta ile gönderilirken mutlaka şifrelenerek gönderilmelidir. E-posta hizmeti tüm uzak bağlantılar için Aktarım Katmanlı Güvenliği (TLS) kullanan giden e-posta için şifrelemeyi ve gelen Basit Posta Aktarım Protokolü (SMTP) oturumları için TLS şifrelemesini destekler. Giden iletilerin içeriği ve eklerini korumak için S/MIME şifrelemesi kullanılmalıdır.

Anahtar Yönetimi

Şifreleme kullanılırken dijital anahtarların korunması çok önemlidir. Şifreleme Anahtarı Yönetimi, doğru şekilde yapılmazsa, hassas verilerin güvenliğini sağlamak için özel anahtarların kullanımının tehlikeye atılmasına ve ifşa edilmesine ve dolayısıyla verilerin tehlikeye atılmasına neden olabilir. Kullanıcılar belirli belgeleri ve elektronik iletişimleri şifrelemenin önemli olduğunu anlayabilirler, ancak koruma şifreleme anahtarları için minimum standartlara aşina olmayabilirler.

Anahtar yönetiminin ilk yönü anahtarları oluşturmaktır. Kullandığınız herhangi bir anahtar tahmin edilebilir olmamalıdır. Bir diğer önemli husus, anahtarların güvenli bir şekilde saklanmasıdır. Anahtarlar, erişimin kısıtlanacağı şekilde saklanmalıdır. Anahtarların SBÜ'de halka açık bir yerde saklanması veya anahtarların tüm geliştiricilerin erişebileceği kaynak koduna yerleştirilmesi kabul edilemez.

Bu politika kapsamındaki tüm şifreleme anahtarları, izinsiz ifşa edilmelerini ve müteakip hileli kullanımlarını önlemek için korunmalıdır.

Gizli Anahtar Şifreleme Anahtarları

Simetrik şifreleme olarak da adlandırılan gizli anahtar şifrelemesi için kullanılan anahtarlar, onları kullanacak tüm taraflara dağıtıldıkları için korunmalıdır. Dağıtım sırasında simetrik şifreleme anahtarları, en az 2048 bitlik bir RSA anahtarı kullanılarak şifrelenir. Bu hem SSH hem de HTTPS kullanılırken standart OpenSSL kitaplıkları kullanılarak gerçekleştirilir, bu da uygun anahtar değişimi ve depolama sağlar.

Genel Anahtar Şifreleme Anahtarları

Genel anahtar şifrelemesi veya asimetrik şifreleme, genel-özel anahtar çiftlerini kullanır. Açık anahtar, son kullanıcıya verilen dijital sertifikaya dahil edilmek üzere sertifika yetkilisine iletilir. Dijital sertifika, yayınlandıktan sonra herkes tarafından kullanılabilir.

Özel anahtar, yalnızca ilgili dijital sertifikanın verildiği son kullanıcı tarafından kullanılabilir olmalıdır.

Kayıp ve Hırsızlık

Bu politika kapsamındaki herhangi bir şifreleme anahtarının kaybolması, çalınması veya olası yetkisiz ifşası durumunda, "Olay Bildirim Formu" doldurulur ve "Bilgi Güvenliği İhlal Olay Yönetimi Prosedürü" uygulanır. Bilgi Teknolojileri Birimi'ndeki yetkili personel daha sonra sertifikaların veya genel-özel anahtar çiftlerinin iptali ile ilgili olarak gerekli olacak uygun eylemleri uygulamalıdır.

13. ÜÇÜNCÜ TARAF GÜVENLİK POLİTİKASI

13.1. AMAÇ

Bu politikanın amacı SBÜ'nün bilgi varlıklarına ve sistem odalarına üçüncü taraflar tarafından ulaşılması durumunda güvenliğini sağlamaktır.

13.2. KAPSAM

SBÜ'nün bilgi varlıklarına ve sistem odalarına erişişim sağlayan üçüncü tarafları ve personelini kapsar.

13.3. SORUMLULUK

Bilgi İşlem Dairesi Yetkilisi

Bilgi İşlem Dairesi Personeli

13.4. TANIMLAR

Harici bir tanım belirtilmediği için eklenmemiştir.

13.5. İLGİLİ DOKÜMANLAR

Üçüncü Taraf Gizlilik Sözleşmesi

Bilgi Güvenliği Politikası

Hazırlayan	Kontrol eden	Onaylayan

Uzaktan Erişim Politikası

Uzaktan Erişim Kayıt Formu

13.6. UYGULAMA

SBÜ varlığına bağlanan veya onu kullanan (sunucular, iş istasyonları, altyapı, internet ağ geçidi veya ağ dahil) tüm sağlayıcılar, SBÜ'nün geçerli tüm kullanım koşullarına, politikalarına, standartlarına ve prosedürlerine uymalıdır. Üçüncü tarafların SBÜ'nün varlıklarını akıllıca korumaları ve kullanmaları gerekmektedir ve SBÜ'nün sistemleri, bilgisayarları, telefonları, internet erişimi, e-posta, yazıcıları, fotokopi makineleri, faks makineleri, araçları veya diğer mülkleri dahil olmak üzere SBÜ'nün varlıklarını kullanırken sağduyulu ve hassas davranacaktır.

Üçüncü taraflar, SBÜ'nün doğrudan yazılı onayı olmadan asla SBÜ'ye ait olmayan varlıkları kurum ağına bağlamamalıdır.

SBÜ ağına bağlanan varlıklar, yapılandırma, yama, erişim kontrolü ve virüs koruma süreçleri dahil ancak bunlarla sınırlı olmamak üzere SBÜ'nün güvenlik Politikaları, Standartları, İşletim uygulamaları ve kontrollerine uymalıdır.

Üçüncü taraflarla ilgili çalışmalarda aşağıdaki hususlar dikkate alınmalıdır;

Kurum dışından gelen bakım ve destek personeli ile diğer tedarikçilerde de olduğu gibi, kurum içinde olduğu süre boyunca bir gizlilik anlaşması imzalanır.

Kurum dışından gelen üçüncü taraflar ve personeller kurumun bilgi güvenliği politikası ve güvenlik politikalarına uymakla yükümlüdür.

Kurumun bilişim varlıklarına erişim yetkisi tanımlanması durumunda, erişimi yapacak yetkili, Uzaktan Erişim Kayıt Formu doldurulduktan sonra uzaktan erişim izni aktif hale getirilir. Uzaktan erişim yapacak üçüncü taraf firmalar için Uzaktan Erişim Politikası uygulanır.

Kurum içinde kullanılan telefon rehberleri üçüncü tarafların eline geçmemelidir.

Sadece uygun yetkileri almış olan personellerin organizasyonun bilgi veya iletişim sistemlerine erişimi vardır.

Üçüncü taraflarla herhangi bilgi alışverişi yapılmadan önce bir KVKK hükümlerini içeren gizlilik anlaşması yapılır.

Üçüncü taraflara kurumun bilişim ağına erişim izni verilmeden önce bilgisayarlarında güvenlik yazılımları bulundurmaları gerekir. Kurum, üçüncü taraflara herhangi bir uyarıda bulunmadan ağa olan erişimlerini kesebilir.

Kurum isminin halka yayınlanacak dokümanlarda kullanılabilmesi için üçüncü tarafların uygun kişiler tarafından yetkilendirilmesi gerekir.

Sadece yetkilendirilmiş tedarikçiler, kurumla çalışmakta olduklarını veya yapmakta oldukları işin doğasını halka yayabilirler.

Tedarikçiler kurum sistemlerine erişmeden önce koşulların tanımlanmakta olduğu bir anlaşma imzalanır.

Gizli bilgilerin dağıtımını içeren kurallar belirlenir ve üçüncü taraflara bu bilgiler iletilmeden önce taraflarla bu kurallar hakkında anlaşılır.

14. AĞ YÖNETİMİ POLİTİKASI

14.1. AMAÇ

Bu politikanın amacı, kurumun bilişim ağ altyapısının bakımı, yönetimi, genişletilmesi ve kullanımına ilişkin kuralları oluşturmak, kablosuz altyapı cihazlarının SBÜ ağına bağlanmak için karşılaması gereken teknik gereksinimleri ve kurum ağındaki yönlendirici (router) ve anahtarların (switch) sahip olması gereken minimum güvenlik konfigürasyonlarını tanımlamaktadır.

14.2. KAPSAM

SBÜ bilgisayar ve sistem ağ altyapısının yapılandırılması, bakımı veya genişletilmesinde yer alan kişileri ve ağ cihazlarını kapsar.

14.3. SORUMLULUK

Bilgi İşlem Dairesi Yetkilisi

Bilgi İşlem Dairesi Personeli

14.4. TANIMLAR

Virtual Private Network (VPN): Sanal özel ağ. Herkese açık olan iletişim altyapısını kullanan özel bir veri ağıdır. Tünel protokolü ve çeşitli güvenlik prosedürleri ile izinsiz girişlere karşı korunur.

VLAN (Virtual LAN): Sanal yerel ağ. Birçok farklı ağ bölümüne dağılmış olan, ancak aynı kabloya bağlıymışlar gibi birbiri ile iletişim kurmaları sağlanan, bir veya birkaç yerel ağ üzerindeki cihazlar grubu.

Yönlendirici (router): Bir veya daha fazla bilgisayar ağı arasında bir yol tesis eden fonksiyonel birim.

Anahtar (switch): Her frame'in hedef adresine dayanarak frame'leri filtreleyen ve ileten ağ cihazı. Anahtar, OSI modelinin veri bağlantı katmanı olarak çalışır.

Source routing: Bilgisayar ağında, yol adresleme olarak da adlandırılan kaynak yönlendirme, bir paket göndericisinin paketin ağ üzerinden geçtiği yolu kısmen veya tamamen belirtmesine olanak tanır.

IP directed broadcasts: Yönlendirilmiş broadcast olarak adlandırılan bu adres, ağdaki en yüksek adresi kullanır; bu, tüm host bitlerinin 1 olduğu adrestir.

SNMP (Simple Network Management Protocol): Özellikle TCP/IP ağlarında kullanılan ağ yönetim protokolu. Ağ cihazlarının izlenmesi ve kontrolünü, konfigürasyonların, istatistik işlemlerinin, performansın ve güvenliğin yönetimini sağlar.

Community string: SNMP'de iletişim için parola yerine geçen Community Stringler kullanır.

Firmware: Salt okunur olarak yalnızca okunabilir olan ve silinmeyen, sadece güncelleme başta bilgisayar aygıtları olmak üzere birçok elektronik ürünün içerisinde bulunarak tüm bu çevre birimlerinin görevleri ve işlevlerinin ne olduğunu söz konusu donanımlara bildiren küçük bir yazılımdır.

UTP kablo: Unshielded Twisted Pair ya da Türkçe olarak Korumasız Bükümlü Kablo, dokuz tür olarak üretilen analog veri iletim kablolarından biridir. UTP kabloda veriler bakır teller üzerinden analog sinyaller halinde gönderilir. Sağladıkları bant genişliklerine göre kendi içinde dokuz türe ayrılır. Ethernet protokülünün fiziksel katmanında en çok kullanılan kablo türüdür.

WPA2 (Wi-Fi Protected Access2): Kablosuz Korumalı Erişim Şifreleme türüdür. Kablosuz bağlantılar üzerinde güvenliği sağlayan ve aktarımların şifrelenerek gerçekleşmesine yardımcı olan bir güvenlik protokolüdür. Şu an için Wi-Fi güvenliği konusunda en çok tercih edilen ve en az güvenlik zafiyetine sahip olan şifreleme türüdür.

SSID (Service Set Identifier): Kablosuz ağların veya bağlantı noktalarının (Hotspot) kimliğini tanımaya ve giriş yapmaya yardımcı olan isimlerdir. SSID bir diğer değişle "Wi-Fi ağının adı" dır.

14.5. İLGİLİ DOKÜMANLAR

Parola Politikası

Uzaktan Erişim Politikası

14.6. UYGULAMA

SBÜ'nün bilişim ağ alt yapısı Bilgi Teknolojileri Birimi tarafından izlenmeli ve kontrol edilmelidir.

1. Ağ Cihazları Yönetimi

Hazırlayan	Kontrol eden	Onaylayan

SBÜ'nün, ağ altyapısının sahibidir ve bundan sorumludur ve altyapıda daha fazla gelişme ve iyileştirmeyi yönetmeye devam edecektir.

Yeni ağ geliştirme gelişmelerinden yararlanabilecek tutarlı bir ağ altyapısı sağlamak için tüm kablolama Bilgi İşlem Dairesince veya onaylı bir yüklenici tarafından yapılır.

Bilgi güvenliği gereksinimleri, herhangi bir yeni bilgi sistemine veya mevcut sistemdeki iyileştirmelere dahil edilir.

Gizli bilgileri yetkisiz aktarım, değişiklik veya ifşadan korumak için uygun teknik çözümler uygulanır (yani yeni nesil güvenlik duvarları, IDS/IPS, DLP).

Ağın kontrol edeceği alan belirlenir.

Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için özel kontroller uygulanır.

Ağ servisleriyle ilgili standartlarda, erişimine izin verilen ağlar ve ağ servisleri ve ilgili yetkilendirme yöntemleri belirtilir.

Ağ üzerinde kullanıcının erişeceği servisler kısıtlanır.

Sınırsız ağ dolaşımı engellenir.

İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden teknik önlemler alınır.

Ağ erişimi gerek duyulduğunda VPN, VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılır.

Harici bağlantılar dahil olmak üzere ağ ve veri akışının bir haritası veya diyagramı muhafaza edilir. Bu harita veya diyagram, ağda herhangi bir değişiklik meydana geldikten sonra güncellenir. Bu diyagram, ağ mimarisini temsil etmeye devam etmesini sağlamak için her 6 ayda bir gözden geçirilir.

Hazırlayan	Kontrol eden	Onaylayan

Ağdaki tüm sistemlerin kimliği doğrulanır. Ağa bağlantılar Bilgi İşlem Dairesi Personeli tarafından yetkilendirilir.

SBÜ'nün ağına bağlı tüm donanımlar Bilgi İşlem Dairesi yönetim ve izleme standartlarına tabidir.

Gizli veya dahili bilgileri oluşturan, toplayan, depolayan ve/veya işleyen tüm Bilgi Kaynakları için belgelenmiş temel yapılandırmalar sürdürülmeli ve ağa bağlı tüm kaynaklar bu spesifikasyonlara göre yapılandırılır.

Gerekli sistem performansını sağlamak için kaynak kullanımı izlenir.

Bilgi işleme tesisleri, kullanılabilirlik gereksinimlerini karşılamak için yeterli fazlalığı ele alır.

Aktif ağ yönetim cihazlarının konfigürasyonunda değişiklikler "Değişikli Yönetimi Prosedürü" 'ne göre yapılır.

SBÜ'nün ağ altyapısı, iyi tanımlanmış bir dizi onaylanmış ağ protokolünü destekler. Onaylanmamış protokollerin herhangi bir şekilde kullanılması Bilgi Teknolojileri Birimi tarafından onaylanır.

Ağ altyapısının harici üçüncü taraf ağlara olan tüm bağlantıları Bilgi Teknolojileri Biriminin sorumluluğundadır.

Bilgi hizmetleri grupları, kullanıcılar ve bilgi sistemleri ağ üzerinde ayrılır. Her etki alanının çevresi iyi tanımlanmalı ve ilgili güvenlik gereksinimlerine dayanmalıdır.

Ağ cihazları SBÜ uygulama standartlarına göre kurulur ve yapılandırılır.

SBÜ Bilgi Teknolojileri Biriminden yazılı izin alınmadan birim ağ cihazlarının kullanımına izin verilmez.

Personelin mevcut ağ donanımına hiçbir şekilde erişmesine veya bunları değiştirmesine izin verilmez.

Hazırlayan	Kontrol eden	Onaylayan

2. Kablosuz ağ

Ağa bağlantı sağlayan kablosuz cihazlar ve ağa kablosuz bağlantı sağlayan tüm kablosuz altyapı cihazları, SBÜ ağına bağlanan notebook, masa üstü pc, cep telefonları ve tabletler dahil ancak bunlarla sınırlı olmamak üzere uç nokta cihazlarına kablosuz bağlantı sağlayan tüm kablosuz altyapı cihazları için geçerlidir.

SBÜ kablosuz ağına erişim sağlayan tüm kablosuz erişim noktaları veya cihazlar yönetim tarafından onaylanmalıdır.

Kablosuz erişim cihazları herkesin ulaşamadığı yerlerde konumlandırılır ve güvenliği sağlanır.

Kablosuz erişimde Wi-Fi Protected Access (WPA2, WPA3) şifreleme kullanılır.

Kablosuz ağlar uygun teknik kontroller kullanılarak bölümlere ayrılır.

Kimlik doğrulama ayarları (parolalar, şifreleme anahtarları vb.), bu tür bilgilerin güvenliğinin ihlal edildiğinden şüphelenildiğinde veya bilgiye sahip herhangi birinin kuruluştan ayrılması durumunda olduğu gibi periyodik olarak değiştirilir.

Tüm kablosuz ağ trafiği, bilgi duyarlılığına bakılmaksızın SBÜ Şifreleme Politikası ve destekleyici standartlara uygun olarak şifrelenmelidir.

Donanım üreticisi tarafından çıkarılan firmwareler güvenlik ile ilgili yamaların uygulanması açısından düzenli olarak güncellenir.

Kablosuz cihazlar için varsayılan ayarları (örneğin; parolalar, kablosuz şifreleme anahtarları, SNMP topluluk dizileri vb.), cihazı kurmadan önce değiştirilir.

Kablosuz cihazların yönetimi ve kontrolü için kurumun Parola Politikasına uygun parolalar belirlenir.

Varsayılan SSID isimleri kullanılmaz ve SSID ismi içerisinde SBÜ ile ilgili bilgi kullanılmaz.

Kablosuz ağ ile sağlanan İnternet çıkışları Firewall üzerinden sağlanır.

Kullanıcı bilgisayarlarında antivirüs yazılımı ve işletim sistemi ile birlikte gelen güvenlik duvarı yazılımı yüklü ve açıktır.

Hem kullanıcı bilgisayarlarında hem de kablosuz erişim cihazlarında statik ip adresleri kullanılır.

SBÜ ağındaki tüm ağ cihazları ve kablosuz ağ erişim cihazları ağ yönetimi yazılımı ile devamlı olarak izlenir.

Wireless ağlarında WPA2, WPA3 şifreleme metodu kullanılmaktadır. Kullanıcılar misafir ağına giriş yaparken ortak belirlenen birinci parola ve SMS ile cep telefonuna gelen ikinci parolayı girerek misafir ağına giriş yaparlar.

SBÜ Kablosuz Ağı uygunsuz şekilde kullanılmamalıdır; özellikle, kullanıcılar ağı şu amaçlarla kullanmamalıdır:

Gizli dinleme amacıyla diğer kablosuz iletimleri engellemek veya engellemeye çalışmak.

Ağın genel performansını olumsuz etkileyebilecek veya ağa erişimi engelleyebilecek yardımcı programlara veya hizmetlere erişin veya çalıştırın, örneğin RF sıkışması, Hizmet Reddi (DoS).

SBÜ kablosuz ağ kullanıcıları, ağ erişim noktalarını veya güvenlik ayarlarını değiştirmemelidir.

Kullanıcılar başka bir kablosuz ağa ve SBÜ kablosuz ağına aynı anda bağlanmamalıdır.

SBÜ kablosuz erişim noktalarının kontrolünü yaparak en az üç ayda bir tüm yetkili ve yetkisiz kablosuz erişim noktalarını belirler.

14.7. 3 VPN

VPN ile kurum ağına bağlanacak kurum dışı hizmet alınan firmalar, personeller, sözleşmeliler, danışmanlar, geçici personeller ve diğer bütün personeli için geçerlidir.

SBÜ birim yöneticileri tarafından onay verilen kullanıcılar ve Bilgi İşlem Dairesi Personeli SSL VPN ile kurum ağına bağlantı sağlayabilirler.

Buna ek olarak,

Yetkisiz kullanıcıların uzaktan SBÜ dahili ağlarına erişmesine izin verilmez.

Kurum sistemlerine uzaktan erişim için Uzaktan Erişim Politikası uygulanır.

Kullanım ve erişim hakkı; güçlü kimlik doğrulama mekanizmaları kullanılarak kontrol edilir.

VPN bağlantıları SSL VPN teknolojisi kullanılarak ve SMS destekli iki faktörlü kimlik doğrulama kullanılarak sağlanır.

VPN bağlantılarında kullanılacak bağlantı parolaları kurumun Parola Politikasına uygun olarak oluşturulmalıdır.

Personel uygulamaları ile kullanıcı iş bilgisayarına gelen ve giden tüm internet trafiği VPN tüneli aracılığıyla iletilir, diğer tüm yerel ve internet trafiği kesilir.

Yalnızca bir ağ bağlantısına izin verilir, çift tünellemeye izin verilmez.

VPN ağ geçitleri yalnızca bilgi sistemleri sorumlu birimi tarafından kurulacak ve yönetilecektir.

VPN kullanıcıları, kişisel makinelerinin SBÜ ağının bir uzantısı olduğunu ve bu nedenle SBÜ'ye ait ekipman için geçerli olan aynı kural ve düzenlemelere tabi olduğunu anlamalıdır.

VPN aracılığıyla SBÜ dahili ağlarına bağlanan tüm bilgisayarlar, kurumsal standart olan en güncel anti-virüs yazılımını kullanmalıdır; buna kişisel bilgisayarlar da dahildir.

4. Ağ Cihazları Güvenliği

Aşağıdaki genel prosedürler ve protokoller, SBÜ'ye ait tüm yönlendirici (router) ve anahtarlara (switch) uygulanacaktır:

Kurum bilişim ağ altyapısında bulunan tüm ağ cihazlarının IP ve MAC adres bilgileri varlık envanteri dosyasına kaydedilir.

Tüm ağ cihazları kilitli kabinetler içerisinde bulundurulur ve erişim kontrolü sağlanır.

SBÜ ağında bulundurulan her router ve switch, uygun şekilde yapılandırılır ve kendi amaçları için güvenlik gereksinimlerini karşılar.

Ağ tabanlı erişim için ayrı kimlik doğrulama, yetkilendirme ve hesap kontrolü hizmetleri sağlamak için erişim kontrolü kullanılır.

Konfigürasyonlar, genel ağlar (örn. internet) ve herhangi bir dahili SBÜ ağı arasında doğrudan genel erişimi yasaklar.

Yapılandırmalar, güvenilmeyen ağlardan (misafir ve harici kablosuz bağlantılar dahil) ve ana bilgisayarlardan gelen ve giden tüm trafiği kısıtlar.

Güvenlik, gerekli protokoller dışında tüm diğer trafiği özellikle reddetmelidir.

Router üzerinde hiçbir yerel kullanıcı hesabı yapılandırılmayacak ve tüm router parolaları güvenli bir şekilde şifrelenmiş biçimde saklanır.

Tüm varsayılan ACL parolaları değiştirilir.

Parolalar, SBÜ Parola Politikasında belirtilen güçlü parolalardan oluşturulur.

Tüm ağ trafiği loglanır.

Router 'lar uzaktan yapılandırıldığında, Secure Shell (SSH) tercih edilen yönetim protokolüdür. Yönlendiriciler, asgari düzeyde aşağıdaki iletişim ve aktarımlara izin vermeyecek şekilde yapılandırılır:

IP yönlendirmeli yayınlar

Yönlendiricide geçersiz adreslerden kaynaklanan gelen paketler

TCP küçük hizmetleri

UDP küçük hizmetleri

Kaynak yönlendirme

Yönlendiricide çalışan web hizmetleri

Bilgisayar ağında bulunan kabinetler, aktif cihazlar, UTP kabloları, cihazların portları yetkisiz erişime yasaklanmış olması durumunda etiketlenir.

Etiket Bilgisi;

"BU CİHAZA YETKİSİZ ERİŞİMLER YASAKLANMIŞTIR. Bu cihaza erişim ve konfigürasyon olması için yasal hakkınız olmak zorundadır. Bu cihazla yapılan her şey loglanabilir, bu politikaya uymamak disiplin kuruluna sevk ile sonuçlanabilir veya yasal yaptırım olabilir.

15. GÜVENLİ YAZILIM GELİŞTİRME POLİTİKASI

15.1. AMAÇ

Bu politikanın amacı, SBÜ personelinden gelen talepler ya da eksikliği tespit edilen yazılım/otomasyon ihtiyacını karşılamak için üretilecek ve geliştirilecek yazılımların güvenli yazılım geliştirme süreçlerini belirleyen çerçeveyi oluşturmaktır.

15.2. KAPSAM

SBÜ bünyesinde üretilen tüm yazılım süreçlerini kapsar.

15.3. SORUMLULUK

Bilgi Teknolojileri Birimi Müdürü

Hazırlayan	Kontrol eden	Onaylayan

Tüm Bilgisayar Kullanıcıları

15.4. TANIMLAR

SDLC: Yazılım Geliştirme Yaşam Döngüsü (Software Development Life Cycle)

15.5. İLGİLİ DOKÜMANLAR

Harici bir doküman belirtilmediği için eklenmemiştir.

15.6. UYGULAMA

SBÜ personelinden gelen talepler ya da eksikliği tespit edilen yazılım/otomasyon ihtiyacını karşılamak için üretilecek ve geliştirilecek yazılımlar "Yazılım Geliştirme Prosedürü"nde belirtilen hususlar dikkate alınarak ve bu politika da belirtilen güvenli yazılım geliştirme adımları da dikkate alınarak gerçekleştirilir.

Yazılım Geliştirme Süreci

Güvenli yazılım geliştirme; yazılım geliştirme yaşam döngüsünün (SDLC) gereksinimler, tasarım, uygulama ve test gibi farklı aşamalarında güvenliğin entegre edilmesini içerir. Güvenlik gereksinimi mühendisliğinin temel görevi, güvenli yazılım sistemleri geliştirmek için gereken eylemleri belirlemek ve belgelemektir. Yazılım geliştirme yaşam döngüsünün güvenlik öğeleri şunları içermelidir:

Güvenlik gereksinimlerini ve hedeflerini karşılamayı planlama.

Tehdit modellemesi.

Güvenlik ve gizlilik endişelerini içerecek şekilde tasarımlar.

Sistem mimarisi (ör. web, uygulamalar, kullanıcı arayüzleri, dosya içe/dışa aktarma, raporlar, veri tabanları).

Belgeler

Değişiklik yönetimi

Hazırlayan	Kontrol eden	Onaylayan

Test planları oluşturma, test sonuçlarını inceleme ve düzeltmeleri ve yamaları onaylama dahil olmak üzere test etme.

Güvenli dağıtım uygulamaları ve görevlerin ayrılması.

Kod incelemesi ile ilgili olarak, koruma düzeyi yüksek veya erişilebilirlik düzeyi yüksek olarak sınıflandırılan kurumsal bilgileri işleyecek, depolayacak veya iletecek yazılım geliştiren birim:

Siber riski azaltmak için kod incelemeleri gerçekleştirmeli.

Genel güvenlik hatalarını göz önünde bulundurmalı ve kontrol edilmeli.

İnceleme sürecine kıdemli bir yazılım geliştiriciyi dahil edilmeli ve mümkünse bağımsız bir tane seçilmeli.

Spesifik güvenlik deneyimine sahip bir personeli inceleme sürecine dahil edilmeli.

Otomatik güvenli kod testi/kontrol araçları ile:

Statik kod analizi gerçekleştirilmeli.

Dinamik kod analizi gerçekleştirilmeli.

Girdi Doğrulama

Yazılım geliştiren Birim personeli:

Giriş verilerini programlı olarak kullanmadan önce kullanıcı girişini doğrulayın.

Kod yerleştirme saldırılarına karşı koruma sağlamak için geçersiz kullanıcı girişini temizleyin veya reddedin.

Kullanıcı için uyumlu ve güvenli girişi kolaylaştırmak için giriş doğrulama stratejisine kullanıcı arabirimi kontrollerini dahil edin.

Arabellek taşması saldırılarına karşı koruyun.

Dizi indeks hatalarına karşı koruyun.

Parametre manipülasyon saldırılarına karşı koruyun.

Parametreli SQL sorguları kullanın.

SQL enjeksiyon saldırılarına karşı savunun.

Tüm SQL kodunu/komutlarını sunucu tarafı koduna koyun.

Birleştirilmiş veri tabanı sorguları kullanmayın.

SQL'i istemci tarafı koduna koymayın.

Hassas bilgilerin önbelleğe alınmasını önlemek için HTML 'de Otomatik Tamamlama=kapalı olarak ayarlayın.

URL sorgu dizesi manipülasyon saldırılarına karşı koruyun. Yazılım geliştiren birim personeli, URL/URI 'de aşağıdaki bilgi türlerini kullanmamalıdır:

Kimlik bilgileri

Kayıt numaraları

İsimler, SGK numaraları, ehliyet numaraları veya doğum tarihleri).

İstisna ve Hata İşleme

Yazılım geliştiren Birim personelleri aşağıdaki hususlara dikkat etmelidir:

Çalışma zamanı ortamlarını, çerçeve hataları için ekrana/tarayıcıya özel hata sayfalarında yerel çerçeve hatalarını (örn.Net, J2EE) göstermeyecek şekilde yapılandırın.

Beklenen hataları ele alın ve sorunları gidermek için hata mesajlarında kullanıcılara/yönetim personellerine yeterli ayrıntı sağlayın.

İşlenmeyen hata olmaması için kod yazın.

Hazırlayan	Kontrol eden	Onaylayan

Asla boş yakalama blokları kullanmayın.

Yakalama bloklarının uygulamanın aşağıdakilerden en az birini yapmasına neden olduğundan emin olun:

Çalışmayı durdurun ve güvenli bir durumda çıkın.

İstisnayı uygun şekilde ele alın.

Ayrıntılı istisna ve hata mesajlarını uygulama olay günlüklerine kaydedin.

Siteler Arası Komut Dosyası Çalıştırma (XSS) ve Geçersiz Yönlendirmeler/İletmeler

Yazılım geliştiren Birim personelleri, güvenilmeyen verileri veya kodları bir web tarayıcısına göndermeden önce test etmelidir. Test, yaygın XSS saldırıları için uygun doğrulamayı içermelidir.

Güvensiz Doğrudan Nesne Referansları

Yazılım geliştiren Birim personelleri, herhangi bir nesneye, dosyaya, dizine veya veri tabanı anahtarına doğrudan nesne referanslarının bir erişim kontrolünü veya başka bir koruma içermesini sağlamalıdır.

Logging (Loglama)

Yazılım geliştiren Birim personelleri aşağıdaki hususlara dikkat etmelidir:

Kimlik doğrulama (başarılı veya başarısız), ayrıcalıklı işlevlerin kullanımı, yönetim etkinlikleri ve sistem/bileşen başlatma ve durdurma ile ilgili olayların loğlarını kaydedin.

Mümkün olduğunda güvenlikle ilgili olayları ayrı bir log dosyasına kaydedin. Bu işlem, geliştiricilere günlük dosyasıyla ilgili belirli kurallar (örneğin, özel roller/izinler, gözetim zinciri vb.) için ek esneklik sağlar.

Özellikle güvenlik olayları diğer uygulama olaylarıyla birlikte geliyorsa, günlük ayrıntılarındaki bilgileri sınırlayın (örneğin, hassas bilgileri günlüğe kaydetmeyin).

SIEM hizmeti veya bilgi güvenliği personelinin logları alabilmesi için dosya adlandırma kurallarını kullanın.

Mümkün olduğunda güvenlikle ilgili logları uygulamadan ayrı olarak saklayın.

Gerekli saklama süresi boyunca logları tutmak için yeterli depolama alanı bulunduğundan emin olun.

TLS ve Güvenli API 'ler

Yazılım geliştiren Birim personelleri aşağıdaki hususlara dikkat etmelidir:

Tüm tarayıcı bağlantıları için HTTPS 'i zorlayın.

HTTP 'yi devre dışı bırakın.

Makineden makineye bağlantıları korumak için TLS 1.2 veya üstünü kullanın (ör. uygulama sunucusundan veritabanı sunucusuna bağlantılar).

Gizli veya üzeri olarak sınıflandırılan kurumsal bilgileri ayrı ve benzersiz bir kimlik bilgisi anahtarı kullanarak şifreleyin.

Kullanılan şifreleme teknolojisinin Bilgi İşlem Dairesi Müdürü tarafından onaylandığından emin olun.

Yazılım, gizli veya daha yüksek olarak sınıflandırılan kurumsal bilgilerin iletimini içerdiğinde oturumu doğrulayın ve şifreleyin.

Kimlik Bilgileri/Parolalar

Yazılım geliştiren Birim personelleri aşağıdaki hususlara dikkat etmelidir:

Kullanıcı parolalarını asla kaydetmeyin.

Hizmet hesabı kimlik bilgilerini koruyun.

Kimlik bilgilerini asla sabit kodlamayın.

5 başarısız kimlik doğrulama girişiminden sonra kilitleme uygulayın.

Kimlik bilgileri veya diğer gizli değiş tokuşlar için güvenli protokolleri kullanın (ör. TLS 1.2 veya üstü).

Oturum ve Çıkış

Yazılım geliştiren Birim personelleri aşağıdaki hususlara dikkat etmelidir:

Oturum zaman aşımının uygulandığından emin olun.

Oturum belirteçlerinin rastgele ve uzun (GUID uzun) olduğundan emin olun.

Her oturum açmada ve her ayrıcalık yükseltmesinde oturumları değiştirin (eskiyi silin ve yeni oluşturun).

Çıkışta oturumları silin, kaldırın ve geçersiz kılın.

Tüm oturum tanımlama bilgileri için TLS 1.2 veya üstünü kullanın.

Bir çıkış işlevi sağlayın.

Uygulama boyunca oturum kapatma işlevini belirgin bir şekilde görüntüleyin.

Sunucudaki kayıtları düzgün bir şekilde kapatın, geçici nesneleri silin ve işlemleri kapatın:

Çıkış işleminin bir parçası olarak.

Belirli bir etkinlik dışı kalma süresinden sonra (örneğin, bir saatten az).

Bir tarayıcı penceresi kapandıktan sonra.

Güvenli Yapılandırma

Yazılım geliştiren Birim personelleri aşağıdaki hususlara dikkat etmelidir:

Yazılımı canlıya almadan önce güvenlik açığı taraması yapın ve riske dayalı bulguları uygun şekilde düzeltin.

Bir uygulamada kullanılan bileşenleri sabitleyin.

Bileşenleri mümkün olan en az ayrıcalıkla çalıştırın.

Bileşenleri yamalı ve güncel tutun.

SQL'i mümkün olan en az ayrıcalıkla çalıştırın.

Güvenlik ayarları tanımlayın, uygulayın ve koruyun (varsayılan ayarlara güvenmeyin).

Bir uygulamada kullanılan yazılım yapılandırmasını güvenli hale getirin.

Uygulamanın hangi HTTPS metodlarını (örneğin, Get - Al veya Post - Gönder) destekleyeceğini ve HTTPS yöntemlerinin uygulamanın farklı sayfalarında farklı şekilde ele alınıp alınmayacağını tanımlamak için yapılandırmayı ayarlayın.

Yaptırım

Bu politikaya uygun olarak çalışmayan tüm personel hakkında Disiplin Prosedürü hükümleri uygulanır.

16. GÜVENLİK AÇIKLARI TESPİT ETME POLİTİKASI

16.1. AMAÇ

Bu politikanın amacı SBÜ bilişim ağının (firewall, sunucu, son kullanıcı, switch, elektronik ve bağlantı ekipmanları vs.) güvenlik açıklarına karşı taranması hususunda politika belirlemektir.

16.2. KAPSAM

Bu politika SBÜ bünyesinde sahip olunan bütün bilgisayar ve ağ cihazlarını kapsamaktadır.

16.3. SORUMLULUK

Bilgi İşlem Dairesi Yetkilisi

Bilgi Teknolojileri Personeli

16.4. TANIMLAR

Harici bir tanım belirtilmediği için eklenmemiştir.

16.5. İLGİLİ DOKÜMANLAR

Gizlilik Sözleşmesi (Dış taraflar)

16.6. UYGULAMA

SBÜ bilişim ağında yapılacak olan güvenlik açıklıklarının tespit edilebilmesi için dışarıdan alınacak olan sızma testleri hizmeti kapsamında Bilgi Teknolojileri Birimi tarafından sızma testlerini yapacak kurum personellerine bilgi güvenliği gizlilik sözleşmesi imzalandıktan sonra gerekli erişim izni verilecektir. Bilgi Teknolojileri Birimi testleri yapacak olan kuruma ağ taraması yapması için gerekli protokol, adres bilgileri ve ağ bağlantıları hakkında bilgi verecektir.

Yetkili Birim Personeli

Yazılım geliştiren Birim tarafından testleri gerçekleştirecek kurumda oluşabilecek sorunlar hakkında danışabileceği yetkili personeli bu konuyla ilgili görevlendirmelidir.

2 Tarama Zamanı

Bilgi Teknolojileri Birimi sızma ve güvenlik açıklarını tespit etme çalışmalarından etkilenecek birimlere ve personellere testlerin yapılacağı zamanı önceden e-posta ile duyuracaktır.

Hazırlayan	Kontrol eden	Onaylayan

3 Gizlilik Anlaşması

SBÜ ile sızma ve güvenlik açıklarını tespit etme taraması yapacak firma arasında testler sonucunda tespit edilecek bilgilerin hiçbir şekilde üçüncü taraflara aktarılmayacağına dair gizlilik anlaşması yapılacaktır.

dilebilir17. BİLGİ SİSTEMLERİ YEDEKLEME POLİTİKASI

17.1. AMAÇ

Bu politikanın amacı şu araçları sağlamaktır:

i. bir donanım/yazılım arızası veya fiziksel bir felaket durumunda bilgisayar sistemlerinin bütünlüğünü geri yüklemek;

ii. insan hatasına veya önemli dosyaların yanlışlıkla silinmesine karşı bir koruma önlemi sağlar.

17.2. KAPSAM

Tüm kritik bilgi sistemlerinin yedeklenmesi ve bu sistemlerin işletilmesinden sorumlu Bilgi İşlem Dairesi personeli bu politikanın kapsamında yer almaktadır.

17.3. SORUMLULUK

Bilgi İşlem Dairesi Yetkilisi

Bilgi Teknolojileri personeli

17.4. TANIMLAR

Harici bir tanım belirtilmediği için eklenmemiştir.

17.5. İLGİLİ DOKÜMANLAR

Yedekleme Prosedürü

Hazırlayan	Kontrol eden	Onaylayan

17.6. UYGULAMA

SBÜ yedeklerinin alınması ile ilgili uygulamalar "Yedekleme Prosedürü" 'ne göre yapılır. Aşağıda genel olarak uyulması gereken kurallardan bahsedilmiştir;

Bilgi İşlem Dairesi Personeli tarafından dosya sunucusu ve sistem düzeyindeki bilgiler periyodik olarak yedeklenir. Yedekleme ortamı, yeterli koruma ve uygun çevre koşulları ile saklanır.

Yedeklemelerin sıklığı ve kapsamı, bilginin önemine ve veri sahibi tarafından belirlenen kabul edilebilir riske uygun olmalıdır.

Her sistem için yedekleme ve kurtarma süreci belirlenir ve periyodik olarak gözden geçirilir.

Herhangi bir sebepten dolayı yedekleme alınamadığı takdirde xxxx@sbu.edu.tr adresine e-posta olarak uyarı mesajı gelir.

Yedekler mutlaka şifreli olarak alınır.

İşletim sistemlerinin ve diğer kritik bilgi sistemi yazılımlarının yedek kopyaları, operasyonel yazılımlarla aynı yerde saklanmaz.

Sistem yedekleme bilgileri, yetkisiz değişikliklerden ve çevre koşullarından korunur.

Yedekler, kurtarılabilir olduklarından emin olmak için periyodik olarak test edilir. Medya güvenilirliğini ve bilgi bütünlüğünü doğrulamak için, yedekleme bilgileri belirli bir sıklıkta test edilir.

Yedekleme bilgileri, iş sürekliliği sürecinin bir parçası olarak bilgi sistemi işlevlerini geri yüklemek için seçici olarak kullanılır.

18. BİLGİ TRANSFERİ POLİTİKASI

18.1. AMAÇ

Bu politikanın amacı SBÜ ve diğer organizasyonlar arasında gerçekleşebilecek kişisel ve hassas verilerin herhangi bir bilgi kaybı, değişikliği veya yanlış kullanımını önleyerek bu bilgilerin korunmasına yönelik prosedürleri düzenler ve SBÜ içinde ve SBÜ dışında güvenli ve korumalı bir şekilde nasıl aktarılması gerektiğini belirler.

18.2. KAPSAM

SBÜ ve diğer organizasyonlar arasında gerçekleşebilecek bilgi transferini kapsamaktadır.

18.3. SORUMLULUK

Rektörlük

Bilgi İşlem Daire Başkanlığı Yetkilisi

Bilgi İşlem Daire Başkanlığı Personeli

18.4. TANIMLAR

Harici bir tanım belirtilmediği için eklenmemiştir.

18.5. İLGİLİ DOKÜMANLAR

Disiplin Prosedürü

18.6. UYGULAMA

Kişisel veya hassas verileri işleyen herkes, veri aktarımına izin vermek için ilgili yöneticisinden izin almalıdır. Veriler (hassas veya değil) yalnızca SBÜ'nün etkin bir şekilde işletilmesi için kesinlikle gerekli olduğu durumlarda aktarılmalıdır. Buna göre herhangi bir veri aktarımı talep edilmeden önce aktarımın gerekliliği önceden düşünülmelidir.

Üçüncü taraflarla iş yaparken, bu verilerin transferini kapsayan herhangi bir veri paylaşım anlaşmaları veya sözleşmelerinin mevcut olup olmadığı değerlendirilir. Kullanılması gereken transfer yöntemine ilişkin herhangi bir hüküm bulunup bulunmadığı kontrol edilir.

Hazırlayan	Kontrol eden	Onaylayan

Kişisel veya hassas veriler içeren tüm bilgi aktarımları için, alıcının kimliğini ve yetkisini uygun şekilde belirlenmesi önemlidir.

SBÜ'de Personel ve 3. Taraflarla KVKK hükümleri içeren gizlilik ve ifşa etmeme anlaşmaları yapılmalı ve bu anlaşmalar periyodik olarak ilgili sorumlularca gözden geçirilir.

Üçüncü tarafların kurumun yazılımlarını veya verilerini izinsiz kullanması, değiştirmesi veya çoğaltmasını engellemek için kurumu koruyan hükümler içeren yazılı bir sözleşme imzalanır.

Üçüncü taraflarla bilgi ve veri alışverişi yapmadan önce kiminle iletişim kurulacağı belirlenir.

Gizli bilgiler ülke dışına çıkartılamaz.

Bilginin uluslararası seyahati sırasında sadece yetkili personellerin gizlilik içeren bilgiye erişimi vardır.

Üçüncü taraflara tamir için gönderilen bilgisayarların içerisinde herhangi bir bilgi olmamalıdır.

Yetkisi olmayan personeller tarafından gönderilen e–postalar SBÜ'yü bağlamaz.

Üyelerden gelen ödeme hakkındaki bilgiler üyelere tam olarak yollanmamalıdır. Bilgi yollanırken hesap numarası vb. bilgilerin belirli bir kısmını maskeleyerek yollamak daha doğru olacaktır.

İş iletişiminin sağlanması için sadece organizasyon tarafından yetkilendirilen personellerin e–posta adresleri kullanılır.

Gizli bilgiler sadece SBÜ'nün belirlediği uygun sunucularda kayıt altına alınır.

Kritik bir dosyada çeşitli değişikliklerin yapılacaksa, öncelikle dosyanın yedeği alınır.

Yazılım yükleme veya yazılım güncellemelerini yapma ve sistem bakımını gerçekleştirme yetkisi sadece Bilgi İşlem Daire Başkanlığı ekibinindir.

Hazırlayan	Kontrol eden	Onaylayan

SBÜ'de bilgi sistemleri aracılığı ile gönderilen mesajlar, saldırgan veya ayrımcılık içeren bildiriler içermemelidir. SBÜ'nün bilgi sistemi sadece iş gereklilikleri için kullanılmalıdır.

Bir e-postaya gizlilik içermekte olduğuna dair bir not eklendiğinde, bu mesajı sadece e-postanın gönderildiği kişinin aldığından emin olunmalıdır.

Şüpheli tüm spam e-postalar ile ilgili, uygun faaliyetleri yürütecek olan Bilgi İşlemn Daire Başkanlığı BT Ekibine haber verilmelidir.

SBÜ'nün personelleri çeşitli tartışma gruplarına katılmamalıdır.

E-postalarda taranmış imzalar bulunmamalıdır.

E-posta yoluyla gönderilen bilgiler, bu bilginin kimden gelmekte olduğunu içermelidir.

E-posta yoluyla gönderilen bilgiler, spesifik bir geri dönüş adresi içermelidir.

SBÜ, bilgi sistemi vasıtasıyla gönderilmiş herhangi bir bilgiyi algılayabilmeli veya zararlı olabileceğini düşündüğü herhangi bir veriyi silme hakkında sahiptir. Böylece SBÜ'nün itibarını zedeleyebilecek illegal malzemenin transfer edilmesi veya depolanması engellenmiş olur.

Gizlilik içeren bilgiler, hoparlörü açık telefonlarda görüşülmemelidir.

Gizlilik içeren bilgilerin umumi yerlerde konuşulmaması gerekir.

Silinebilir ortamlara kaydedilmiş olan gizli bilgilerin kullanımdan sonra etkin yöntemler kullanılarak silinmesi gerekir.

Personeller gizlilik içeren bilgileri telesekreterlere veya sesli mesajlaşma sistemlerine kayıt etmemelidir.

SBÜ içindeki donanım malzemelerin yerini değiştirmek için Bilgi İşlem Daire Başkanlığı Teknik ekibinden izin alınmalıdır.

Toplantılarda yapılan video konferanslar, yönetim veya katılımcılar tarafından izin verilmedikçe kayıt edilmemelidir.

İşle ilgili tüm aramalar SBÜ sabit hatları kullanımı ile yapılır.

Posta aracılığı ile gönderilen gizli bilgiler iki zarf içinde yollanır. Dış zarfta, içerideki bilginin hassaslığı ile ilgili hiçbir bilgi yazmamalı, ancak iç zarfta bilginin gizli olduğu belirtilir.

Gizli bilgilerin bir toplantıda tartışılması durumunda, toplantı süresince, bu bilginin gizli olduğu ve dinleyenlerin bu bilginin gizliliğini korumaları gerektiği belirtilir.

Kablosuz bağlantı ile gönderilen bilgilerin yollanmadan önce şifrelenmesi gerekir.

Kâğıt üzerindeki gizli bilgilerin gönderilmesi durumunda, bilgilerin taahhütlü yollanması gerekir.

İç dokümanlardaki herhangi bir değişiklik talebi, değişikliği talep eden kişinin kim olduğunu göstermelidir.

Üçüncü taraflar, SBÜ'de bir toplantıya katılmak durumunda olduklarında, bu kişilerin gizli bilgiler barındıran bölgelerde dolaşması engellenmelidir.

Kişisel verilerin yurt dışına transferi için KVKK kapsamında uyulması gereken teknik ve idari tedbirlere uyulmalıdır.

Kişisel verilerin 3.taraflarla paylaşılması durumunda KVKK kapsamında uyulması gereken teknik ve idari tedbirlere uyulmalıdır.

19. TEÇHİZATIN VE ORTAMIN ELDEN ÇIKARILMASI POLİTİKASI

19.1. AMAÇ

Sisteme bağlı ya da bağlı olmayan sunucu, bilgisayar, ağ cihazları ve içerisinde SBÜ verilerinin bulunduğu ortamların elden çıkarılmasının nasıl yapılacağını açıklar.

19.2. KAPSAM

Sistemden çıkartılacak sunucu, bilgisayar ve ağ cihazlarını, basılı, yazılı ve elektronik her türü ortamın saklama ve kullanım ömrü bittiğinde elden çıkarılması, değiştirilmesi veya dönüştürülmesini kapsar.

19.3. SORUMLULUK

Bilgi İşlem Dairesi Yetkilisi

Bilgi İşlem Dairesi Personeli

Birim Yöneticileri

19.4. TANIMLAR

Harici bir tanım olmadığı için eklenmemiştir.

19.5. İLGİLİ DOKÜMANLAR

Doküman İmha Formu

19.6. UYGULAMA

19.7. ELEKTRONİK ORTAM

Sunucular ve Bilgisayarlar

Elden çıkartılacak sunucular ve bilgisayarlarda öncelikle üzerinde bulunan donanım ve parça listesi hazırlanıp bu listede SBÜ dışına çıkmaması gereken ve/veya gizli olan verilerin bulunduğu ortamlar ayrılır.

Hazırlayan	Kontrol eden	Onaylayan

Bilgisayar, ağ cihazları ve diğer bilişim cihazları içerdikleri bilgiler kullanılamaz ve erişilemez hale getirildikten sonra "Doküman İmha Formu" doldurularak kalite biriminin belirlediği elektronik ortamların elden çıkarılması prosesleri uygulanır.

Ağ Cihazları

Elden çıkartılacak olan ağ cihazlarında öncelikle nerede kullanıldığına dair bir liste hazırlanır. Liste işleminden sonra cihaz üzerinde varsa modüller sökülerek ayrılır. Ardından ağ cihazı üzerindeki yazılım ve yapılandırma sıfırlanır. Elden çıkartılan ağ cihazı sistem envanterinden düşülerek, kutusuna konulup depoya kaldırılır.

19.8. BASILI ORTAM

"Saklama ve İmha Politikası"na göre ilgili birim yöneticisi onayıyla saklama süresi dolan kayıtlar "Doküman İmha Formu" imzalanarak birim personeli tarafından imha edilir.

CD, DVD, disket, harici harddisk, flash bellek gibi taşınabilir ortamlar aşağıdaki seçeneklerine göre elden çıkarılırlar. Elden çıkarma sırasında "İmha Tutanağı" imzalanarak dosyalanırlar.

20. ACİL DURUM YÖNETİMİ POLİTİKASI

20.1. AMAÇ

Bu politikanın amacı, acil ve beklenmedik durumların; SBÜ'nün iş sürekliliğinin bilişim altyapısından kaynaklı kurum faaliyetlerinin çalışmasını olumsuz yönde etkileyecek sonuçlar yaratmasını engellemek, "Acil Eylem Planı" sırasında ve ertesinde olağan hizmetlerinin sunumuna devam edebilmesini sağlamaktır.

20.2. KAPSAM

Bu politika, SBÜ faaliyetlerini sürdürebilmesi için gerekli olan, teknik donanım ihtiyaçlarının karşılanması da dahil olmak üzere tüm bilgi teknolojileri faaliyetlerini kapsar.

20.3. SORUMLULUK

Bilgi İşlem Dairesi Yetkilisi

Bilgi Teknolojileri Personeli

20.4. TANIMLAR

Harici bir tanım belirtilmediği için eklenmemiştir.

20.5. İLGİLİ DOKÜMANLAR

Bilgi Güvenliği İhlal Olay Yönetimi Prosedürü

İş Sürekliliği Planı

Acil Eylem Planı

20.6. UYGULAMA

SBÜ'nün iş sürekliliğini etkileyen bilişim altyapısında meydana gelebilecek acil bir durumda "İş Sürekliliği Prosedürü" çerçevesinde belirtilen esaslar doğrultusunda uygulamalar planlanmalıdır.

İş Sürekliliği planında, kritik varlıklar için süreklilik faaliyetleri bilgi güvenliği hususları da dikkate alınarak belirlenir.

Acil durum sorumlusu atanmalı, yetki ve sorumluluklar belirlenmeli ve yazılı hale getirilmelidir.

SBÜ acil durumlarda kurum içi iş birliği gereksinimlerini tanımlıdır.

Ortaya çıkabilecek güvenlik ihlali ve açıklarının rapor edilebilmesi "Bilgi Güvenliği İhlal Olay Yönetimi Prosedürü"nde belirtilen hususlara göre davranılır.

Bir acil durum veya güvenlik ihlali ortaya çıktığında öncelikle Bilgi İşlem Dairesi Yetkilisi'ne ulaşılmalı, ulaşılamadığı durumlarda ilgili yöneticiye bilgi verilmeli ve hasar tespit edilerek önceden tanımlanmış felaket kurtarma faaliyetleri hızlı bir şekilde etkinleştirilir.

Personel acil bir durumda "Acil Eylem Planı"nda belirtilen kişilere erişebilmelidir.

Bilişim sistemleri logları acil durumlarda incelenmek üzere saklanır.

Politikalar ve süreçler yaşanan acil durumlar sonrasında yeniden incelenir ve ihtiyaçlar doğrultusunda düzenlenir.

Acil durum kapsamında değerlendirilen olaylar farklı seviyelerde gerçekleşebilir;

Seviye A: Değerli kurumsal bilgilerin kaybı. Yetkisiz kişiler tarafından bu bilgilere erişilmesi, bozulması, silinmesi

Seviye B: Kurumsal servislerin kesintisi veya bu kesintiye yol açabilecek durumlar

Seviye C: A ve B seviyesinde tanımlanan durumların ortaya çıkmasına sebep olmasından şüphe duyulan ancak gerçekliği ispatlanamamış durumlar.

Yönetim Kurulu tarafından gerekli görülen durumlarda konu hukuksal yönden incelenmek üzere ilgili makamlara iletilmelidir.

21. YAZILIM YÖNETİM POLİTİKASI

21.1. AMAÇ VE KAPSAM

Bu politika, Sağlık Bilimleri Üniversitesi (SBÜ) bünyesinde kullanılan, geliştirilen veya tedarik edilen yazılımların güvenli, verimli ve uyumlu bir şekilde yönetilmesini sağlamak

amacıyla hazırlanmıştır. Politika, SBÜ'nün tüm birimlerini, çalışanlarını, yazılım geliştiricilerini ve üçüncü taraf hizmet sağlayıcılarını kapsar.

21.2. ROLLER VE SORUMLULUKLAR

Bilgi İşlem Daire Başkanlığı: Yazılım yönetim politikalarının uygulanmasını sağlar ve süreçleri denetler.

Yazılım Geliştirme Ekibi: SBÜ için geliştirilen yazılımların güvenlik, güncellik ve uyumluluk açısından yönetilmesinden sorumludur.

Kullanıcılar: Yetkili yazılımları kullanır ve politikaya uygun hareket eder.

Üçüncü Taraf Hizmet Sağlayıcıları: SBÜ yazılım politikalarına uygun olarak yazılım geliştirir ve hizmet sunar.

21.3. YAZILIM GELİŞTİRME VE GÜNCELLEME SÜREÇLERİ

Yazılımlar, belirlenen standartlara uygun olarak geliştirilir ve test edilir.

Güncellemeler, güvenlik açıklarını kapatmak ve performansı artırmak amacıyla düzenli olarak yapılır.

Geliştirme süreçlerinde güvenli kodlama ilkeleri uygulanır.

Kaynak kodları versiyon kontrol sistemleri ile yönetilir.

Değişiklik yönetimi sürecinde, test ve onay mekanizmaları işletilir.

21.4. TEDARİK EDİLEN YAZILIMLARIN YÖNETİMİ VE GÜVENLİK DEĞERLENDİRMESİ

Satın alınan veya dışarıdan temin edilen yazılımlar, SBÜ güvenlik standartlarına uygun olmalıdır.

Tüm yazılımlar düzenli olarak güvenlik taramalarına tabi tutulur.

Kullanım hakları ve lisans yönetimi Bilgi İşlem Daire Başkanlığı tarafından takip edilir.

Tedarik edilen yazılımların güncelliği ve bakım desteği takip edilir.

Kullanım ömrü dolan veya güvenlik riski oluşturan yazılımlar devre dışı bırakılır.

21.5. AÇIK KAYNAK VE ÜÇÜNCÜ TARAF YAZILIM KULLANIMI

Açık kaynak yazılımlar kullanılmadan önce güvenlik değerlendirmesinden geçirilir.

Üçüncü taraf yazılımlar, SBÜ'nün bilgi güvenliği politikalarına uygun olmalıdır.

Kullanılan açık kaynak yazılımlar düzenli olarak güncellenmeli ve güvenlik açıkları takip edilmelidir.

21.6. ERİŞİM VE YETKİLENDİRME POLİTİKALARI

Yazılım erişimleri, yetkilendirme prensiplerine göre düzenlenir.

Kullanıcı erişimleri, ihtiyaç bazlı yetkilendirme prensibine göre tanımlanır.

Kullanıcı yetkileri düzenli olarak gözden geçirilir ve gereksiz yetkiler kaldırılır.

Erişim kayıtları düzenli olarak izlenir ve kayıt altına alınır.

21.7. YEDEKLEME VE GÜNCELLEME YÖNETİMİ

Tüm kritik yazılımlar düzenli olarak yedeklenir ve yedeklerin güvenliği sağlanır.

Yazılım güncellemeleri düzenli aralıklarla gerçekleştirilir ve test edilir.

Yedekleme süreçleri belirlenen politikalar doğrultusunda otomatikleştirilir.

Acil durumlarda kullanılmak üzere yedeklerin erişilebilirliği sağlanır ve test edilir.

21.8. DENETİM VE UYUM SÜREÇLERİ

Yazılım yönetimi süreçleri her yıl düzenli olarak denetlenir.

BİG Rehberi ve diğer ilgili mevzuatlara uyum sağlanır.

Denetim sonuçları kayıt altına alınır ve gerekli iyileştirmeler yapılır.

İç denetimler ile sürekli iyileştirme sağlanır.

21.9. YÜRÜRLÜK VE GÜNCELLEME

Bu politika, SBÜ yönetimi tarafından onaylandığı tarihte yürürlüğe girer ve yılda bir kez gözden geçirilerek güncellenir.

Politika güncellemeleri, ilgili paydaşların görüşleri alınarak gerçekleştirilir.

Değişiklikler, tüm ilgili taraflara duyurulur ve uygulanması sağlanır.

22. SOSYAL MEDYA KULLANIM POLİTİKASI

Değerli Çalışanlarımız,

Sosyal medya olgusu, başta Facebook olmak üzere Twitter, Friendfeed, Flickr, TikTok, Youtube, LinkedIn, Instagram gibi sosyal ağların yoğun ve kitlesel etkileri her geçen gün büyük önem kazanmaktadır.

SBÜ olarak hedefimiz; sosyal medyayı etkin şekilde kullanabilmektir. Bu doğrultuda, SBÜ çalışanlarının internet ve sosyal ağlarda, kendi itibar ve konumları kadar dahil oldukları SBÜ geleneğini de göz önünde bulundurmaları büyük önem arz etmektedir.

Bu konuda tüm çalışanlarımızın SBÜ için "SBÜ Sosyal Medya Kullanım Politikası" oluşturulmuştur.

Bir kurumun sanal ortamda yayınladığı metinlerin dillerinden çalışanların hareketlerine, kurumla ilgili yayımlanan finansal haberlerden videoya çekilmiş birkaç dakikalık görüntülere kadar pek çok şeyi itibarı olumlu ya da olumsuz etkileyebilmektedir. Bu nedenle tüm çalışanlarımızın sosyal medya konusunda belirtilen Sosyal Medya Kullanım Politikası kurallarına uymasını önemle rica ederiz.

Saygılarımızla,
Bilgi İşlem Daire Başkanlığı

SBÜ'yü temsil ettiğinizi unutmayınız.

Kurumun sırlarını ifşa etmeyiniz

Kurumumuza ait dış ve iç mekan fotoğraflarını ve bilgilerini paylaşmayınız.

Telif hakları, adil kullanım vb. ilgili yasalara uygun şekilde davranınız.

İtibarımızı korumak hepimizin görevidir, unutmayınız.

Siyasi görüşlerinizi SBÜ ile özdeşleştirmeyiniz.

Sosyal ağlarda algı karışıklığı yaratmayınız.

Sosyal ağlarda kurumumuz adına karar vermeyiniz.

Kişisel blog yazarken dikkatli olunuz.

Çatışmaya yol açacak yaklaşımlardan uzak durunuz.

Kişilere hizmet verirken kişi odaklı olunuz ve hizmet kalitenize dikkat ediniz.

Emin olmadığınız her türlü konuda lütfen birim sorumlunuz ile iletişime geçiniz.

Bilgi İşlem Daire Başkanlığı

23. SİSTEM ODASI / VERİ MERKEZİ GÜVENLİĞİ POLİTİKASI

23.1. AMAÇ VE KAPSAM

Bu politika, Sağlık Bilimleri Üniversitesi (SBÜ) bünyesinde bulunan sistem odası ve veri merkezlerinin fiziksel ve siber güvenliğinin sağlanmasını amaçlamaktadır. Politika, SBÜ

Bilgi İşlem Daire Başkanlığı tarafından yönetilen tüm veri merkezi ve sistem odalarını, bu alanlarda çalışan personeli, hizmet sağlayıcıları ve yetkilendirilmiş üçüncü tarafları kapsar.

23.2. ROLLER VE SORUMLULUKLAR

Bilgi İşlem Daire Başkanlığı: Sistem odalarının güvenlik politikalarının uygulanmasını sağlar, süreçleri denetler ve ilgili iyileştirmeleri yapar.

Sistem Yöneticileri: Sistem odasında bulunan donanımların ve yazılımların güvenliğini sağlamakla yükümlüdür.

Fiziksel Güvenlik Ekibi: Sistem odasına yetkisiz erişimi engellemek, giriş-çıkış kontrollerini sağlamak ve güvenlik tedbirlerini uygulamakla sorumludur.

Yetkilendirilmiş Personel: Sistem odasına erişim yetkisi bulunan ve ilgili güvenlik prosedürlerine uygun hareket etmekle yükümlü olan kişiler.

Üçüncü Taraf Hizmet Sağlayıcıları: Sistem odasında gerçekleştirilecek bakım ve destek hizmetleri sırasında SBÜ güvenlik kurallarına uymakla yükümlüdür.

23.3. FİZİKSEL GÜVENLİK ÖNLEMLERİ

Sistem odası yetkisiz girişlere karşı elektronik kartlı geçiş sistemi ile korunmalıdır.

Tüm giriş ve çıkışlar kayıt altına alınmalı, güvenlik kameraları ile izlenmelidir.

Yangın, su baskını ve doğal afet risklerine karşı gerekli sensörler ve alarm sistemleri bulunmalıdır.

Fiziksel erişim sadece yetkilendirilmiş personele verilmeli, geçici erişimler için kayıt tutulmalıdır.

Sistem odasında kullanılmayan cihazlar düzenli olarak envanterden çıkarılmalı ve güvenli şekilde imha edilmelidir.

23.4. SİBER GÜVENLİK ÖNLEMLERİ

Tüm sistemler güncel güvenlik yamaları ile düzenli olarak güncellenmelidir.

Hazırlayan	Kontrol eden	Onaylayan

Ağ güvenliği için güvenlik duvarları ve izinsiz giriş tespit sistemleri (IDS/IPS) aktif olarak çalıştırılmalıdır.

Tüm veri merkezi erişimleri kayıt altına alınmalı ve düzenli olarak incelenmelidir.

Kritik sistemler için çok faktörlü kimlik doğrulama (MFA) uygulanmalıdır.

Sistem odasındaki ağ bağlantıları yetkilendirilmiş cihazlarla sınırlandırılmalıdır.

23.5. GÜÇ VE İKLİMLENDİRME YÖNETİMİ

Kesintisiz güç kaynağı (UPS) ve jeneratör sistemleri düzenli olarak bakım ve testlerden geçirilmelidir.

Sistem odası sıcaklık ve nem değerleri sürekli olarak izlenmeli ve belirlenen eşiklerde tutulmalıdır.

İklimlendirme sistemlerinde yedeklilik sağlanmalı ve kritik bileşenlerin arızalanması durumunda otomatik devreye girecek sistemler kurulmalıdır.

23.6. YEDEKLEME VE FELAKET KURTARMA

Tüm kritik sistemlerin düzenli olarak yedekleri alınmakta ve farklı bir lokasyonda saklanmaktadır.

Felaket kurtarma planları hazırlanmış ve yılda en az bir kez test edilmektedir.

Yedekleme politikaları doğrultusunda yedeklerin bütünlüğü ve erişilebilirliği periyodik olarak kontrol edilmektedir.

23.7. DENETİM VE UYUM SÜREÇLERİ

Sistem odası güvenliği, periyodik olarak iç ve dış denetimlere tabi tutulmaktadır.

Bilgi ve İletişim Güvenliği Rehberi (BİG Rehberi) başta olmak üzere ISO 27001, KVKK ve ilgili mevzuatlara tam uyum sağlanmaktadır.

Denetim sonuçlarına göre gerekli güvenlik iyileştirmeleri yapılmaktadır.

Hazırlayan	Kontrol eden	Onaylayan

YÜRÜRLÜK VE GÜNCELLEME Bu politika, SBÜ yönetimi tarafından onaylandığı tarihte yürürlüğe girer ve yılda bir kez gözden geçirilerek güncellenir. Değişiklikler ilgili birimlere duyurulur ve uygulanması sağlanır.