P00 BİLGİ GÜVENLİĞİ POLİTİKAMIZ

1. AMAÇ VE KAPSAM

Bu politikanın amacı, hukuka, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklere ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemek için, üst yönetiminin yaklaşımını ve hedeflerini tanımlamak, tüm çalışanlara ve ilgili taraflara bu hedefleri bildirmektir.

2. REFERANS DOKÜMANLAR:

3. SORUMLULUK:

Bilgi Güvenliği Politikasının hazırlanması, gözden geçirilmesi ve güncellenmesinden BGYS Yöneticisi ve/veya BGYS Temsilcisi sorumludur. CELAL BAYAR ÜNİVERSİTESİ (CBÜ) yönetimi Bilgi Güvenliği Politikasını onaylar ve duyurulmasını sağlar.

4. POLİTİKA DETAYI:

4.1. TANIMLAR

4.1.1. Bilgi Güvenliği Yönetim Sistemi - BGYS:

Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır.

4.1.2. BGYS Yöneticisi:

Bilgi Güvenliği Yönetim Sistemi'nin operasyonundan ve sürekli iyileştirilmesinden sorumludur. BGYS Yöneticisi, Sistem Yöneticisidir.

4.1.3. Bilgi Varlığı:

CBÜ'nün sahip olduğu, işlerini aksatmadan yürütebilmesi için önemli olan varlıklardır.

Bu politikaya konu olan bilgi varlıkları şunlardır:

a. Kağıt,elektronik, görsel veya işitsel ortamda sunulan her türlü bilgi ve veri
b. Bilgiye erişmek ve bilgiyi değiştirmek için kullanılan her türlü yazılım ve donanım
c. Bilginin transfer edilmesini sağlayan ağlar
d. Birimler, ekipler ve çalışanlar
e. Tesisler ve Özel alanlar
f. Çözüm ortakları
g. Üçüncü taraflardan sağlanan servis, hizmet veya ürün

4.1.4. Bilgi Varlığının İş Sahibi:

Bilgi varlıklarının üretimi, geliştirilmesi, bakımı, kullanımı ve güvenliğini kontrol etmek için onaylanmış yönetim sorumluluğu bulunan kişi veya varlıkları tanımlar. 'Sahip' terimi, gerçekten varlık üzerinde mülkiyet hakları olan kişi anlamına gelmez.

4.1.5. Bilgi Varlığının Teknik Sahibi:

Bilgi varlıklarının kurum içinde kullanılması için gerekli olan teknik operasyonda sorumluluğu bulunan kişi veya ekipleri tanımlar.

4.2. POLİTİKA:

Bilgi kaynakları, tesisler ve cihazlar gibi CBÜ açısından büyük önem taşıyan varlıklardır. Bilgi varlıklarını ve kaynaklarını kullanan veya bilgi sağlayan herhangi bir kişi, bilgi varlıklarını korumakla yükümlüdür.

Ortak bilgi varlıklarını kullanan tüm çalışanların, gereken duyarlılığı göstermesi ve diğer meslektaşlarını, kurum çalışanlarını ve kurumsal değerleri gözeterek hareket etmesi beklenir.

Kurumsal değerlerin gereği olarak gizliliğe önem verilir, her türlü kişisel bilgi en yüksek güvenlik standartlarına sahip sistemlerle korunur. Bilginin sahibi istemedikçe, yetki verilmedikçe veya yasal gereklilikler oluşmadıkça bilgi paylaşılmaz.

CBÜ için tüm bu bilgi varlıkları ve kaynakları içerisinde en kritik olanı, özenle korunması, gizliliğinin sağlanması, ihtiyaç duyulduğu anda erişilmesi gereken bilgi varlıkları, **demo sistemleri ve** CBÜ **yazılım kataloğunu içinde barındıran sunucu sistemi ve bu sistemi barındıran sistem odasıdır.**

Bilgi varlıkları ve kaynakları farklı konumlarda veya ortamlarda bulunabilir. Hangi konumda veya ortamda olursa olsun müşteri iletişim gereksinimleri ve kurumsal değerler bu varlıkların ve kaynakların kullanımını belirler.

Bilgi güvenliği, sadece bilginin gizliliğinin değil, bütünlüğünün ve kullanılabilirliğinin de sağlanması ile mümkündür. Bilginin gizlilik gerekliliği, sadece yetkilendirme dahilinde gereken bilgi varlıklarına erişim verilmesi anlamına gelir. Bilginin bütünlüğü, tüm bilgi varlıklarının tamlığını ve doğruluğunu sağlamayı gerektirir. Bilginin kullanılabilirliği, bilgi varlıklarının ihtiyaç duyulduğu anda ulaşılabilir ve kullanılabilir olması anlamına gelir.

Bilginin kullanımı, yerleşimi ve korunması ile ilgili ihtiyaçların karmaşıklığı ve çokluğu, kapsamlı ve geniş bilgi güvenliği süreçlerinin ve politikalarının tanımlanmasını zorunlu kılmaktadır. Bu nedenle belirlenen süreçler doğrultusunda bilgi güvenliği riskleri, bilgi varlığından sorumlu olan kişiler tarafından değerlendirilir, risklerin önceliği belirlenir ve gereken önlemler alınır.

Sistem odası ve sunucuların güvenliğinin sağlanması öncelikli olarak ele alınır. Varlık envanterinin ve bu envanterin olası risklerinin önceden belirlenerek müşterilerin güven içinde ve kesintisiz hizmet almaları için çalışılır.

Karar ve eylemlerde, güvenilir nesnel bilgiler ile teknolojinin tüm olanaklarının kullanılmasına önem ve öncelik verilir. Hareketler sezgilere, duygulara ya da doğru görünene göre değil; bilimsel ve teknolojik gerçeklerin ortaya koyduğu objektif esaslara göre düzenlenir. Bunu sağlamak için bilgi dünyadaki en ileri kaynaklardan transfer edilir, benimsenir ve mesleki uygulamalar bu doğrultuda yapılır. Kaynaklar verimli kullanılarak teknolojiye yatırım yapılır, gelişim bu doğrultuda sürdürülür.

Bu nedenle bilgi güvenliği yönetim sisteminin planlama, uygulama, izleme ve iyileştirme adımları ISO/IEC 27001 BGYS standardına ve bu standardı destekleyen standartlara uygun olarak yürütülür.

4.2.1. Bilgi Varlıklarının ve Kaynaklarının Kullanımı

CBÜ'de yürütülen yazılım ve danışmanlık hizmetlerinin doğası gereği, bilginin gizliliğinin korunması öte yandan bilginin ve fikirlerin paylaşılması ve yaygınlaştırılması gerekir. Bilginin hassasiyeti ve güvenliği ile ilgili ihtiyaçlar gözetilirken, aynı zamanda bilgiye ihtiyaç anında hızla ulaşılması büyük önem taşımaktadır. O nedenle, bilgi kaynaklarının değerinin iyi tespit edilmesi, bilginin korunmasını sağlayacak çaba ve maliyetin bilginin hassasiyeti ile orantılı olması gerekir.

CBÜ bilgi kaynaklarını kullanarak etik dışı veya yasalara karşı faaliyetlerde bulunmak, hiç kimse için kabul edilemez.

Bu politikanın asgari gereği olarak,

- Verinin kasıtlı olarak değiştirilmesi;
- Kasıtlı olarak veride hataların oluşmasına veya veri kaybına neden olunması;
- Bilgi kaynaklarının yasaları ihlal eden bir faaliyet için kullanılması;
- Bilgi güvenliğinin ihlal edilmesi veya suiistimal edilmesi;
- Cihazların, yazılımların veya herhangi diğer bir bilgi kaynağının çalınması, tahrip edilmesi;
- Bilgi kaynaklarının bilişim sistemlerinin performans kaybına sebep olacak şekilde kullanılması;
- Tesislerin, fiziksel cihazların, ağların tahrip edilmesi kabul edilemez.

Bu ve benzeri faaliyetler ve teşebbüsler disiplin suçu olarak ele alınır, gereken disiplin süreçleri ve yasal süreçler İdari İşler tarafından uygulanır.

Belirtilen tarzda bilgi güvenliği ihlallerinin, ihlal teşebbüslerinin veya bu tür ihlaller ile sonuçlanabilecek zafiyetlerin, tespit edildiği anda zaman kaybetmeden BGYS Yöneticisi/veya BGYS Yöneticisi Yardımcısı'na bildirilmesi gerekir.

4.2.2. Rol ve Sorumluluklar

Bilgi varlıklarının teknik sahipleri bilginin gizlilik bütünlük ve kullanılabilirliğini sağlamak için;

- Bilgi varlıklarına yetkisiz olarak erişilmesini; bilgi varlıklarının yetkisiz olarak değiştirilmesini veya tahribatını önlemek suretiyle, bilgi varlıklarını korurlar.
- Operasyonun mümkün olan en kısa hizmet kesintisi ile devam etmesini sağlamak için gerekli süreçlerin tanımlanmasını ve uygulanmasını sağlarlar.
- Bilgi güvenliği gerekliliklerini gözetirken, ihtiyaç duyulduğunda bilgiye hızla erişilebilmesi için karmaşıklığı ortadan kaldıracak dengeyi kurarlar.
- Çalışanlarını ve birlikte çalıştıkları üçüncü taraf çalışanlarını bilgi güvenliği gereklilikleri, rolleri ve sorumlulukları konusunda bilgilendirirler ve bilinçlendirirler.

Bütün bu faaliyetlerin kurumsal ISO/IEC 27001 standardı ile uyumlu bir çerçevede ele alınması için, tüm kuruluşun süreç ve hizmetlerini kapsayan bir BGYS kurulmuş ve İdari ve Mali Hizmetler Şube Müdürü, "BGYS Ekip Lideri" olarak atanmıştır.

4.2.3. BGYS EKİBİ

BGYS Ekibi aşağıdaki kişilerden oluşur:

- Birim Yöneticisi
- İdari ve Mali Hizmetler Şube Müdürü
- İletişim ve Akıllı Kart Şube Müdürü
- Ağ ve Sistem Birimi
- Teknik Hizmetler Birimi
- Yazılım ve WEB Birimi

BGYS Ekibi, yılda bir kere, YGG toplantılarından 2-4 hafta önce gerçekleştirilir BGYS Ekip Lideri'nin oluşturduğu gündem çerçevesinde toplanır. Toplantılarda görüşülen konular aşağıda belirtilen maddeleri içerir, ancak bunlarla sınırlı kalmayabilir:

- Bilgi Güvenliği Politikası'nın gözden geçirilmesi
- Risk Yönetim Metodolojisinin onaylanması
- Güncel risk raporunun değerlendirilmesi
- Kabul edilebilir risk seviyesinin üst yönetim tarafından onaylanması
- Artık risklerin üst yönetim tarafından onaylanması
- Risk işleme planının üst yönetim tarafından onaylanması
- Güvenlik ihlal olaylarının değerlendirilmesi
- İş süreklilik stratejisinin gözden geçirilmesi

- İş sürekliliği tatbikat sonuçlarının değerlendirilmesi
- Bilgi güvenliği bilinçlendirme çalışmalarının gözden geçirilmesi
- İç denetim raporlarının değerlendirilmesi
- Kurumu etkileyebilecek önemli değişiklikler.
- Varlık Envanteri, varlık sahiplik ve kullanıcı erişim hakları.
- Sistem Loglarının incelenmesi.
- Yedekli Yazılım ve Teçhizatların gözden geçirilmesi.
- Gizlilik ya da ifşa etmeme anlaşmalarının gözden geçirilmesi.

4.2.3 Yasal Şartlara Uyumluluk

CBÜ Türkiye Cumhuriyeti kanunlarına ve tüm uluslararası kanunlara uymayı kabul ve taahhüt eder. Bilginin saklanması, kullanılması ve ifşasında TCK 5846 (Fikir ve Sanat Eserleri Kanunu), TCK 5651 (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu), TCK 5237 (Kişi Hak ve Özgürlüklerini, Kamu Düzen ve Güvenliğini, Hukuk Devletini, Kamu Sağlığını ve Çevreyi, Toplum Barışını Korumak, Suç İşlenmesini Önleme Kanunu), TCK 5070 (Elektronik İmza Kanunu), TCK 5809 (Elektronik Haberleşme Kanunu), İş Kanunu olmak üzere tüm kanunlara uygun hareket eder. CBÜ yönetimi, bu kanun ve yönetmeliklerine aykırı bir davranışta bulunan çalışanı veya tedarikçisi ile ilgili gerekli suç duyurusunda bulunmakla sorumludur.

5651 sayılı Internet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun ile içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlenmiştir. Bu kapsamda 5651 sayılı kanun hem içerik, yer, erişim ve toplu kullanım sağlayıcıları ile ilgili düzenlemeleri hem de Internet ortamında işlenen suçlar ile ilgili cezai hükümleri ortaya koyan bir kanundur. Kanunla verilen görevler Bilgi Teknolojileri ve İletişim Kurumu bünyesinde bulunan Telekomünikasyon İletişim Başkanlığı'nca yerine getirilmektedir.

5070 sayılı elektronik imza kanunu ile birlikte güvenli elektronik imza, elle atılan ıslak imzaya eşdeğer kabul edilmiş ve aynı hukuki sonuçları doğuracağı belirtilmiştir. Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmelerinin güvenli elektronik imza ile gerçekleştirilemeyeceği kanunda ifade edilmiştir. (Örn: emlak alım satımı, veraset ve intikal, evlenme gibi işlemler) Elektronik sertifika hizmet sağlayıcıları, elektronik imzalarla ilgili hizmetleri sağlarlar. Elektronik sertifika hizmet sağlayıcılarının elektronik imza kanununun uygulanmasına ilişkin faaliyet ve işlemlerinin denetimi Bilgi Teknolojileri ve İletişim Kurumu tarafında yerine getirilmektedir.

5809 sayılı elektronik haberleşme kanunu elektronik haberleşme sektöründe düzenleme ve denetleme getiren bir kanundur. Bu düzenleme ve denetleme unsurları içerisinde bilgi güvenliği ile ilgili hususlar da yer almaktadır. Örneğin, kanunun dört numaralı maddesinde ilgili merciler tarafından elektronik haberleşme hizmetinin sunulmasında ve bu hususta yapılacak düzenlemelerde "bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi" ilkesinin göz önüne alınması gerektiği ifade edilmektedir. Kanunla verilen düzenleme ve denetleme görevleri Bilgi Teknolojileri ve İletişim Kurumu tarafından yerine getirilmektedir.

Bu politika CBÜ Yönetimi tarafından gözden geçirilmiş ve onaylanmıştır.

CBÜ uyulması zorunlu tüm yasal şartlar DIŞ KAYNAKLI DOKÜMAN LİSTESİ'nde tanımlanmıştır.

POLİTİKA LİSTESİ

- ✓ P01 BİLGİ SİSTEMLERİ GENEL KULLANIM POLİTİKASI
- ✓ P02 PERSONEL GÜVENLİĞİ POLİTİKASI
- ✓ P03 İNTERNET ERİŞİM POLİTİKASI
- ✓ P04 E-POSTA POLİTİKASI
- ✓ P05 ANTİ-VİRÜS POLİTİKASI
- ✓ P06 ŞİFRE POLİTİKASI
- ✓ P07 KABLOSUZ İLETİŞİM POLİTİKASI
- ✓ P08 UZAKTAN ERİŞİM POLİTİKASI
- ✓ P09 KRİZ / ACİL DURUM YÖNETİMİ POLİTİKASI
- ✓ P10 FİZİKSEL GÜVENLİK POLİTİKASI
- ✓ P11 SUNUCU GÜVENLİK POLİTİKASI
- ✓ P12 AĞ CİHAZLARI GÜVENLİK POLİTİKASI
- ✓ P13 AĞ YÖNETİMİ POLİTİKASI
- ✓ P14 RİSK DEĞERLENDİRME POLİTİKASI
- ✓ P15 DONANIM VE YAZILIM ENVANTERİ OLUŞTURMA POLİTİKASI
- ✓ P16 VERİTABANI GÜVENLİK POLİTİKASI
- ✓ P17 DEĞİŞİM YÖNETİMİ POLİTİKASI
- ✓ P18 GÜVENLİK AÇIKLARI TESPİT ETME POLİTİKASI
- ✓ P19 SANAL ÖZEL AĞ (VPN) POLİTİKASI
- ✓ P20 KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI
- ✓ P21 BİLGİ SİSTEMLERİ YEDEKLEME POLİTİKASI
- ✓ P22 BAKIM POLİTİKASI
- ✓ P23 BİRLİKLER İÇİN UZAKTAN ERİŞİM POLİTİKASI

- ✓ P24 YAZILIM GELİŞTİRME
- ✓ P25 PERSONEL VE EĞİTİM
- ✓ P26 BELGELENDİRME
- ✓ P27 KABUL EDİLEBİLİR KULLANIM POLİTİKASI
- ✓ P28 ORTAMIN ELDEN ÇIKARILMASI POLİTİKASI
- ✓ P29 TEÇHİZATIN ELDEN ÇIKARILMASI POLİTİKASI
- ✓ P30 TEMİZ MASA TEMİZ EKRAN POLİTİKASI
- ✓ P31 KRİPTOGRAFİK KONTROLLER POLİTİKASI
- ✓ P32 ZİYARETÇİ KABUL POLİTİKASI
- ✓ P33 TAŞINABİLİR MOBİL CİHAZ POLİTİKASI
- ✓ P34 SİBER SALDIRI POLİTİKASI
- ✓ P35 BİLGİ VE YAZILIM ALIŞVERİŞİ POLİTİKASI
- ✓ P36 ÜÇÜNCÜ TARAF GÜVENLİK POLİTİKASI
- ✓ P37 VARLIKLARA YÖNELİK SORUMLULUK POLİTİKASI
- ✓ P38 BASILI ÇIKTI VE DAĞITIM POLİTİKASI
- ✓ P39 BİLGİ SINIFLANDIRMA VE ETİKETLEME POLİTİKASI
- ✓ P40 OLAY İHLAL BİLDİRİM VE YÖNETİM POLİTİKASI
- ✓ P41 GÜVENLİ YAZILIM GELİŞTİRME POLİTİKASI

P01 BİLGİ SİSTEMLERİ GENEL KULLANIM POLİTİKASI

1. Genel Bakış

Kurumun amacı herhangi kimse üzerinde kısıtlayıcı politikalar üretmek değil aksine açıklık, güven ve bütünlüğe yönelik kültürü yerleştirmektir. Kurum bilerek veya bilmeyerek yapılan yasadışı veya zararlı eylemlerine karşı çalışanların ve kurumun haklarını korumaya adamıştır. Bilişim ile alakalı sistemler kurumun sahip olduğu değerlerdir. Güçlü bir güvenlik bütün çalışanların içerisine dahil olduğu takım çalışmasıyla oluşturulabilir. Bütün bilgisayar kullanıcıları günlük aktivitelerini yerine getirebilmesi için bu kuralları iyi bilmeli ve uygulamanın sorumluluğunu taşımalıdır.

2. Amaç

Bu politikanın amacı kurum bünyesindeki bilişim cihazlarının uygun kullanımı hakkında taslak oluşturmaktır. Uygunsuz kullanım kurumu virüs saldırılarına, ağ sistemlerinin çökmesine hizmetlerin aksamasına sebep olabilir ve bunlar yaptırımlara dönüşebilir.

3. Kapsam

Bu politika kurumun bütün çalışanları, sözleşmelileri ve kurum adı altında çalışan bütün kişiler için geçerlidir. Aynı zamanda kurumun sahip olduğu ve kiraladığı bütün cihazlar için geçerlidir.

4. Politika

4.1 Genel Kullanım ve Sahip Olma

a) Kullanıcılar şunun farkında olmalıdırlar; kurumun güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da kurumun bünyesinde oluşturulan tüm veriler kurumun mülkiyetindedir.

b) Çalışanlar bilgi sistemlerini kendi kişisel kullanımı için makul seviyede yararlanabilirler. Her bir departman kendi bilgi sistemlerinin kişisel kullanımı için gerekli kuralları koymalıdır. Departmanlar böyle bir kural koymamış ise kurumun koyduğu genel güvenlik politikaları geçerlidir.

c) Kullanıcı herhangi bir bilginin çok kritik olduğunu düşünüyorsa o bilgi şifrelenmelidir.

d) Güvenlik ve ağın bakımı amacı ile yetkili kişiler cihazları, sistemleri ve ağ trafiğini "Denetim Politikası" çerçevesinde gözlemleyebilir

e) Kurum, bu politika çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.

f) 25 kullanıcıdan daha büyük ağlarda domain yapısı oluşturulmalıdır. Bu durumda bütün bilgisayarlar domaine login olmalıdır. Domain'e bağlı olmayan bilgisayarların yerel ağdan çıkarılmalı, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi yapılmamalıdır.

g) Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı, kopyalanmamalıdır.

h) Bilgisayarlar üzerinden resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.

J) Birimlerde sorumlu bilgi işlem personeli ve ilgili teknik personel dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vb. üzerinde mevcut yapılan düzenlemeler hiçbir surette değiştirilmemelidir.

k) Bilgisayarlara hiçbir surette lisanssız program yüklenmemelidir.

l) Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.

4.2 Güvenlik Ve Kişiye Ait Bilgiler

a) Bilgi sistemlerinde bulunan kritik bilgilere yetkisiz kişilerin erişimini engellemek için gerekli erişim hakları tanımlanmalıdır.

b) Şifreleri güvenli bir şekilde tutun ve hesabınızı başka kimselerle paylaşmayın. Sistem seviyeli şifreler 3 ayda bir kullanıcı seviyeli şifreler ise en az ayda bir şifrelenmelidir.

c) Bütün PC ve Laptoplar otomatik olarak 10 dakika içerisinde şifreli ekran korumasına geçebilmelidir.

d) Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. Bios ve işletim sistemi şifreleri aktif hale getirilmelidir. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmalıdır.

e) Laptop bilgisayarın çalınması / kaybolması durumunda, durum fark edildiğinde en kısa zamanda yetkili kişiye haber verilmelidir.

f) Bütün cep telefonu ve PDA cihazları kurumun ağı ile senkronize olsun veya olmasın şifreleri aktif halde olmalıdır. Kullanılmadığı durumlarda kablosuz erişim özellikleri aktif halde olmamalıdır ve mümkünse anti-virüs programları ile yeni nesil virüslere karşı korunmalıdır.

g) Çalışanlar tarafından haber gruplarına gönderilen maillerde şöyle bir açıklama olmalıdır.

" Bu e-posta iş için gönderilenler hariç sadece yukarıda isimleri belirtilen kişiler arasında özel haberleşme amacını taşımaktadır. Size yanlışlıkla ulaşmışsa lütfen gönderen kişiyi bilgilendiriniz ve mesajı sisteminizden siliniz. CBÜ bu mesajın içeriği ile ilgili olarak hiçbir hukuksal sorumluluğu kabul etmez."

1.0 Çalışanlar bilinmeyen kimselerden gelen dosyaları açarken çok dikkatli olmalıdırlar.
2.0 Çünkü bu mailler virüs, e-mail bombaları ve Truva atı gibi zararlı kodları içerebilirler.
3.0 Bütün kullanıcılar ağın kaynaklarının verimli kullanımı konusunda dikkatli olmalıdırlar. E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olun ve gerekirse dosyaları sıkıştırın.
4.0 Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek kuruma veya kişiye yönelik saldırılardan sistemin sahibi sorumludur.

5. Uygunsuz Kullanım

Genel olarak aşağıdaki eylemler yasaklanmıştır. Sistem yöneticileri bu kapsamın dışında olabilir. Herhangi bir kullanıcı kurumun kaynaklarını kullanarak hiçbir şart altında herhangi bir yasadışı aktivitede bulunamaz.

Sistem ve Ağ Aktiviteleri

Aşağıdaki aktiviteler hiçbir istisna olmadan kesinlikle yasaklanmıştır.

Herhangi bir kişi veya kurumun izinsiz kopyalama, ticari sır, patent veya diğer şirket bilgileri, yazılım lisansları vs. haklarını çiğnemek.
Kitapların izinsiz kopyalanması, magazinlerdeki fotoğrafların dijital formata dönüştürülmesi, lisans gerektiren yazılımların kopyalanması.
Zararlı programların ağa veya sunuculara bulaştırılması.
Kendi hesabınızın şifresini başkalarına vermek veya kendi hesabınızı kullandırmak. Bu evden çalışırken aile bireylerini de kapsar.
Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışmak.
Ağ güvenliğini etkilemek, ağ haberleşmesini bozmak.
Kullanıcı kimlik tanıma yöntemlerinden kaçmak
Program/script/komut kullanarak kullanıcının bağlantısını etkilemek
Kurum bilgilerini kurum dışından üçüncü şahıslara iletmek
Kullanıcıların kişisel bilgisayarları üzerine bilgi işlem bölümünün onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapması
Cihaz, yazılım ve verinin izinsiz olarak kurum dışına çıkarılması

Kurumun politikaları olarak belirlediği programlar dışında kaynağı belirsiz olan programları kurmak ve kullanmak yasaktır.

E-mail ve Haberleşme Aktiviteleri

Kurum dışından web posta sistemini güvenliğinden emin olunmayan bir bilgisayardan kullanmak
İstenilmeyen e-posta mesajlarının iletilmesi. Bunlar karşı tarafın özellikle istemediği reklam mesajlarını içeren mailler olabilir.
E-posta veya telefon vasıtası ile taciz etmek
E-posta başlık bilgilerini yetkisiz kullanmak veya değiştirmek
Zincir e-postaları oluşturmak veya iletmek
İş ile alakalı olmayan mesajları birçok haber gruplarına iletmek.

P02 PERSONEL GÜVENLİĞİ POLİTİKASI

1. Amaç

Kurumun bilgi kaynaklarının güvenliğinin sağlanması, çalışanlarının bu konuya duyarlı olması, bilinç seviyesi kendisine verilen yetki ve sorumlulukları iyi anlaması ve yerine getirmesiyle çok yakından bağlantılıdır. Bu nedenle kurum, ilgili personelin seçimi sorumluluk ve yetkilerin atanması, işten atılması, eğitilmesi, vb. konularının güvenlik ile ilgili boyutunu ne şekilde ele alacağını bu politika ile belirler.

2. Kapsam

Personel Güvenlik Politikası, Kurum bilgi sistemlerini kullanan tüm yönetici ve çalışanlarını kapsamaktadır.

3. Politika

a) Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılmalıdır.
b) Kullanıcılara erişim haklarını açıklayan yazılı bildiriler verilmeli ve teyit alınmalıdır.
c) Yetkisi olmayan personelin, kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.
d) Bilgi sistemlerinde sorumluluk verilecek kişinin özgeçmişi araştırılmalı, beyan edilen akademik ve profesyonel bilgiler teyit edilmeli, karakter özellikleriyle ilgili tatmin edici düzeyde bilgi sahibi olmak için iş çevresinden ve dışından referans sorulması sağlanmalıdır.
e) Bilgi sistemleri ihalelerinde sorumluluk alacak üniversite personeli için güvenlik gereksinim ve incelemeleriyle ilgili koşullar eklenmelidir.
f) Kritik bilgiye erişim hakkı olan çalışanlar ile gizlilik anlaşmaları imzalanmalıdır.
g) Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenmelidir.
h) Çalışanlara telefon görüşmeleri yaparken civardakiler tarafından işitilebileceği veya dinlenebileceği için hassas bilgilerin konuşulmaması hatırlatılmalıdır.
i) Çalışanlara kamuya açık alanlarda, açık ofis ortamlarında ve ince duvarları olan odalarda gizliliği olan konuşmaların yapılmaması hatırlatılmalıdır.
j) İş tanımı değişen veya kurumdan ayrılan kullanıcıların erişim hakları hemen silinmelidir.
k) Kurum bilgi sistemlerinin işletilmesinden sorumlu personelin konularıyla ilgili teknik bilgi düzeylerini güncel tutmaları çalışma sürekliliği açısından önemli olduğundan eğitim planlamaları periyodik olarak yapılmalı, bütçe ayrılmalı eğitimlere katılım sağlanmalı ve eğitim etkinliği değerlendirilmelidir.
l) Yetkiler "görevler ayrımı" ve "en az ayrıcalık" esaslı olmalıdır. "Görevler ayrımı "rollerin sorumlulukların paylaştırılması ile ilgilidir ve bu paylaşım sayesinde kritik bir sürecin tek kişi tarafından kırılma olasılığı azaltılır."En az ayrıcalık" ise kullanıcıların

gereğinden fazla yetkiyle donatılmamaları ve sorumlu oldukları işleri yapabilmeleri için yeterli olan asgari erişim yetkisine sahip olmaları demektir.

m) Kritik bir görevin tek kişiye bağımlılığını azaltmak ve aynı işi daha fazla sayıda çalışanın yürütebilmesini sağlamak amacıyla, bir sıra dahilinde çalışanlara görev ve sorumluluk atanmalıdır. Böylece kritik bir iş birden fazla kişi tarafından öğrenilmiş olacaktır.

n) Çalışanlar kendi işleri ile ilgili olarak bilgi güvenliği sorumlulukları, riskler görev ve yetkileri hakkında periyodik olarak eğitilmelidir.Yeni işe alınan elemanlar içinde bu eğitim, oryantasyon sırasında verilmelidir.

Çalışanların başka görevlere atanması ya da işten ayrılması durumlarında işletilecek süreçler tanımlanmalıdır. Erişim yetkilerinin, kullanıcı hesaplarının, token, akıllı kart gibi donanımların iptal edilmesi, geri alınması veya güncellenmesi sağlanmalı, varsa devam eden sorumluluklar kayıt altına alınmalıdır.

P03 İNTERNET ERİŞİM POLİTİKASI

1. Amaç

CBÜ güvenli internet erişimi için sahip olması gereken standartları belirlemektir. İnternetin uygun olmayan kullanımı, kurumun yasal yükümlülükleri, kapasite kullanımı ve kurumsal imajı açısından istenmeyen sonuçlara neden olabilir. Bilerek ya da bilmeyerek bu türden olumsuzluklara neden olunmaması ve internetin kurallarına, etiğe ve yasalara uygun kullanımının sağlanmasını amaçlamaktadır.

2. Kapsam

Bu politika CBÜ'nün bütün kullanıcılarını kapsamaktadır.

3. Politika

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

a) Kurumun bilgisayar ağı erişim ve içerik denetimi yapan bir firewall üzerinden internete çıkacaktır. Ağ güvenlik duvarı kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır. Ağın dışından ağın içine erişimin denetimi burada yapılır. Güvenlik duvarı aşağıda belirtilen hizmetlerle birlikte çalışarak ağ güvenliğini sağlayabilmelidir.

b) Kurumun ihtiyacı doğrultusunda içerik filtreleme sistemleri kullanılmalıdır. İstenilmeyen siteler (kumar,şiddet vs.) yasaklanabilmelidir.

c) Kurumun ihtiyacı doğrultusunda saldırı tespit ve önleme sistemleri kullanılmalıdır. (Intrusion Detection an Prevention Systems IPS) şüpheli olayları, nüfuz ve saldırıları tespit etmeyi hedefleyen bir sistemdir. IPS, şüpheli durumlarda e-posta veya sms gibi yöntemlerle sistem yöneticisini uyarabilmektedir.

d) Anti-virüs gateway sistemleri kullanılmalıdır. İnternete giden veya gelen bütün trafik virüslere karşı taranmalıdır.

e) Ancak yetkilendirilmiş sistem yöneticileri internete çıkarken bütün servisleri kullanma hakkına sahiptir.(ftp ,telnet)

f) Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemeli ve dosya indirimi yapılmamalıdır.

g) Üçüncü şahısların kurum internetini kullanmaları bilgi işlem daire başkanının izni ve bu konudaki kurallar dahilinde gerçekleştirilebilecektir.

P04 E-POSTA POLİTİKASI

1. Amaç

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

2. Kapsam

Bu politika kurumda oluşturulan e-postaların doğru kullanımını içermektedir ve bütün çalışanları kapsamaktadır.

3. Politika

3.1 Yasaklanmış Kullanım

a) Kurumun e-posta sistemi, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz. Bu tür özelliklere sahip bir mesaj alındığında hemen ilgili birim yöneticisine haber verilmesi ve daha sonra bu mesajın tamamen silinmesi gerekmektedir.

b) Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.

c) Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemeli.

d) Kişisel kullanım için internetteki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.

e) Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.

g) Kullanıcıların kullanıcı kodu / şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.

h) Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) gönderemezler.

3.2 Kişisel Kullanım

a) CBÜ'de kişisel amaçlar için e-posta kullanımı mümkün olduğunca makul seviyede olmalıdır. Ayrıca iş dışındaki e-postalar farklı bir klasör içerisinde saklanmalıdır.

b) Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu yüzden şifre kullanılmalı ve e-posta erişimi için donanım /yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.

c) Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-maillerin sahte e-mail olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.

d) Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplandırmalıdır.

e) Kurum çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesi ve okunmasını engellemekten sorumludurlar.

g) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir.

h) Elektronik postaların sık sık gözden geçirilmesi, gelen mesajların uzun süreli olarak genel elektronik posta sunucusunda bırakılmaması ve bilgisayardaki kişisel klasöre çekilmesi gereklidir.

J) E-posta adresine sahip kullanıcının herhangi bir sebepten (emekli olma, işten ayrılma gibi nedenlerle) kurumdaki değişikliğinin yetkililer tarafından Bilgi İşlem Daire Başkanlığına bildirilmesi gereklidir.

3.3 Gözlemleme

CBÜ çalışanları gönderdikleri, aldıkları veya sakladıkları e-maillerde kişisellik aramamalıdır. Bu yüzden yetkili kişiler önceden haber vermeksizin e-mail mesajlarını denetleyebilirler.

3.4 E-Posta Yönetimi

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

3.5 E- Posta Virüs Koruma

Virüs, solucan, Truva atı veya diğer zararlı kodlar bulaşmış olan bir e-posta kullanıcıya zarar verebilir. Bu tür virüslerle bulaşmış e-postalar anti-virüs sistemleri tarafından analiz edilip temizlenmelidir. Ağ güvenlik yöneticileri bu sistemden sorumludur.

P05 ANTİ-VİRÜS POLİTİKASI

1. Amaç

CBÜ' deki bütün bilgisayarların efektif virüs algılama ve engelleme standardına sahip olması için gereklilikleri belirlemektir.

2. Kapsam

Bu politika CBÜ'de ki bütün PC tabanlı bilgisayarları kapsamaktadır. Bunlar desktop bilgisayarlar, file/ftp/tftp/proxy vb. sunuculardır.

3. Politika

Kurumun bütün pc tabanlı bilgisayarları anti-virüs yazılımına sahip olmalıdır ve belli aralıklarda düzenli olarak güncellenmelidir. Buna ek olarak anti-virüs yazılımı ve virüs patternleri otomatik olarak güncellenmelidir. Virüs bulaşan makineler tam olarak temizleninceye kadar ağdan çıkarılmalıdır. Sistem yöneticileri anti-virüs yazılımının sürekli ve düzenli çalışması ve bilgisayarların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur. Zararlı programları (solucan,truva atı vs) kurum bünyesinde oluşturmak ve dağıtmak yasaktır. Hiçbir kullanıcı herhangi bir sebepten dolayı anti-virüs programını sistemden kaldıramaz.

Anti-Virüs Prosesi

Virüs problemlerine karşı tavsiye edilen adımlar:

a) Anti-virüs güncellemeleri; her makinanın lokalinde otomatik update şeklinde gerçekleşmektedir.

b) Bilinmeyen kişilerden e-posta ile birlikte gelen dosya ve makroları kesinlikle açmayın. Bu ekli dosyaları hemen silin. Daha sonra silinmiş öğelerden tekrar silin.

c) Spam, zincir ve junk e-mailleri silin.

d) Bilinmeyen ve şüpheli kaynaklardan asla dosya indirmeyin.

e) Bilinmeyen kaynaklardan gelen CD'lere virüs tarama yapın.

f) Kritik data ve sistem konfigürasyonlarını düzenli aralıklar ile yedekleyin ve güvenli bir yerde saklayın.

P06 ŞİFRE POLİTİKASI

1. Genel Bakış

Şifreleme bilgisayar güvenliği için önemli bir özelliktir. Kullanıcı hesapları için ilk güvenlik katmanıdır. Zayıf seçilmiş bir şifre ağ güvenliğini tümüyle riske atabilir. CBÜ çalışanları ve uzak noktalardan erişenler aşağıda belirtilen kurallar dahilinde şifreleme yapmakla sorumludurlar.

2. Amaç

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

3. Kapsam

Bu politika kullanıcı hesabı olan (Bilgisayar ağına erişen ve şifre gerektiren kişiler) bütün kullanıcıları kapsamaktadır.

4. Politika

4.1 Genel

a) Bütün sistem seviyeli şifreler (örnek, root, administrator) en az 3 ayda bir değiştirilmelidir.

b) Bütün kullanıcı seviyeli şifreler (örnek, e-posta, web vs.) en az 3 ayda bir değiştirilmelidir. Tavsiye edilen değiştirme süresi ayda birdir.

c) Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.

d) Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.

e) Kullanıcı, şifresini başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlara yazmaması konusunda eğitilmelidir.

f) Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de kolayca kırılamayacak güçlü bir şifreye sahip olmalıdır.

g) Bir kullanıcı adı ve şifresi birim zamanda birden çok bilgisayarda kullanılmamalıdır.

4.2 Ana Noktalar

A. Genel Şifre Oluşturma Kuralları

Şifreler değişik amaçlar için kullanılmaktadır. Bunlardan bazıları: Kullanıcı şifreleri, Web erişim şifreleri, e-posta erişim şifreleri, ekran koruma şifreleri, yönlendirici erişim şifreleri vs. Bütün kullanıcılar güçlü bir şifre seçimi hakkında özen göstermelidir.

Zayıf şifreler aşağıdaki karakteristiklere sahiptir.

a) Şifreler sekizden daha az karaktere sahiptir.

b) Şifreler sözlükte bulunan bir kelimeye sahiptir.

c) Şifreler 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 Şifreler aşağıdaki karakteristiklere sahiptir.

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

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

c) En az sekiz adet alfanumerik karaktere sahiptir.

d) Herhangi bir dildeki argo lehçe veya teknik bir kelime olmamalıdır.

e) Şifreler herhangi bir yere yazılmamalıdır veya elektronik ortamda tutulmamalıdır.

B. Şifre Koruma Standartları

CBÜ bünyesinde kullanılan şifreleri kurum dışında herhangi bir şekilde kullanmayınız. Kimse ile paylaşmayınız. İlgili şifreler CBÜ‘e ait gizli bilgiler olarak düşünülmelidir. Değişik sistemler için farklı şifreleme kullanın.

a) Aşağıdakiler yapılmayacaklar listesidir.

- Herhangi bir kişiye telefonda şifre vermek,
- E-posta mesajlarında şifre belirtmek,
- Üst yöneticinize şifreleri söylemek,
- Başkaları önünde şifreler hakkında konuşmak,
- Aile isimlerini şifre olarak kullanmak,

- Şifreleri işten uzakta olduğunuzda iş arkadaşlarınıza bildirmek,

b) Uygulamalardaki "şifre hatırlatma " özelliklerini seçmeyiniz.

c) Şifreler en fazla 3 ayda bir değiştirilmelidir. Tavsiye edilen aralık ise ayda birdir.

d) Şifrelerin değiştirilip değiştirilmediği yapılan testler ile takip edilir.

C. Uygulama Geliştirme Standartları

Uygulama geliştiricileri programlarındaki aşağıdaki güvenlik özelliklerinin sağlandığından emin olmalıdırlar.

a) Bireylerin (grupların değil) kimlik doğrulaması işlemini destekleyebilmelidir.

b) Şifreleri text olarak veya kolay anlaşılabilir formda saklamamalıdır.

c) Kural yönetim sistemini desteklemelidir.

D Uzaktan Erişen Kullanıcılar İçin Şifre Kullanımı

Kurumun bilgisayar ağına uzaktan erişim tek yönlü şifreleme algoritması veya güçlü bir passphrase ile yapılacaktır.

E Passphrase

a) Bir passphrase standart şifrelerden 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.

b) Passphrase'ler şifreler gibi değildir. Passphrase şifrelerden daha uzundur, dolayısı ile daha güvenlidir.

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

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

e) "?*@102incicaddedekiTrafik*&#!#Busabah"

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

P07 KABLOSUZ İLETİŞİM POLİTİKASI

1. Amaç

Bu politika kablosuz cihazların gerekli güvenlik tedbirleri alınmaksızın kurumun bilgisayar ağına erişimini engellemeyi amaçlamaktadır. Sadece bu politikanın güvenlik kriterlerine uyan cihazlar kurumun bünyesinde kullanabilirler.

2. Kapsam

Bu politika kurum bünyesinde kullanılabilecek bütün kablosuz haberleşme cihazlarını kapsamaktadır. Kablosuz veri transferi sağlayabilen herhangi bir cihaz bunun kapsamındadır. Kuruma bağlantısı olmayan herhangi bir cihaz veya bilgisayar ağı bu politikanın kapsamı içerisinde değildir.

3.Politika

3.1 Onaylanmış Teknoloji

Bütün kablosuz erişim cihazları yetkili birim tarafından onaylanmış olmalıdır ve belirlenen güvenlik ayarlarını kullanmalıdır.

3.2 Güvenlik Ayarları

a) Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmalıdır. Bunun için Wi-Fi Protected Access şifreleme kullanılmalıdır.

b) Erişim cihazlarındaki firmwareleri düzenli olarak güncellenmelidir. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlar.

c) Erişim cihazlarını kolayca erişilebilir bir yerde olmaması gereklidir. Çünkü cihaz resetlendiğinde fabrika ayarlarına geri dönebilmekte ve güvenlik açığı oluşturabilmektedir.

d) Cihaza erişim için güçlü bir şifre kullanılmalıdır. Erişim şifreleri varsayılan ayarda bırakılmamalıdır.

e) Varsayılan SSID isimlerini kullanmayınız. SSID bilgisi içerisinde kurumla ilgili bilgi olmamalıdır. Mesela kurum ismi, ilgili bölüm çalışanın ismi vs.

f) Erişim cihazları üzerinden gelen kullanıcılar Firewall üzerinden ağa dahil olmalıdırlar.

g) Kullanıcı bilgisayarlarında kişisel firewall yazılımları yüklü olmalıdır.

h) Kritik yerlerde kullanıcılar VPN teknolojilerini kullanarak kurum ağına erişmelidirler.

j) Hem kullanıcılar hem de erişim cihazları statik IP adresleri kullanmalıdır. Aynı zamanda donanım adresleme kullanılmalıdır.

k) Erişim cihazlarını bir yönetim yazılımı ile devamlı olarak gözlemlenmelidir. Sistemde hackerler tarafından konulmuş casus bir erişim cihazı olabilir veya mevcut erişim cihazı resetlenmiş olup kurumun güvenlik politikalarına aykırı bir şekilde ayar yapılmış olabilir.

l) Kablosuz ağa dahil olan kurum çalışanları için bile erişimler sınırlandırılmalıdır. Sadece internete çıkacak olan kullanıcıların kablosuz ağ üzerinden diğer uygulamaların (ses, güvenlik, mobilite vb) çalıştığı networklere erişimi engellenmeli gerekirse networkler farklı IP aralıkları üzerinde ayarlanmalı, cihaz üzerinde Access Control Listler (Yetki kuralları) oluşturulmalıdır.

P08 UZAKTAN ERİŞİM POLİTİKASI

1. Amaç

Bu politikanın amacı herhangi bir yerden kurumun bilgisayar ağına erişilmesine ilişkin standartları saptamaktır. Bu standartlar kaynaklarının yetkisiz kullanımından dolayı kuruma gelebilecek potansiyel zararları minimize etmek için tasarlanmıştır. Bu zararlar şunlardır; CBÜ'nün gizli ve hassas bilgilerin kaybı, prestij kaybı ve içerideki kritik sistemlerde meydana gelen zararlar vs.

2. Kapsam

Bu politika kurumun bütün çalışanlarını, sözleşmelileri veya kurum adına çalışanları ve kısaca kurumun herhangi bir birimindeki bilgisayar ağına erişen bütün kişi ve kurumları kapsamaktadır.

Bu politika, kuruma bağlı bütün uzak erişim bağlantılarını kapsamaktadır ve bunun içerisine e-posta okuma veya gönderme ve intranet web kaynaklarını gözlemleme dâhildir. Bütün uzaktan erişim uygulamaları bu politika tarafından kapsanmaktadır. Modemden port yönlendirmesi (RDP), VPN ile sınırlıdır.

3. Politika

3.1Genel

a) Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir.

b) Uzaktan erişim metotları ile kuruma bağlantılarda bilgi sistemlerinin güvenliğinin sağlanması için aşağıdaki politikalara göz atmak gerekmektedir.

Kabul edilebilir şifreleme politikası

Sanal Özel Ağ (VPN) Politikası

3.2 Gereklilikler

a) İnternet üzerinden kurumun herhangi bir yerindeki bilgisayar ağına erişen kişi veya kurumlar VPN teknolojisini kullanacaklardır. Bu, veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlayacaktır. VPN teknolojileri IpSec , L2TP, SSL, PPTP vs. protokollerinden birini içermelidir.

b) Mümkünse uzaktan erişim güvenliği sıkı bir şekilde denetlenmelidir. Kontrol tek yönlü şifreleme (one time password authentication) veya güçlü bir passphrase (uzun şifre) destekli public /private key sistemi kullanılması tavsiye edilmektedir. Daha fazla bilgi için şifreleme bölüme bakınız.

c) Kurum çalışanları hiçbir şekilde kendilerinin login ve e-posta şifrelerini aile bireyleri dâhil olmak üzere hiç kimseye veremezler.

d) Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmadıklarından emin olmalıdırlar. Kullanıcının tamamıyla kontrolünde olan ağlarda bu kural geçerli değildir.

e) Çalışanlar kurum ile ilgili çalışmalarında kurumun dışındaki e-posta hesaplarını kullanamazlar.

g) Uzaktaki kullanıcı cihazını split-tunnel veya dual homing (VPN bağlantısı esnasında başka bir bağlantı daha yapmak) olarak konfigure edemez.

i) Kurum ağına standart dışı erişim isteğinde bulunan organizasyon veya kişiler birimin özel izni ile geçici olarak izin verilebilirler.

j) Periyodik olarak yapılan kontrollerle kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcı kimlikleri ve hesapları kaldırılmalıdır

P09 KRİZ / ACİL DURUM YÖNETİMİ POLİTİKASI

1.0 Amaç

Bu politika kurum çalışanlarının, bilgi güvenliği ve iş sürekliliği ile ilgili acil bir durum oluştuğunda sorumlulukları dâhilinde gerekli müdahale yapabilmelerine yönelik standartları belirlemektedir. İzlenen olayın uygun şekilde raporlanması ve belirlenen önlem ve acil durum faaliyetlerinin uygulanması önemlidir.
Kurum çalışanlarının, bilgi güvenliği veya iş sürekliliği ile ilgili acil bir durum oluştuğunda sorumlulukları dâhilinde gerekli müdahaleyi yapabilmelerine yönelik normlar aşağıda belirtilmiştir.

2.0 Kapsam

Bahse konu acil durum senaryoları yaşanmadan önce uygun acil durum hareket planının yapılması esastır. Bilgi güvenliğine yönelik tehlike senaryolarından bazıları sistemlere yapılacak direkt saldırılar, zararlı kod içeren programların, kişilerin sisteme sızması, bilginin hırsızlığı, dışarıdan veya içeriden gerçekleştirilebilecek saldırı öncesi taramalar olarak tanımlanabilir.

3.0 Politika

a) Acil durum sorumluları atanmalı ve yetki ve sorumlulukları belirlenmeli ve dökümante edilmelidir.
b) Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınmalıdır. Örneğin uygulama veya veritabanı sunucularından donanım ve yazılıma ait problemler oluştuğunda yerel veya uzak sistemden yeniden kesintisiz çalışma sağlanabilmelidir.
c) Kurum bilişim sistemlerinin kesintisiz çalışmasını sağlaması için aynı ortamda kümeleme veya uzaktan kopyalama veya pasif sistem çözümlerini hayata geçirilebilir. Kurumlar sistemlerini tasarlarken ne kadar süre iş kaybını tolere edeceklerini göz önüne almalıdırlar.
d) Acil durumlarda kurum içi işbirliği gereksinimleri tanımlanmalıdır.
e) Acil durumlarda sistem logları incelenmek üzere saklanmalıdır.
f) Güvenlik açıkları ve ihlallerinin rapor edilmesi için kurumsal bir mekanizma oluşturulmalıdır.
g) Yaşanan acil durumlar sonrası politikalar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilmelidir.
h) Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulmalı ve bu bildirim süreçleri tanımlanmış olmalıdır.
i) Acil durum kapsamında değerlendirilen olaylar aşağıda farklı seviyelerde tanımlanmıştır.
- Seviye A: Bilgi kaybı. Kurumsal değerli bilgilerin yetkisiz kişilerin eline geçmesi, bozulması, silinmesi
- Seviye B: Servis kesintisi. Kurumsal servislerin kesintisi veya kesintisine yol açabilecek durumlar

- Seviye C: Şüpheli durumlar. Yukarıda tanımlı ilk iki seviyedeki duruma sebebiyet verebileceğinden şüphe duyulan ancak gerçekliği ispatlanmamış durumlar.

j) Acil durumlarda BGYS yöneticisine erişilmeli, ulaşılamadığı durumlarda koordinasyonu sağlamak üzere önceden tanımlanmış ilgili yöneticiye bilgi verilmeli ve zararın tespit edilerek süratle daha önceden tanımlanmış felaket kurtarma faaliyetleri yürütülmelidir.

k) BGYS yöneticisi tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmek üzere ilgili makamlara iletilmelidir.

P10 FİZİKSEL GÜVENLİK POLİTİKASI

1.0 Amaç

Bu politika kurum personeli ve kritik kurumsal bilgilerin korunması amacıyla sistem odasına, kurumsal bilgilerin bulundurulduğu sistemlerin yer aldığı tüm çalışma alanlarına ve kurum binalarına yetkisiz girişlerin yapılmasını önlemek amacını taşımaktadır.

2.0 Kapsam

Kurum binalarında yer alan bilgi varlıklarına erişim sağlayan tüm fiziksel güvenlik konularını kapsamaktadır.

3.0 Politika

a) Kurumun fiziksel olarak korunması, farklı koruma mekanizmaları ile donatılması temin edilmelidir.
b) Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binada ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanmalı ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilmelidir.
c) Kurum dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili görevliler gözetiminde gerçekleştirilmelidir.
d) Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin güncelliği sağlanmalıdır.
e) Kritik sistemler özel sistem odalarında tutulmalıdır.
f) Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmalı, yangın ve benzer felaketlere karşı koruma altına alınmalıdır.
g) Fotokopi, yazıcı vs türü cihazlar mesai saatleri dışında kullanıma kapatılmalı, mesai saatleri içerisinde yetkisiz kullanıma karşı koruma altına alınmalıdır.
h) Kuruma giriş yapacak ziyaretçi veya kurye teslimatları yetkili görevliler gözetiminde gerçekleştirilmelidir.
j) Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve kontrol altında tutulması temin edilmelidir.
k) Fotoğraf, video, ses vb. kayıt cihazlarının yetki verilmeyen kişiler tarafından güvenli alanlara sokulması yasaklanmalıdır.

P11 SUNUCU GÜVENLİK POLİTİKASI

1. Amaç

Bu politikanın amacı kurumun sahip olduğu sunucularının temel güvenlik konfigürasyonları için standartları belirlemektir. Bu politikanın etkili kullanılması ile CBÜ bünyesindeki bilgilere ve teknolojiye yetkisiz erişimler minimize edilecektir.

2. Kapsam

Bu politika kurumun sahip olduğu bütün dahili sunucular için geçerlidir.

3. Politika

3.1 Sahip Olma ve Sorumluluklar

Kurum bünyesindeki bütün dahili sunucuların yönetiminden sadece yetkilendirilmiş sistem yöneticileri sorumludur. Sunucu konfigürasyonları sadece bu gruptaki kişiler tarafından yapılacaktır.

a) Bütün sunucular (kurumun sahip olduğu) ilgili kurumun yönetim sistemine kayıtlı olmalıdır.

En az aşağıdaki bilgileri içermelidir.

- Sunucuların yeri ve sorumlu kişi
- Donanım ve işletim sistemi
- Ana görevi ve üzerinde çalışan uygulamalar
- İşletim sistemi versiyonları ve yamalar

b) Bütün bilgiler tek bir merkezde güncel olarak tutulmalıdır.

3.1 Genel Konfigürasyon Kuralları

a) İşletim sistemi konfigürasyonları kurumun bilgi işlem biriminin talimatlarına göre yapılacaktır.

b) Kullanılmayan servisler ve uygulamalar kapatılmalıdır.

c) Active directory de 1 hafta süreyle loglanacaktır. (IP bazlı)

d) Üniversite içi yapılan bağlantılar RDC ile yapılmaktadır.

e) Üniversite dışı yapılan bağlantılar müşterinin belirlediği kurallara göre yapılmaktadır

f) Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdırlar.

3.2 Gözlemleme

a) Kritik sistemlerde oluşan bütün güvenlikle ilgili olaylar loglanmalı ve aşağıdaki şekilde saklanmalıdır.

- IP bazlı olarak 6 ay süreyle erişilebilmelidir.

b) Güvenlikle ilgili loglar sorumlu kişi tarafından değerlendirilecek ve gerekli tedbirler alınacaktır. Güvenlikle ilgili olaylar aşağıdaki gibi olabilir fakat bunlarla sınırlı değildir.

- Yetkisiz kişilerin ayrıcalıklı hesaplara erişmeye çalışması
- Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar

3.3 Uygunluk

- Denetimler yetkili organizasyonlar tarafından kurum bünyesinde belli aralıklarda yapılmalıdır.
- Denetimlerde kurumun işleyişine zarar vermemesi için maksimum gayret gösterilecektir.

3.4 İşletim

- Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir.
- Sunucuların yazılım ve donanım bakımları 1 aylık sürelerde, sistem yöneticileri tarafından yapılmalıdır.
- Sistem odalarına yetkisiz girişler engellenmelidir. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalıdır.

P12 AĞ CİHAZLARI GÜVENLİK POLİTİKASI

1.0 Amaç

Bu doküman Kurumun ağındaki yönlendirici (router) ve anahtarların (switch) sahip olması gereken minimum güvenlik konfigürasyonlarını tanımlamaktadır.

2.0 Kapsam

Kurumun ağına bağlı olan ağ cihazları için geçerlidir.

3.0 Politika

Bütün yönlendirici ve anahtarlar aşağıdaki konfigurasyon standartlarına sahip olmalıdır.

a) Bilgisayar ağında bulunan tüm cihazların IP ve MAC adres bilgileri envanter dosyasında yer alacaktır.

b) Aşağıdakileri yapmayınız

- IP directed broadcasts
- RFC1918 de tanımlandığı gibi yönlendirici giriş portuna gelen geçersiz IP adresleri
- Source routing
- Yönlendiricide çalışan web servisleri

c) Kurumun standart SNMP community stringlerini kullanılmalıdır.

d) Yönlendirici ve anahtarlar kurumun yönetim sisteminde olmalıdır.

e) Yazılım ve firmware güncellemeleri önce test ortamlarında denendikten sonra çalışma günlerinin dışında üretim ortamına taşınacaktır.

f) Bilgisayar ağında bulunan kabinetler, aktif cihazlar, UTP kabloları, cihazların portları etiketlenecektir.

"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."

P13 AĞ YÖNETİMİ POLİTİKASI

1.0 Amaç

Kurumun bilgisayar ağında yer alan bilgilerin ve ağ alt yapısının güvenliği, gizlilik, bütünlük ve erişilebilirlik kavramları göz önüne alınarak sağlanmalıdır. Uzaktan erişim hususunda özel önem gösterilmelidir. Yetkisiz erişimle ilgili tedbirler alınmalıdır. Ağın güvenliği ve sürekliliğini sağlamak amacıyla birtakım kontroller gerçekleştirilmelidir. Ağ Yönetimi politikası bu gereksinimleri karşılayan kuralları belirlemek amacıyla geliştirilmiştir.

2.0 Kapsam

CBÜ bilgisayar ağının sistem ve ağ yöneticileri, teknik sorumluları faaliyetlerini Ağ Yönetimi Politikasına uygun şekilde yürütmekle yükümlüdür.

3.0 Politika

a) Ağın kontrol edeceği alan belirlenmelidir.

b) Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için özel kontroller uygulanmalıdır.

c) Ağ servisleriyle ilgili standartlarda, erişimine izin verilen ağlar ve ağ servisleri ve ilgili yetkilendirme yöntemleri belirtilmelidir.

d) Ağ üzerinde kullanıcının erişeceği servisler kısıtlanmalıdır.

e) Sınırsız ağ dolaşımı engellenmelidir.

f) İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden teknik önlemler alınmalıdır.

g) Ağ erişimi gerek duyulduğunda VPN, VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılmalıdır.

h) Uzaktan teşhis ve müdahale için kullanılacak portların güvenliği sağlanmalıdır.

i) Gerek görülen uygulamalar için e-posta, tek yönlü dosya transferi, çift yönlü dosya transferi, etkileşimli erişim, güne ve günün saatine bağlı erişim gibi uygulama kısıtlamalarıyla ağ erişimi denetimi yapılmalıdır.

j) Ağ üzerindeki yönlendirme kontrol edilmelidir.

k) Bilgisayar ağına bağlı bütün makinelerde kurulum ve konfigürasyon parametreleri kurumun güvenlik politika ve standartlarıyla uyumlu olmalıdır.

l) Sistem tasarım ve geliştirmesi yapılırken kurum tarafından onaylanmış olan ağ ara yüzü ve protokolleri kullanmalıdır.

m) İnternet trafiği erişim ve kullanımı izleme politikası ve ilgili standartlarda anlatıldığı şekilde izlenebilecektir.

n) Bilgisayar ağındaki adresler, ağa ait konfigürasyon ve diğer tasarım bilgileri 3.şahıs ve sistemlerin ulaşamayacağı bir şekilde saklanmalıdır.

o) Ağ üzerindeki firewalllar üzerinde, ilgili konfigürasyon dokümanlarında belirtilen servisler dışında tüm servisler kapatılmalıdır.

p) Bilgisayar ağıyla ilgili sorumlulukları desteklemek amacıyla ağ dokümantasyonu hazırlanmalı, ağ cihazlarının güncel konfigürasyon bilgileri saklanmalıdır.

P14 RİSK DEĞERLENDİRME POLİTİKASI

1. Amaç

Kurumun bilgisayar ağında sistem açıklarını tespit etmek ve gerekli tedbirlerin alınmasını sağlamak amacıyla yetkili birimlere risk analizi yaptırılmasına dair kuralları belirlemektir.

2. Kapsam

Sistemi mükemmelleştirmeyi amaçlayan bu programın çalıştırılması, geliştirmesi ve uygulaması kurum ve ilgili birliğin sorumluluğundadır. Risk analizi süresince çalışanlar gerekli noktalarda yardımcı olacaklardır. Risk değerlendirme çalışmaları esnasında sistemler üzerinde servis reddi veya herhangi bir sebeple iş sürekliliği aksatılmayacaktır.

3. Politika

Sistemi mükemmelleştirmeyi amaçlayan risk değerlendirme yöntemlerinin geliştirilmesi, uygulanması ve denetlenmesi BGYS ekibinin ve bilgi işlemin sorumluluğundadır. Risk analizi raporları BGYS Ekip Lideri'ne onaylatılır. Risk ve uygunsuzluklar giderilene kadar raporlar Bilgi İşlem Sorumlusu tarafından gerekli fiziksel güvenlik önlemleri alınmış alanlarda muhafaza edilir.

P15 DONANIM VE YAZILIM ENVANTERİ OLUŞTURMA POLİTİKASI

1.0 Amaç

Bu politika kurumun sahip olduğu donanım ve yazılımların envanterinin oluşturulması ile ilgili kuralları belirlemektedir

.

2.0 Kapsam

Bu politika kurum bünyesinde kullanılan bütün donanım ve yazılımları kapsamaktadır. Bu politikanın uygulanmasından yetkili ve birim yöneticileri sorumludur.

3.0 Politika

Bütün cihazların formal donanım ve yazılım envanteri oluşturulmalı ve güncel tutulmalıdır.

a) Oluşturulan envanter tablosunda şu bilgiler olmalıdır; Sıra No, Bilgisayar Adı, Bölüm, Marka, Model, Seri no, Özellikler, Ek aksamlar, İşletim sistemi vs.
b) Bu tablolar merkezi bir web sunucuda tutulacak ve belirli periyotlarda ilgili kurum tarafından güncellenecektir.
c) Bilgi güncelleme denetimi bilgi işlem birimi tarafından yapılacaktır.
d) Envanter bilgisi doğru bir şekilde tutulmalıdır. Eksik veya yanlış envanter bilgisi ileride yapılacak donanım ve yazılım değişikliklerinde sağlıklı karar alınmasını engelleyebilir.
e) Envanter bilgileri sık sık kontrol edilmelidir. Envanter bilgisi eksikliğinden dolayı oluşacak hırsızlık veya değişim ciddi kayıplara yol açabilir.

P16 VERİTABANI GÜVENLİK POLİTİKASI

1.0 Amaç

Kurumun veri tabanı sistemlerinin, kesintisiz ve güvenli şekilde işletilmesine yönelik standartları tanımlar.

2.0 Kapsam

Tüm veri tabanı sistemleri, bu politikaların kapsamı altında yer alır.

3.0 Politika

d) Veri tabanı envanteri, tanımlanır ve dokümante edilir.
e) Veri tabanı kullanım şekli belirlenir ve dokümante edilir.
f) Kritik verilere erişim işlemleri (okuma, değiştirme, silme, ekleme) loglanır. Log kayıtlarına, idarenin izni olmadan kesinlikle hiçbir şekilde erişim yapılamaz.
g) Veri tabanı sistemlerinde tutulan bilgiler sınıflandırılır ve uygun yedekleme politikaları oluşturulur. Yedeklemeden sorumlu sistem yöneticileri belirlenir ve yedeklerin düzenli alınması sağlanır.
h) Yedekleme talimatına uyulur.
i) Veri tabanı erişimi, PR.15 Sistem Güvenliği Prosedürü çerçevesinde oluşturulur.
j) Hatadan arındırma ve geri yedekleme kuralları, "Acil Durum Yönetimi" politikasına uygun olarak oluşturulur ve dokümante edilir.
k) Bilgilerin saklandığı sistemler, fiziksel güvenliği sağlanmış sistem odalarında tutulur.
l) Veri tabanı sistemlerinde yapılacak bakım onarım, yama ve güncelleme çalışmalarından önce, ilgili yetkililer bilgilendirilir.
m) Bilgi saklama medyaları, BGYS Ekip Lideri'nin yazılı onayı olmadan, kurum dışına çıkarılamaz.
n) Ortaya çıkan beklenmedik durumlarda, destek için önceden belirlenmiş personel ile iletişime geçilir.
o) Veri tabanı sunucularına erişim şifreleri, kapalı ve imzalı bir zarfla, çelik kasada saklanır. Zarfın açılması gerektiğinde,BGYS yönetim temsilcisine bildirilir.
p) Veri tabanı sunucusuna, sadece admin hakkına sahip olanlar bağlanır. (Erişim ve Kullanım Matrisi)
q) Bağlanacak kişilerin kendi adına kullanıcı adı verilir ve yetkilendirme yapılır.
r) Bütün kullanıcıların yaptıkları işlemler, loglanır.

P17 DEĞİŞİM YÖNETİMİ POLİTİKASI

1.0 Amaç

Kurumun bilgi sistemlerinde yapılması gereken konfigürasyon değişikliklerinin güvenlik ve sistem sürekliliğini aksatmayacak şekilde yürütülmesine yönelik politikaları belirler.

2.0 Kapsam

Tüm bilgi sistemleri ve bu sistemlerinden işletilmesinden sorumlu personel bu politikanın kapsamında yer almaktadır.

3.0 Politika

a) Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümante edilmelidir.

b) Yazılım ve donanım envanteri oluşturularak, yazılım sürümleri kontrol edilmelidir.

c) Herhangi bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenmeli ve dokümante edilmelidir.

d) Değişiklikler gerçekleştirilmeden önce kurumun ilgili biriminden onay alınmalıdır.

e) Tüm sistemlere yönelik yapılandırma dokümantasyonu oluşturulmalı, yapılan her değişikliğin bu dokümantasyonda güncellenmesi sağlanarak kurumsal değişiklik yönetimi ve takibi temin edilmelidir.

f) Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanmalı ve ilgili yöneticiler tarafından onaylanması sağlanmalıdır.

g) Ticari programlarda yapılacak değişiklikler, ilgili üretici tarafından onaylanmış kurallar çerçevesinde gerçekleştirilmelidir.

h) Teknoloji değişikliklerinin kurumun sistemlerine etkileri belirli aralıklarla gözden geçirilmeli ve dokümante edilmelidir.

i) Değişiklik yönetimini işletmek için bir talep yönetim sistemi kurmak ve işletmek önemlidir. Talebin nasıl alınacağı ve değerlendirileceği gibi esaslar tanımlanmalıdır.

j) Değişiklik onayının, “hangi kontroller ne şekilde yapıldıktan sonra verileceği” tanımlanmalıdır.

k) Değişiklik öncesi test süreci tanımlanmalıdır.

l) Değişikliğin varlık kritikliğine göre yapılacağı zaman ve yöntemler tanımlanmalıdır.

P18 GÜVENLİK AÇIKLARI TESPİT ETME POLİTİKASI

1.0 Amaç

Bu politikanın amacı kurumun bilgisayar ağının (firewall, sunucu vs.) güvenlik açıklarına karşı taranması hususunda politika belirlemektir.

Denetim Sebepleri:

- Bilgi kaynaklarının bütünlüğü ve gizliliğini sağlamak
- Kurumun güvenlik politikalarına uyumunun kontrolü için güvenlik açıklarının tespit edilmesi
- Gerektiği zaman kullanıcıların veya sistemin aktivitelerini kontrol etmek

2.0 Kapsam

Bu politika CBÜ bünyesinde sahip olunan bütün bilgisayar ve haberleşme cihazlarını kapsamaktadır. Bu politika kurumun bünyesinde bulunan fakat kurumun sahip olmadığı herhangi bir sistemi de kapsamaktadır. Denetim yapan kişi veya kurum hizmetlerin durdurulması aktivitesi yapmayacaktır.

2.0 Politika

İstenildiğinde denetim yapan firmanın bireylerine erişim izni verilecektir. Kurumun birimleri denetim yapan firmaya ağ taraması yapması için protokol, adres bilgileri, ağ bağlantıları hakkında bilgi verecektir.

3.1 Tarama esnasında muhatap olan kişi

Kurum denetimi yapan firmaya oluşabilecek sorunlar hakkında danışabileceği bir kişiyi yazılı olarak verecektir.

3.2 Tarama Periyodu

Kuruma denetim yapacak olan firma denetim yapılacak zamanı yazılı olarak bildirecektir.

3.3 Gizlilik Anlaşması

Kurum ile güvenlik taraması yapacak firma, tarama sonucunda elde edilecek bilgilerin hiçbir şekilde üçüncü şahıslara aktarılmayacağına dair gizlilik anlaşması yapacaktır.

P19 SANAL ÖZEL AĞ (VPN) POLİTİKASI

1.0 Amaç

Bu politikanın amacı VPN protokolünün kullanım standartlarını belirlemektir.

2.0 Kapsam

Bu politika VPN ile müşteri ağına bağlanacak kurumları, çalışanları, sözleşmelileri, danışmanları, geçici çalışanları ve diğer bütün personeli kapsamaktadır. Bu politika VPN bağlantılarının sonlandırıldığı ürünlere uygulanacaktır.

3.0 Politika

CBÜ yetkili çalışanları ve üçüncü şahıslar VPN'in faydalarından yararlanabilirler. Kullanıcılar varsa müşterinin tercih ettiği internet sağlayıcıyı kullanmak zorundadırlar, müşteriden konu ile ilgili bir açıklama gelmemesi durumunda istedikleri internet sağlayıcıyı kullanabilirler.

Buna ek olarak,

a) VPN kullanım hakkı verilen kişiler yetkisiz kişilere bu hakkı kullandırmaması için gerekli tedbirleri almakla sorumludur.

b) Kurum ağına bağlanıldığında, PC'den çıkan ve giren trafik sadece VPN kanalından iletilecektir ve diğer bütün trafik düşecektir.

c) Çift tünel sistemine izin verilmemektedir, sadece tek ağ bağlantısına izin verilmektedir.

d) Kurumun VPN ağ geçitlerinin kurulması ve yönetimi müşteriye ait yetkili personel tarafından yapılacaktır.

e) Kuruma ait bilgisayarlara sahip olmayan kişiler CBü'nün VPN ve ağ politikalarına uygun bir şekilde cihazlarını konfigüre etmelidirler.

f) Sadece kurumun onay verdiği kullanıcılar VPN'i kullanabilir.

g) VPN teknolojisini kendi kişisel cihazları ile kullanan kişiler şunu bilmelidirler ki, bütün makineler kurum ağının bir parçasıdır bundan dolayı CBÜ, sorumlu olduğu cihazlar ile aynı kurallara sahiptir ve aynı güvenlik politikaları ile kon figüre edilmelidir.

P20 KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI

1.0 Amaç

Kurumun bilgi sistemlerine erişimde kimlik doğrulaması ve yetkilendirme politikalarını tanımlamaktır.

2.0 Kapsam

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

3.0 Politika

a) Kurum sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenecektir.
b) Kurum sistemlerine erişmesi gereken kullanıcılara yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanacak.
c) Kurum bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veri tabanları, işletim sistemleri ve log-on olarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkiler belirlenmeli, denetim altında tutulmalıdır.
e) Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilmelidir.
f) Kullanıcılar da kurum tarafından kullanımlarına tahsis edilen sistemlerin güvenliğinden sorumludur.
g) Sistemler başarılı ve başarısız erişim logları düzenli olarak tutulmalı, tekrarlanan başarısız log-on girişimleri incelenmelidir.
h) Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.
I) Sistemlere log-on olan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve yetki ihlalleri kontrol edilmelidir.
k) Kullanıcı hatalarını izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.

P21 BİLGİ SİSTEMLERİ YEDEKLEME POLİTİKASI

1.0 Amaç

Bilgi Sistemlerinde oluşabilecek hatalar karşısında sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için sistemler üzerindeki konfigürasyon, sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmesi gerekir. Bu politika yedekleme kurallarını tanımlamaktadır.

2.0 Kapsam

Tüm kritik bilgi sistemleri ve bu sistemlerin işletilmesinden sorumlu personel bu politikanın kapsamında yer almaktadır.

3.0 Politika

a) Bilgi sistemlerinde oluşabilecek hatalar karşısında; sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigürasyon, sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmesi gerekmektedir.
b) Verinin operasyon el ortamda online olarak aynı disk sisteminde farklı disk volümlerinde ve offline olarak manyetik kartuş, DVD veya CD ortamında yedekleri alınmalıdır.
c) Taşınabilir ortamlar fiziksel olarak bilgi işlem odalarından farklı odalarda ve güvenli bir şekilde saklanmalıdır. Veriler offline ortamlarda en az 30 yıl süreyle saklanmalıdır.
d) Kurumsal kritik verilerin saklandığı sistemler ile sistem kesintisinin kritik olduğu sistemlerin bir varlık envanteri çıkartılmalı ve yedekleme ihtiyacı bakımından sınıflandırılarak dokümante edilmelidir.
e) Yedekleme konusu bilgi güvenliği süreçleri içinde çok önemli bir yer tutmaktadır. Bu konuyla ilgili sorumluluklar tanımlanmalı ve atamalar yapılmalıdır.
f) Yedekleri alınacak sistem, dosya ve veriler dikkatle belirlenmeli ve yedeği alınacak sistemleri belirleyen bir yedekleme listesi oluşturulmalıdır.
g) Yedek ünite üzerinde gereksiz yer tutmamak üzere, kritiklik düzeyi düşük olan veya sürekli büyüyen izleme dosyaları yedekleme listesine dahil edilmemelidir.
h) Yedeklenecek bilgiler değişiklik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilmeli ve güncellenmelidir.
i) Yeni sistem ve uygulamalar devreye alındığında yedekleme listeleri güncellenmelidir.
j) Yedekleme işlemi için geçerli sayı ve kapasitede yedek üniteler seçilmeli ve temin edilmelidir. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilmelidir.
k) Yedekleme ortamlarının düzenli periyotlarda test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanmalıdır.
l) Geri yükleme prosedürlerinin düzenli olarak kontrol ve test edilerek etkinliklerinin doğrulanması ve operasyon el prosedürlerin öngördüğü süreler dahilinde tamamlanabileceğinden emin olunması gerekir.
m) Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanmalıdır.

n) Yedekleme standardı ile doğru ve eksiksiz yedek kayıt kopyalarının bir felaket anında etkilenmeyecek bir ortamda bulundurulması gerekmektedir.

o) Veri Yedekleme Standardı; yedekleme sıklığı, kapsamı, gün içinde ne zaman yapılacağı, ne koşullarda ve hangi aşamalarla yedeklerin yükleneceği ve yükleme sırasında sorunlar çıkarsa nasıl geri dönüleceği, yedekleme ortamlarının ne şekilde işaretleneceği, yedekleme testlerinin ne şekilde yapılacağı ve bunun gibi konulara açıklık getirecek şekilde hazırlanmalı ve işlerliği periyodik olarak gözden geçirilmelidir.

P22 BAKIM POLİTİKASI

1.0 Amaç

Kurum bilgi sistemlerinde kullanılan sistemlerin bakımı ile ilgili politikaları belirlemektir.

2.0 Kapsam

Bakım politikası, kurum bilgi sistemlerini işletmekle sorumlu sistem yöneticilerini kapsar.

3.0 Politika

a) Kurum sistemlerinin tamamı periyodik bakım güvencesine alınmalıdır. Bunun için gerekli zaman planlamaları yapılmalıdır.
b) Üreticilerden sistemler ile ilgili bakım prosedürleri sağlanmalıdır.
c) Teknik destek elemanlarının bakım yaparken "CBÜ Bilgi Güvenlik Politikaları" na uygun davranmaları sağlanmalı ve kontrol edilmelidir.
d) Sistem üzerinde yapılacak değişiklikler ile ilgili olarak "Değişim Yönetimi Politikası" ve ilişkili standartlar uygulanmalıdır.
e) Bakım yapıldıktan sonra tüm sistem dokümantasyonu güncellenmelidir.
f) Sistem bakımlarının ilgili politika ve standartlar tarafından belirlenmiş kurallara aykırı bir sonuç vermediğinden ve güvenlik açıklarına yol açmadığından emin olmak için periyodik güvenlik ve uygunluk testleri yapılmalıdır.
g) Sistem bakımından sonra bir güvenlik açığı yaratıldığından şüphelenilmesi durumunda "CBÜ Bilgi Güvenlik Politikaları" uyarınca hareket edilmelidir.

P23 FİRMALAR İÇİN UZAKTAN ERİŞİM POLİTİKASI

1.0 Amaç

Bu politikanın amacı firmaların herhangi bir yerden kurumun bilgi sistemlerine erişmesine ilişkin normları belirlemektir.

2.0 Kapsam

Bu politika kuruma uzaktan hizmet veren kişi veya kurumları kapsamaktadır.

3.0 Politika

a) Kurum ve internet arasında şifreli iletişim hatları kullanılacaktır; internet üzerinden kurumun herhangi bir yerindeki bilgisayara erişen kişi veya kurumlar VPN teknolojisini kullanacaklardır.
b) Uzaktan erişilen yer mutlaka statik IP ye sahip olmalı ve bu IP kurumun güvenlik cihazlarında tanımlanmış olmalıdır.
c) Üniversite uzaktan kimlerin hangi rollerde kurum bilgisayarlarına eriştiğini belirtecek ve ayrıca ilgili kişilerin bilgisayarlara erişimde kullandığı kullanıcı adı ve şifreleri kurumdaki en üst yetkiliye teslim edecektir.
d) Kullanıcıların erişim şifreleri en az 4 ayda bir değiştirilecektir. Verilen şifreler kurumun şifreleme politikasına uygun olacaktır.
e) Firma, kurumun hiçbir bilgisini görüntüleyemez, ekran çıktısını alamaz, transfer edemez ve kurum dışına çıkartamaz. Aksi takdirde oluşacak yasal yükümlülüklerden firma sorumlu olacaktır.
f) Uzaktan erişim için mümkünse tek yönlü şifreleme veya güçlü bir uzun şifre destekli public/private key sistemi kullanılması tavsiye edilmektedir.
g) Firma çalışanları hiçbir şekilde kendilerinin login şifrelerini aile bireyleri dahil olmak üzere hiç kimseye veremezler
h) Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar bağlantı esnasında aynı anda başka bir ağa bağlı olmadıklarından emin olmalıdırlar.
i) Uzaktan bağlanan kişi makinasında zararlı kod, truva atı, vs. olduğundan şüpheleniyorsa bağlantıyı gerçekleştirmemelidir.
j) Uzaktan erişim yöntemi ile kuruma erişen bilgisayar ağında güvenlik tedbirleri alınmış olmalıdır.(örn, firewall, Domain altyapısı vs.)
k) Kurum ağına standart dışı erişim isteğinde bulunan organizasyon veya kişiler kurumun bilgi işlem biriminden izin almak zorundadırlar.
l) Üniversite, periyodik olarak kullanıcı kimlikleri ve hesapları kontrol etmeli gereksiz kullanıcı kimlikleri ve hesapları kaldırılmalıdır.
m) Firma, kurum ile hassas veriye erişim hakkında gizlilik anlaşması imzalamalıdır.

n) Kurum, birliğin alması gereken güvenlik tedbirlerinde herhangi bir aksaklık gördüğünde kurum ve firma arasındaki uzaktan erişim bağlantısını eksiklik düzeltilinceye kadar kesebilir.

o) Kurum güvenli erişimin sağlanabilmesi için gerekli gördüğü takdirde birliğin sadece belli zaman aralıklarında veya istek yapılan durumda uzaktan erişimine izin verebilir.

P24 YAZILIM GELİŞTİRME

1.0 Amaç

Yazılım Geliştirme üzerindeki kontroller, kurumların günlük operasyonlarını yürütmek için kullandıkları yazılımların oluşturulması esnasında kullanılan kontrol mekanizmalarıdır. Programların geliştirilmesi esnasında uygulanması gereken kontroller, yazılımların kontrollü bir şekilde geliştirilmesini sağlamayı hedeflemektedir. Bu şekilde güvenlik kriterlerinin hem yazılımın geliştirilmesi aşamasında, hem de geliştirilen yazılım uygulamaya alındıktan sonra gözetilmesi sağlanır. Bu politika yazılım geliştirme hakkındaki kriterleri ortaya koymaktadır.

2.0 Kapsam

Bu politika kurumda yazılım geliştirme alanında faaliyet gösteren kişi ve firmaları kapsamaktadır.

3.0 Politika

Yazılım geliştirme üzerindeki kontroller şu temel kriterlere uygun şekilde oluşturulmalıdır.

a) Sistem yazılımında mevcut olan kontroller, kullanılacak yeni bir yazılım veya mevcut sistem yazılımına yapılacak olan güncellemeler ile etkisiz hale getirilmemelidir.
b) Yönetim sadece uygun yazılım projelerinin başlatıldığından ve proje alt yapısının uygun olduğundan emin olmalıdır.
c) İhtiyaçlar, uygun bir şekilde tanımlanmalıdır.
d) Sistem geliştirmede, ihtiyaç analizi fizibilite çalışması, tasarım, geliştirme, test ve onaylama safhalarını içeren sağlıklı bir metodoloji kullanılmalıdır.
e) Kurum içinde geliştirilmiş yazılımlar ve seçilen paket sistemler ihtiyaçları karşılamalıdır.
f) Kurumda kişisel olarak geliştirilmiş yazılımların kullanılması kısıtlanmalıdır.
g) Hazırlanan sistemler mevcut prosedürler dahilinde, işin ve iç kontrol gerekliliklerini yerine getirdiklerinden emin olunması açısından test edilmeli ve yapılan testler ve test sonuçları belgelenerek onaylanmalıdır.
h) Yeni alınmış veya revize edilmiş bütün yazılımlar test edilmeli ve onaylanmalıdır.
i) Eski sistemlerdeki veriler tamamen, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılmalıdır.
j) Uygulama ortamına aktarılma kararı uygun bilgilere dayalı olarak ilgili yönetim tarafından verilmelidir.
k) Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.
l) Yazılımlar sınıflandırılmalı / etiketlenmeli ve envanterleri çıkarılarak bir yazılım kütüğünde muhafaza edilmelidir.

P25 PERSONEL VE EĞİTİM

1.0 Amaç

Bilişim sistemlerinden kaynaklanan sorunların büyük bir kısmı insanlar tarafından yapılan hata, ihmal ve suiistimallerden kaynaklanmaktadır. Bu nedenle kurumların, personelin hata yapma riskini düşürecek kontroller kurmaları önem kazanmaktadır. Bu, uygun personel ve eğitim politikalarının benimsenmesi sayesinde başarılabilir.

Farklı kişiler tarafından yerine getirilmesi gereken görevlerin ayrılması, işlemlerin yetkilendirilmesi, kaydedilmesi ve varlıkların korunması açısından önemlidir. Görevlerin ayrılması, bir kişinin diğer bir kişinin yaptığı faaliyetleri kontrol etme imkânı vermesi nedeniyle de hata riskini düşürür. Bu politika, personel ve eğitim hakkındaki kriterleri ortaya koymaktadır.

2.0 Kapsam

Bu politika kurum yönetimini kapsamaktadır.

3.0 Politika

Personel ve eğitim politikaları şu temel kriterlere uygun oluşturulmalıdır:

- **a)** Eğitim stratejisi ile bilişim stratejisi birbiriyle aynı doğrultuda olmalıdır. Bu sayede bilişim stratejisinin başarılı bir şekilde uygulanması sağlanır.
- **b)** Personelin sisteme tanımlanması ve yetkilerinin belirlenmesi işlemi yönetim tarafından onaylanmış bir prosedür dahilinde yapılmalıdır.
- **c)** Kurum yapısı içinde yetki ve sorumluluklar açıkça tanımlanmış olmalıdır.
- **d)** İşe alınan personel mevcut yapı ve güvenlik sistemleri hakkında bilgilendirilmelidir.
- **e)** Kurum tarafından, bilişim sistemini kuran, geliştiren ve kullanan personelin görev tanımları yapılmış olmalıdır.
- **f)** Personelin işe alınması, görev yerlerinin değiştirilmesi, görevlerine son verilmesi ve performanslarının değerlendirilmesinde güvenlik göz önünde bulundurulmalıdır.
- **g)** Kurum çalışanları işin gerektirdiği vasıflara sahip olmalı, yeterli seviyede eğitim almalı ve yeteneklerine uygun işlerde çalıştırılmalıdır.
- **h)** Bilişim alanında istihdam edilecek daimi personel ile sözleşmeli veya danışman olarak çalıştırılacak personelin seçiminde, bu kişilerin işin gerektirdiği öğrenim ve eğitimi almış yetenekli ve dürüst kişiler olmalarına azami dikkat gösterilmelidir.
- **i)** Bilişim yöneticileri, personelin bugün ve yakın gelecekte ihtiyaç duyulan yeteneklere sahip olup olmadıklarını bilmeli ve onlara bu ihtiyaçları karşılayacak eğitimi verdirmelidir. Bilişim eğitimi pahalı bir eğitim olduğu için eğitim planları ve bütçeleri kontrol edilmelidir.
- **j)** Bilişim personelinin kurumun mevcut ve uzun vadeli politikaları ile paralellik gösteren bir şekilde sertifika programlarına katılımı ve sertifikasyonlarını tamamlaması gerekmektedir.
- **k)** Görevlerin ayrılması bir kişinin diğer bir kişinin yaptığı faaliyetleri kontrol etme imkanı verecek şekilde olmalıdır.
- **l)** Çalışanlar görev ve sorumluluklarının neler olduğunu bilmelidir.
- **m)** Yönetim, kullanılan kontrollerin ne derecede etkin olduğunu değerlendirmelidir.

n) Personelin faaliyetleri, resmi çalışma prosedürleri, denetim ve gözden geçirme yollarıyla kontrol altında tutulmalıdır.

o) Bütün çalışanlar aktif gözetim ve yönlendirmeye tabi tutularak desteklenmelidir.

P26 BELGELENDİRME

1.0 Amaç

Kurumun belgeleme politikalarının yetersiz olması , personelin hatalı veya yetkisiz işlem yapma riskini yükseltebilir. Ayrıca sistemde bir hata meydana geldiği zaman, eğer işlemler yeterli bir şekilde belgelenmemişse, hatanın sebebinin tespiti de güçleşebilir.

2.0 Kapsam

Bu politika kurum yönetimini kapsamaktadır.

3.0 Politika

Belgeleme politikaları şu temel kriterlere uygun oluşturulmalıdır :

a) Bilişim sisteminin yapısı ile bütün iş ve işlemler açıkça belgelenmeli ve bu belgeleme inceleme amacıyla kolaylıkla ulaşılabilir durumda olmalıdır.
b) İş akışları uygun şekilde belgelenmelidir.
c) Belgeleme, tarih belirtilerek yapılmalı ve yedek kopyaları güvenli bir yerde muhafaza edilmelidir.
d) Girdi türleri ve girdi form örnekleri belgelenmelidir.
e) Ana dosyalar ile diğer dosyaların içerik ve şekilleri belgelenmelidir.
f) Çıktı form örnekleri ve çıktılarım kimlere dağıtılacağı belgelenmelidir.
g) Programların nasıl test edildiği ve test sonuçları belgelenmelidir.
h) Bütün program değişikliklerinin detayları belgelenmelidir.

P27 KABUL EDİLEBİLİR KULLANIM POLİTİKASI

1.0 Amaç :

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

2.0 Kapsam

Bu politika; TELE KURYE personeli ile üniversite için çalışan yüklenici firmalar için olup tüm CBÜ bilişim etkileşimli kritik bilgi varlıklarını kapsar.

3.0 Politika Metni

3.1 Güvenlikten, CBÜ personeli, CBÜ iş yerlerinde CBÜ'nün iş yapan Yüklenici Firmalar her gün sorumludur. İlgili tüm personel, kendi alanlarına ait Güvenlik Politikalarına uymak zorundadır.

3.2 Güvenlik Politika ve ekleri yöneticiler ve BGYS Yöneticisi tarafından CBÜ çalışanlarına, yeni işe başlayanlara ve yüklenici firmalara duyurulacaktır. İlgili Güvenlik Politikalarına uyulacağı personel iş sözleşmesinde yer almalı ve personele imzalatılmalıdır.

3.3 CBÜ ortamında tutulan ve iletilen tüm bilgiler; birliğin malıdır ve CBÜ bu bilgileri izleme ve denetleme hakkına sahiptir.

3.4 CBÜ'nün Gizli olarak belirlediği tüm bilgilerin gizliliğine sıkı bir şekilde uyulacaktır. Birliğin iş gereksinimi dışında bu bilgilerin kopya edilmesi ve iletilmesi yasaktır.

3.5 CBÜ 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.

3.6 Hiçbir personel, bilgisayarlarından anti virüs koruma yazılımını devre dışı bırakamaz.

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

3.8 Hiç bir personel izin almadan kendi PC' sinden veya başka bir kaynak kullanarak, CBÜ'nün Bilişim Ağını tarayamaz, izleyemez veya dinleyemez.

3.9 CBÜ onaylı resmi penetrasyon testleri haricinde, CBÜ bilgisayar sunucuları için içeriden veya dışarıdan port taraması yapılması yasaktır.

3.10 Hiç bir personel, üniversite içinde kendilerine tahsis edilen bilgisayar yetkilerinin dışına çıkamaz ve bu konuda yetki aşma işlemine girişemez.

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

D. Yaptırım

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda, BGYS Ekibi ve ilgili yöneticinin onaylarıyla Bilgi Güvenlik Politika Yaptırımları Dokümanında belirtilen kanunlar ve ilgili maddeleri esas alınarak işlem yapılır.

P28 ORTAMIN ELDEN ÇIKARILMASI POLİTİKASI

1. AMAÇ VE SORUMLULUK

Bilgilerin yedeklendiği, taşındığı, dolaşıma sunulduğu ortamların, ortamlarda taşınan verilerin uygunsuz kişilerin kullanımına geçmemesi, üçüncü şahıslara yönelik hukuki süreçleri başlatmaması, hassas bilgi içeren bilginin izinsiz kişilerin sızmasını minimuma indirmek için elden çıkarılmasının kurallarını ortaya koymak.

Politika uygulanmasından teknik yönetim sorumludur.

2. KAPSAM

Basılı, yazılı her tür ortamın amaç maddesindeki çekinceler çerçevesinde elden çıkarılması, değiştirilmesi veya dönüştürülmesidir.

KÂĞIT ORTAM

a) Kayıtların Kontrolü Prosedürüne göre Kalite Yöneticisi saklama süresi dolan kayıtları İmha Tutanağı imzalayarak imha eder.

ELEKTRONİK ORTAM

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

b) Kayıtların Kontrolü Prosedürü ve Saklama Süreleri Formu'na göre saklanırlar.

	Tekrar Yazılabilir Ortam	Tekrar Yazılamaz Ortam
Risk derecesi yüksek kayıtlar	Silmek ve sonra imha etmek.	Doğrudan imha etmek
Riski olmayan kayıtlar	Silinerek, formatlanarak tekrar kullanıma alınabilir.	Basit elden çıkarma teknikleri ile.

Dokümanlar

FR.14.03 İmha Tutanağı

P29 TEÇHİZATIN ELDEN ÇIKARILMASI POLİTİKASI

1. Amaç:

Sisteme bağlı ya da bağlı olmayan sunucu ve ağ cihazlarının elden çıkarılmasının nasıl yapılacağını açıklar.

2. Kapsam:

Sistemden çıkartılacak sunucu ve ağ cihazlarını kapsar.

3. Uygulama

a) Sunucular için

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

Bu ortamlar kesinlikle elden çıkartılmaz ve sadece "P28 ORTAMIN ELDEN ÇIKARILMASI Politikasına göre imha edilebilir.

b) Ağ Cihazları için

Elden çıkartılacak olan ağ cihazlarında öncelikle üzerinde bulunan modüllerin ve 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.

P30 TEMİZ MASA TEMİZ EKRAN POLİTİKASI

1- Amaç:

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

2- Kapsam:

Çalışma masaları, ekranlar, basılı dokümanlar, belgeler, kayıtlar.

3- Sorumlular:

Tüm çalışanların bu politikaya uygun hareket etmesinden tüm üst yönetim sorumludur.

4- Uygulama:

a) Çalışma sonunda kâğıt ortamında ya da elektronik cihazlar üzerinde tutulan "gizli ya da çok gizli" bilgiler güvenlikli ortamlarda (çelik kasa, kilitli güvenli ortamlar vb) saklanacaktır.

Sorumlu: Tüm personel

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

Sorumlu: Üst yönetim, Tüm personel
Doküman: P28 Ortamın Elden Çıkarılması Politikası

c) Her türlü haberleşmede kullanılan cihazlar (telefon, faks, fotokopi makineleri) yetkisiz erişimlere bırakılmayacaktır. Cihazlar üzerinde belge, doküman bırakılmayacaktır.

Sorumlu: Üst yönetim, Tüm personel

d) Her türlü ekrandan ulaşılabilen bilgiler, şifreler, anahtarlar ve kodlar, bilginin sunulduğu sistemler, ana makineler (sunucu), PC'ler vb. cihazlar şifresiz kullanılmayacaktır.

Sorumlu: Üst yönetim, Tüm personel

e) Ekranlarda çalışılmaması durumunda devreye girecek ekran koruması (parola) tüm PC'lerde, notebooklar da etkinleştirilecektir.

Sorumlu: Üst yönetim, Tüm personel

P31 KRİPTOGRAFİK KONTROLLER POLİTİKASI

AMAÇ;
Bilginin gizliliği, aslına uygunluğu ya da bütünlüğünün korunmasıdır.

UYGULAMA;
Gizlilik: Bilgi, istenmeyen kişiler tarafından anlaşılmamalı.
Bütünlük: Bir iletinin alıcısı bu iletinin iletim sırasında değişikliğe uğrayıp uğramadığını öğrenmek isteyebilir; davetsiz bir misafir doğru iletinin yerine yanlış bir ileti koyma şansına erişmemelidir. Saklanan veya iletilmek istenen bilgi farkına varılmadan değiştirilememeli.
Reddedilemezlik: Bilgiyi oluşturan ya da gönderen, daha sonra bilgiyi kendisinin oluşturduğunu veya gönderdiğini inkar edememeli. Bir gönderici daha sonrasında bir ileti göndermiş olduğunu yanlışlıkla reddetmemelidir.
Kimlik Belirleme: Gönderen ve alıcı, birbirlerinin kimliklerini doğrulayabilirler. Davetsiz bir misafir başkasının kimliğine bürünme şansına erişmemelidir.
Kriptografik Yöntemlere Güven: Kriptografik yöntemler, bilgi ve iletişim sistemlerinin kullanılması için güven oluşturmalıdır.
Özgür Seçim: Kullanılacak kriptografik ürünler, yasalar çerçevesinde özgürce seçilebilmelidir.
Gereksinime Bağlı Gelişme: Kriptografik yöntemler, birey, kurum ve hükümetlerin gereksinim, istem ve sorumluluklarına bağlı olarak gelişmelidirler.
Standartlar: Açık anahtar altyapısı ve şifreleme standartları ulusal ve uluslararası düzeylerde geliştirilmeli ve yaygınlaştırılmalıdır.

Bireysel Gizlilik Hakkı: Ulusal politikalar, bireysel iletişimin gizliliğine ve kişisel bilgilerin korunması gereğine saygı göstermelidir.
Yasal Erişim: Ulusal politikalar, bu kılavuzdaki diğer ilkelerle çelişmemek koşuluyla, şifreli mesajlara ve kişilerin gizli anahtarlarına yasal erişimi öngörebilir.
Yasal Sorumluluk: Kriptografi hizmeti veren ve açık/ gizli anahtarları dağıtma yetkisi taşıyan kuruluşların yasal sorumlulukları açıkça belirlenmelidir.
Uluslar arası Eşgüdüm: Ulusal ve uluslararası politikalar, birbirleriyle eşgüdüm içinde oluşturulmalıdır.

Şifreleme/deşifreleme (encryption-decryption) bir bilgisayar ağında veya kişisel bilgisayarlarda haberleşme ya da dosya güvenliğini sağlamak için kullanılır. Bu nedenle günümüzde bilgisayarlarda ya da bilgisayar ağlarında şifrelemenin önemi gün geçtikçe artmaktadır.

Bu çalışma da genel olarak şifreleme teknikleri hakkında bilgi verildikten sonra RSA şifreleme algoritmasına uygun olarak şifreleme ve deşifreleme işlemi yapan bir simulasyon tasarlanmıştır. Simulasyonu gerçekleştirmek için programlama dili olarak java seçilmiştir. Algoritma gereği kullanılan sayıların boyutları çok büyük olması nedeniyle java programlama dili kullanılmıştır.İnternette yollanan veri paketleri birçok halka açık networklerden geçer, bu da bu paketlere ulaşmayı mümkün kılar. Son derece gizli bilgiler internette nakil olurken, bu durum önemli bir kaygı halini alır. Bu tür bilgileri korumak mümkün olmadıkça, internet iş yapmak veya gizli, şahsi yazışmalarda bulunmak asla güvenli bir yer olmayacaktır. Bilgi güvenliği başkası tarafından dinlenme, bilginin değiştirilmesi, kimlik taklidi gibi tehditlerin ortadan kaldırılması ile sağlanır ve bu amaçla kullanılan temel araç kriptografidir. Kriptografi bilgi güvenliğini inceleyen ve anlaşılabileni anlaşılamaz yapan bir bilim dalıdır. Güvenilirlik, veri bütünlüğü, kimlik doğrulama gibi bilgi güvenliği konularıyla ilgilenen matematiksel yöntemler üzerine yapılan çalışmalar kriptografinin önemli konularıdır.

Şifrelemenin Temel Elemanları;

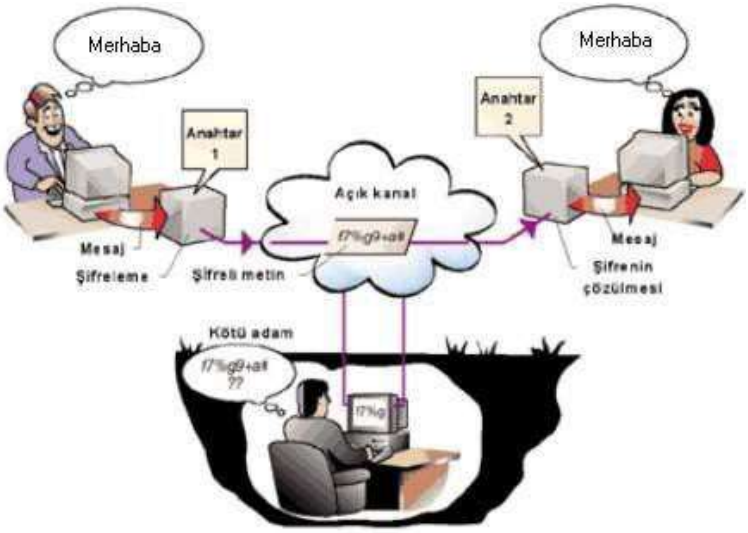
Bir göndericinin bir alıcıya açık ağlar üzerinden bir ileti göndermek istediği zaman, açık ağlardan gönderilen iletiler üçüncü şahıslar tarafından dinlenme ve değiştirilme tehdidi altındadırlar.

Burada söz konusu ileti düz metindir. Bazı kullanımlarda plaintext adı da verilir. Bir iletinin içeriğini saklamak üzere yapılan gizleme işlemi de şifrelemedir (encryption). Bu işlem düz metini şifreli metine dönüştürür. Bilginin içeriğinin başkalarının anlamayacağı hale gelir. Bu bilgi bir yere iletilmek amacıyla şifrelenen bir mesaj veya saklanmak amacıyla şifrelenen bir bilgi olabilir. Şifrelenmiş bir ileti şifreli metindir (ciphertext). Şifreli metini düzmetine geri çevirme işlemi şifre çözümüdür (decrypt). Bu işlemler Şekil1'de gösterilmektedir.

Şekil 1 Şifreleme ve şifreyi çözme işlemleri

İleti güvenliğini sağlama bilimi kriptografidir. Matematiğin hem şifre bilimi hem de şifre analizini kapsayan dalı kriptolojidir ve şifrebilimciler tarafından icra edilir.
Eğer bir algoritmanın güvenliği bu algoritmanın çalışma biçimini gizlemeye dayalıysa, bu bir

sınırlandırılmış algoritmadır. Sınırlandırılmış algoritmalar günümüzün şartlarına pek uymamaktadır; bir gruba ait kullanıcılar bunları kullanamamaktadır, çünkü gruptan bir kullanıcının her çıkışında geri kalan
herkesin başka bir algoritmaya geçmesi gerekmektedir. İçlerinden birisi yanlışlıkla gizleneni açığa vurduğunda, diğer herkesin algoritmalarını değiştirmeleri gerekmektedir. Daha da kötüsü, sınırlandırılmış algoritmalar kalite kontrolüne ve standartizasyona olanak tanımamaktadır. Her bir grup kullanıcının kendisine ait bir algoritması olmalıdır. Bu tür bir grup hazır şifre çözüm anahtarının yazılım veya donanım ürünlerini kullanamaz; davetsiz bir misafir aynı ürünü alıp algoritmayı öğrenebilir. Kendi algoritmalarını ve gerçekleştirimlerini kendileri yazmaları gerekir. Günümüz kriptografisi bu sorunu bir anahtar ile çözmektedir. Bu anahtar çok çeşitli değerler alabilen herhangi bir anahtar olabilir. Günümüzde kullanılmakta olan modern ve güçlü şifreleme algoritmalaları artık gizli değildir. Bu algoritmalar güvenliklerini kullandıkları farklı uzunluk ve yapılardaki anahtarlarla sağlarlar. Bütün modern algoritmalar şifrelemeyi ve şifre çözmeyi kontrol için anahtarları kullanır. Bir anahtar ile şifrelenmiş bilgi, kullanılan algoritmaya bağlı olarak, ilgili anahtar ile çözülebilir. Genel olarak anahtarın kullanımı şu şekildedir (şekil 2):



Şekil 2. Bir mesajın dinlenmesini önlemek için anahtar ile şifreleme.

Kullanıcı bir mesajı (m) göndermeden önce bir anahtar (k1) kullanarak şifreler. Şifreli metin (c) yasadışı dinleyicilere açık olan bir kanaldan gönderilir. Mesajı okumak için alıcı bir anahtar (k2) kullanarak şifreyi çözer ve m mesajını elde eder. Aktif düşmanlar araya girip iletişimi dinleyebilir. Eğer k1 ve k2 eşitse, sistem simetriktir. Aksi takdirde bu sistem asimetrik olarak nitelenir. Güvenliğin garantilenmesi için k2 her zaman gizli olmalıdır, ancak k1'i kullanarak k2'yi elde etmek mümkün olmadığı sürece k1 açıklanabilir. Bu durumda sisteme açık anahtarlı sistem (public key system) adı verilir.

Açık anahtarlı sistemler pek çok ilginç olanaklar sunar; örneğin herkes online bir mağazaya mağazanın açık k1 anahtarını kullanarak şifrelenmiş bir kredi kartı numarası gönderebilir. k2 anahtarını sadece mağaza bildiği için, kartın numarasını sadece mağaza öğrenebilir. Eğer simetrik sistem kullanılsaydı, mağaza potansiyel müşterilerinin her biriyle önceden ve gizlice ayrı ayrı anahtarlar belirlemek zorunda kalırdı. Açık anahtarlı sistemlerin güvenliği her zaman belirli matematiksel problemleri çözmenin zorluğuna dayanır, simetrik sistemler daha çok tek kullanımlık, geçici yapıdadırlar. Açık anahtarlı sistemlerin en büyük dezavantajı matematiksel yapıları nedeniyle simetrik sistemlerden daha yavaş olmalarıdır; özellikle açık anahtarlı sistemlerdeki anahtarların boyutları simetrik sistemlerin anahtarlarının boyutlarından çok daha büyüktür. Kısaca, kullanılacak şifreleme yöntemi gerçekleştirilecek uygulamaya bağlı olarak seçilir. (Şekil 3)

Şekil 1.3. Tek anahtar ile şifreleme ve şifre çözme

Şekil 1.4. İki farklı anahtar ile şifreleme ve şifre çözme

Algoritmalardaki bütün güvenlik anahtara (veya anahtarlara) dayalıdır, hiçbiri algoritmanın ayrıntılarında yer almaz. Bu, algoritmanın yayınlanabildiği ve incelenebildiği anlamına gelir. Bu algoritmayı kullanan ürünler seri üretilebilir. Bir davetsiz misafirin sizin algoritmanızı bilmesi önemli değildir; sizin özel anahtarınızı bilmedikçe, o şahıs iletilerinizi okuyamaz.

Şifreleme algoritmaları anahtar kullanma yöntemlerine göre genel olarak iki kategoriye ayrılmaktadır. Bu yöntemler:

Açık-Anahtar (Asimetrik) Şifreleme Yöntemleri;

Bu şifreleme yöntemi iki ayrı anahtar kullanan yöntemdir. İki anahtar kullanımının; güvenirlik, anahtar dağıtımı ve onaylama alanlarında önemli sonuçları vardır. Bu kriptografi yapısında, açık ve gizli anahtar olarak adlandırılmış olan bir anahtar çifti kullanılmaktadır. Asimetrik algoritmalar da denilen açık anahtarlı algoritmalarda şifreleme için kullanılan anahtar ile şifre çözme için

kullanılan anahtar birbirinden farklıdır. Anahtar çiftlerini üreten algoritmaların matematiksel özelliklerinden dolayı açık-gizli anahtar çiftleri her kişi için farklıdır, diğer bir deyişle her kullanıcının açık-gizli anahtar çifti yalnızca o kullanıcıya özeldir. Ayrıca şifre çözüm anahtarı (en azından makul bir zaman dilimi içerisinde) şifre anahtarından hesaplanamaz. Bu algoritmalara açık anahtarlı algoritmalar denmesinin sebebi şifre anahtarı halka (kamuya/genel kullanıma) açılabilir: Bir yabancı bir iletiyi şifrelemek için şifreleme anahtarını kullanabilir, ancak sadece ilgili şifre çözüm anahtarına sahip bir kişi iletinin şifresini çözebilir. Bu sistemde, şifre anahtarına genellikle açık anahtar denir, şifre çözüm anahtarı da genellikle gizli anahtar olarak adlandırılır. Gizli anahtar kimi zaman özel anahtar olarak da adlandırılır, ancak simetrik algoritmalarla karışmaması için bu terim genelde kullanılmaz.

Bir kullanıcının açık anahtarıyla kilitlenen bir mesajı yalnız ve ancak ona ait gizli anahtar çözebilir. Aynı şekilde, herhangi bir kullanıcının gizli anahtarıyla attığı sayısal imzanın doğrulanabilmesi, yalnızca onun açık anahtarını kullanarak mümkün olabilir. Açık anahtar kamuya açıktır, elektronik kimlik belgelerinin içinde diğer kişisel bilgilerle birlikte tutulur ve herkes birbirinin açık anahtarını e-kimliklerine ulaşmak süretiyle istediği zaman elde edebilir.

Sayısal Şifreleme: Şifreleme açık ağlardan gönderilen bilginin başkaları tarafından görülmesinin (dinlenmesinin) istenmedigi zaman yapılır. Bunun için çift anahtarlı bir kriptografik algoritma kullanılabilir. Buna göre, mesajı gönderen taraf, gönderilen bilginin sayısal içeriğini, mesajı alacak tarafın açık anahtarını, sayısal şifrelemede kullanır. Mesajı alan taraf da, şifreli mesajı çözmek için şifreli mesajın sayısal içeriği, kendisinin gizli anahtarına gereksinim duyar.

Burada dikkat edilecek olursa, şifreli mesajın üçüncü taraflar tarafından dinlenebilmesi ancak "gizli anahtara" sahip olmaları ya da şifreli mesajı matematiksel yollarla deşifre etmeye çalışmaları ile mümkün olabilir. "Güvenlik açısından iyi bir şifreleme" algoritması, gizli anahtar olmadan şifreli mesajı deşifre etmeye imkân tanımıyan bir algoritmadır.

Sayısal İmza: Sayısal imza elektronik mesaja eklenmiş bilgidir. Çift anahtarlı bir kriptografik algoritmayla hazırlanan sayısal imza, hem gönderilen bilginin sayısal içeriğinin değiştirilmediğinin hem de gönderen tarafın kimliğinin ispatlanması için kullanılır ve gönderilecek mesajdan üretilen "mesaj özetinin" sayısal içeriği, gönderen tarafın kendi gizli anahtarına bağlı olarak oluşturulur. Sayısal imzanın doğruluğunu kanıtlamak için mesaji alan taraf, kendisine gelen mesajin ve sayısal imzanın sayısal içeriği, gönderen tarafın açık anahtarını kullanır.

Açık-anahtar şifreleme için pek çok algoritma bulunmaktadır. En yaygın olan iki tanesi RSA (Ron Rivest, Adi Shamir, Leonard Adleman) algoritması ve DSA (Digital Signature Algorithm - Dijital İmza Algortiması) dır. RSA pek çok uygulamada kullanılan bir algoritmadır. Mesajları şifrelemek için kullanılabileceği gibi dijital imzalarda da kullanılabilir. DSA sadece dijital imza kullanımı içindir. Mesajları şifrelemek için kullanılmaz.

P32 ZİYARETÇİ KABUL POLİTİKASI

1- AMAÇ

Bu politikanın amacı CBÜ dışarıdan gelen misafirlerin kabulü, kuruluş içinde dolaşmaları ve kuruluştan uğurlanmaları ile ilgili kuralları belirlemektir.

2- SORUMLULAR:

Bu politikanın uygulanmasından CBÜ de ki tüm yönetici ve çalışanlar sorumludur.

UYGULAMA:

a) Dışarıdan ziyaret amaçlı gelen kişiler kuruluş girişinde ön büro sekreteri tarafından karşılanır ve ziyaret edeceği idarecinin onayı ile kuruluşa kabulü yapılır.

b) İdari kadro haricindeki çalışanlar kuruluşa ziyaretçi kabul edemezler.

c) Gelen ziyaretçi ziyarete geldiği kişi tarafından sekreterlikte karşılanır.

d) Ziyaretçiler sadece toplantı odalarında ve personel odalarında ağırlanır.

e) Dışarıdan ziyaret amaçlı gelen kişiler üretim alanı, yönetim ofisleri, arşiv odası, sistem odası gibi yerlere alınmamalıdır.

f) Kargo elemanları, yemek siparişi için gelen kişilerin kuruluşa girişi yasaktır.

g) Ziyarete gelen kişiler ile ilgili bilgiler ön büro sekreteri tarafından ziyaretçi takip sistemi ile kayıt edilir.

h) Gelen ziyaretçi kuruluş dışına çıkarken ziyaret ettiği idareci kendisine kapıya kadar eşlik etmelidir.

i) Ziyaretçilerin kuruluş içinde yanlarında refakat eden bir kişi olmadan dolaşmalarına izin verilemez.

j) CBÜ misafirlerini en güzel şekilde ağırlar.

3- YAPTIRIM

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

P33 TAŞINABİLİR MOBİL CİHAZ POLİTİKASI

1- AMAÇ
Bu politikanın amacı CBÜ'e ait bilgi içeren taşınabilir cihazların kullanımı ile ilgili kuralları belirlemektir.

2- SORUMLULAR:
Bu politikanın uygulanmasından CBÜ'nün tüm yönetici ve çalışanları sorumludur.

3- UYGULAMA:
a) Kuruluşa ait bilgi içeren taşınabilir cihazlar ilgili kişiye zimmetlenerek teslim edilir.

b) Her çalışan kendisine zimmetlenen cihazın güvenliğinden ve amacına uygun kullanımından sorumludur.

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

d) Kuruluşa bilgisayar, taşınabilir bellek ve PDA cihazlara dışarıdan herhangi bir yazılım, siyasi propaganda, ırkçılık, şiddet, pornografi veya erotizm içeren resim, film veya müzik kopyalanamaz ve cihaz içerisinde bulundurulamaz.

e) Kuruluş telefon hatları ve bilgisayarlar üzerinden üçüncü taraf kişilerle borç alacak ilişkisi, tehdit, küfür, kuruluş itibarını zedeleyecek şeyler ve yasa dışı olan iletişim kurulamaz.

f) Bilgisayarlar ve PDA cihazlar üzerindeki anti virüs programları hiçbir nedenle devre dışı bırakılamaz.

g) Taşınabilir bilgisayarlar üzerinde yapılan çalışmalar ve oluşturulan dosyalar mutlaka ağ üzerinde ilgili adrese kaydedilmelidir.

h) Mobil cihazınızda ne tür bilgiler sakladığınızın farkında olun, hassas ve gizli bilgileri mümkün olduğunca mobil cihazınızda bulundurmayınız.

i) Verilerinizin yedeklerini alın ve güncel bir kopyasını farklı bir yerde saklayınız.

j) Kaybolması ve çalınması kolay olduğundan mobil cihazlar başıboş bırakılmamalıdır.

4- YAPTIRIM
Bu politikaya uygun olarak çalışmayan tüm personel hakkında **Disiplin Prosedürü** hükümleri uygulanır.

P34 SİBER SALDIRI POLİTİKASI

1- AMAÇ

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

2- SORUMLULAR:

Bu politikanın uygulanmasından Bilgi İşlem Daire Başkanlığı sorumludur.

3- UYGULAMA:

a) Tüm bilgisayarlar, CBÜ yönetimi tarafından onaylanmış en son anti virüs yazılımları ile koruma altına alınacaktır.

b) Bilinmeyen ve şüpheli bir kaynaktan gelen e-posta mesaj ve ekleri açılmayacaktır.

c) Bilgisayarlarda kullanılan tüm taşınabilir medya ortamları (disket sürücü, Flash ROM, CD-ROM vs.) kullanılmadan önce virüs taramasına tabi tutulacaktır.

d) Tüm e-posta ve ekleri anti virüs taramasından işlem öncesi geçirilecektir.

e) Anti virüs yazılımının tüm güncel imzaları merkezi olarak anti virüs firmasının onaylı ve sunucusundan otomatik olarak yüklenecek ve ilgili sunuculara dağıtımı yapılacaktır.

f) Internet üzerinden kaynağı belli olmayan web sitesinden yazılım yüklemesi yapılmayacaktır.

g) CBÜ BGYS Yöneticisi tarafından siber saldırılarla mücadele için kullanılması yasaklanan ve üniversite içinde duyurulan yazılım ve bileşenleri hiçbir personel tarafından kullanılmayacaktır.

h) CBÜ kuruluş ağına bağlanması gerekli olan üniversite dışı istemci ve taşınabilir bilgisayarları ağa VPN ile bağlanmaktadırlar.

i) CBÜ personeli, e-posta veya başka yollarla kendilerine gelen ve kendilerinden istenen parola, kullanıcı kimlik veya gizli bilgileri iletmeyecek ve böyle durumlar olursa bunu Bilgi İşlem Daire Başkanlığına hemen bildirecektir.

j) CBÜ personeli, kendi bilgisayarlarından üniversite tarafından kurulmuş olan anti virüs ve/ya SPAM koruma yazılımlarını devre dışı bırakamaz veya kaldıramaz.

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

l) CBÜ ağı ve önemli sunucu bileşenleri için Ağ ve Sunucu Saldırı Tespit sistemleri devreye alınacaktır.

4- YAPTIRIM

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

P35 BİLGİ VE YAZILIM ALIŞVERİŞİ POLİTİKASI

1- AMAÇ

Bu politikanın amacı CBÜ ve diğer organizasyonlar arasında gerçekleşebilecek herhangi bir bilgi kaybı, değişikliği veya yanlış kullanımı önlenmektir.

2- SORUMLULAR:

Bu politikanın uygulanmasından Bilgi İşlem Daire Başkanlığı sorumludur.

3- UYGULAMA:

a) Organizasyon, elektronik transferlere yönelik muhasebe kayıtlarının tutulmakta olduğundan emin olmalıdır. Böylece kuruluşun kayıtları güncel olacaktır.

b) Üçüncü taraflar için geliştirilmiş olan yazılımların, sadece bilgisayar kodu halinde dağıtılması gerekir.

c) Organizasyonun yazılımlarını veya verilerini kullanmakta olan üçüncü taraflar, gerekli koruma ölçütlerini içeren bir yazılı sözleşme imzalamalıdır. Böylece üçüncü tarafların söz konusu bilgiyi izinsiz kullanması, değiştirmesi veya çoğaltması engellenmiş olacaktır.

d) Elektronik ortamda sözleşmenin yapıldığı üçüncü taraflarla, kağıt üzerinde de anlaşma yapılmalıdır. Yazılı sözleşmeler en güvenli sözleşme biçimidir.

e) Bilgi ve veri alışverişinden önce dış tarafların kimliklerinin tespit edilmesi gerekir.

f) Üçüncü tarafa açılan tüm gizli bilgilerin kesinlikle şifrelenmesi gerekir.

g) Gizli bilgilerin ülke dışına çıkartılması veya toplu taşıma ile transfer edilebilmesi için yetki gerekir.

h) Bilginin uluslararası seyahati sırasında sadece yetkili çalışanların gizlilik içeren bilgiye erişimi vardır.

i) Üçüncü taraflara yollanan bilgisayar ortamı yeni olmalı veya herhangi bir bilgi içermemelidir.

j) Güncellenmelerin veya yeni ürünlerin yollanması için müşteri otorizasyonu (onayı) gerekir.

k) Elektronik alışveriş yapmak üzere kuruluşlar arası bir ağ kurulmadan önce bir ticari ortaklık sözleşmesi imzalanmalıdır.

l) Yetkisi olmayan çalışanlar tarafından gönderilen e–mailler, organizasyonu bağlamaz.

m) İş iletişiminin sağlanması için sadece organizasyon tarafından yetkilendirilen çalışanların e–mail adresleri kullanılmalıdır.

n) Organizasyon, yeni ürünler ile ilgilenmeyen müşterilerinin bir listesini tutmalıdır. Buradaki amaç organizasyonun müşterileri ile iyi ilişkiler kurmasının sağlanmasıdır.

o) Müşteriden gelen ödeme hakkındaki bilgiler müşterilere tam olarak yollanmamalıdır. Bilgi yollanırken hesap numarası vb. bilgilerin belirli bir kısmını yollamak daha doğru olacaktır.

p) Organizasyon, web sitesinin korunmasını ve elektronik ticaret standartlarına uyum göstermesini sağlayacaktır.

q) Organizasyonun müşterileri, organizasyonun mailleşme listesinden isimlerini çıkartabilmek için ne yapmaları gerektiğini bilmelidir.

r) Organizasyon, müşterilerini mail listesine eklemeden önce onlardan izin almalıdır.

s) Organizasyon, müşterilerine, yapılan hesaplardaki doğruluğu gösterebilmek için yeterli bilgiyi vermelidir.

t) müşterilerin hesaplarında herhangi bir değişiklik olması durumunda meüşterilerden onay talebi istenmelidir.

u) Alışveriş sırasında kaydedilen bilgiler, transfer sırasında şifrelenmelidir. Böylece gizlilik içeren bilgiler, veri transferi sırasında istenmeyen taraflara geçmeyecektir.

v) E – mail ile gönderilen her türlü hassas bilgi şifrelenmelidir.

w) Gizli bilgiler sadece uygun data server'larda kayıt altına alınmalıdır.

x)Yazılım yükleme veya yazılım güncellemelerini yapma ve sistem bakımını gerçekleştirme yetkisi sadece Bilgi İşlem Daire Başkanlığınındır.

y) Kritik bir dosyada çeşitli değişikliklerin yapılması durumunda, dosyanın en az iki yedeği alınmalıdır.

z) Organizasyon bir e – mail'in içeriğinde herhangi bir değişiklik yapılmasını yasaklamalıdır.

aa) Organizasyonda bilgi sistemleri aracılığı ile gönderilen mesajlar, saldırgan veya ayrımcılık içeren bildiriler içermemelidir. Organizasyonun bilgi sistemi sadece iş gereklilikleri için kullanılmalıdır.

bb) Tüm junk mailler, uygun faaliyetleri yürütecek olan e – mail yöneticisine gönderilmelidir.

cc) Bir e-mail'e gizlilik içermekte olduğuna dair bir not eklendiğinde, bu mesajı sadece e – mailin gönderildiği kişinin maili aldığından emin olunmalıdır.

dd) E – mail'lerde taranmış imzalar bulunmamalıdır.

ee) Organizasyonun çalışanları çeşitli tartışma gruplarına katılmamalıdır.

ff) E – mail yoluyla gönderilen bilgiler, bu bilginin kimden gelmekte olduğunu içermelidir.

gg) E – mail yoluyla gönderilen bilgiler, spesifik bir geri dönüş adresi içermelidir.

hh) Faks yoluyla gönderilen gizlilik içeren herhangi bir bilginin şifrelenmiş ve bir kapak sayfası ile kapatılmış olması gerekir. Bunlara ek olarak, alıcıların kendilerine bir faks gönderilmiş olduğu hakkında bilgilendirilmiş olması gerekir.

ii) Gizlilik içeren bilgiler, handsfree telefonlarda görüşülmemelidir.

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

kk) Bilgi sistemleri gizli bilgilerin akışını engelleyebilmek için Bilgi İşler Daire Başkanlığı tarafından korunması gerekir.

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

mm) Gizlilik içeren bilgiler telefon aracılığı ile paylaşılmamalıdır.

nn) Çalışanlar gizlilik içeren bilgileri telesekreterlere veya sesli mesajlaşma sistemlerine kayıt etmemelidir.

oo) Faturalama bilgilerini transfer edebilmek için umumi telefonların kullanılması durumunda, çalışanlar telefon kartlarını veya kredi kartlarını mümkün olduğu kadar telefonun numaralarından veya ahizesinden uzak tutmalıdır.

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

qq) İşle ilgili tüm aramalar kuruluş telefonları kullanımı ile yapılmalıdır.

rr) Gizlilik içeren bilgilerin umumi yerlerde konuşulmaması gerekir.

ss) Organizasyona ait kredi kartı numaraları varsa, bu numaralar sadece kuruluş telefonu kullanıldığında, telefon aracılığı ile iletilebilir.

tt) Posta aracılığı ile gönderilen gizli bilgiler iki zarf içinde yollanmalıdır. Dış zarfta, içerideki bilginin hassaslığı ile ilgili hiç bir bilgi yazmamalı, ancak iç zarfta bilginin gizli olduğu belirtilmelidir.

uu) Kağıt üzerindeki gizli bilgilerin gönderilmesi durumunda, bilgilerin taahhütlü yollanması gerekir.

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

ww) Bilgi sistemleri sadece iş için kullanılmalıdır.

xx) Gizli bilgilerin cep telefonlarında veya telsizler aracılığı ile paylaşılması kesinlikle yasaktır.

yy) Kablosuz bağlantı ile gönderilen bilgilerin yollanmadan önce şifrelenmesi gerekir.

zz) Üçüncü taraflar, kuruluşta bir toplantıya katılmak durumunda olduklarında, bu kişilerin gizli bilgiler barındıran bölgelerde dolaşması engellenmelidir.

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

bbb) Kuruluşun intranetine yerleştirilen her bilgi veya uygulama daha önceden yetkili kişiler tarafından onaylanmalı ve kuruluşun malı olarak kalmaya devam etmelidir. Bu bilgiler kuruluşun bilgileri olarak saklı tutulacaktır.

ccc) Kuruluş içindeki donanım malzemelerin yerini değiştirmek için ilgili kişilerden Bilgi İşlem Daire Başkanlığından izin alınmalıdır.

4-YAPTIRIM

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

P36 ÜÇÜNCÜ TARAF GÜVENLİK POLİTİKASI

1- AMAÇ

Bu politikanın amacı CBÜ'nün bilgi varlıklarının ve bilgi işleme tesislerine üçüncü taraflar tarafından ulaşılması durumunda güvenliğinin sağlamaktır.

2- SORUMLULAR:

Bu politikanın uygulanmasından Bilgi İşlem Daire Başkanlığı sorumludur.

3- UYGULAMA:

a) Kurum dışından gelen bakım ve tamir çalışanları, diğer tedarikçilerde de olduğu gibi, kurum içinde olduğu süre boyunca bir gizlilik anlaşması imzalamalıdır.

b) Tedarikçilerin finansal durumu senelik olarak gözden geçirilmelidir. Bazı sektörlerde, iflas, batak, dolandırıcılık gibi olaylar çok sık gerçekleşmektedir.

c) Kuruluş dışından gelen bakım ve tamir çalışanları, diğer tedarikçilerde de olduğu gibi, kuruluş ile çalıştığı süre boyunca bir gizlilik anlaşması imzalamalıdır.

d) Kuruluş içinde kullanılan telefon rehberleri üçüncü tarafların eline geçmemelidir. Üçüncü taraflar kendi kuruluşlarına transfer olabilecek çalışanlarımızı görmemelidir.

e)Sadece uygun yetkileri almış olan çalışanların organizasyonun bilgi veya iletişim sistemlerine erişimi vardır.

f) Üçüncü taraflarla herhangi bilgi alışverişi yapılmadan önce bir gizlilik anlaşması yapılmalıdır.

g) Üçüncü taraflara kurumun network' üne erişim izni verilmeden önce bilgisayarlarını güvenliğe almaları gerekir. Kuruluş, üçüncü taraflara herhangi bir uyarıda bulunmadan ağa olan erişimlerini kesebilir.

h) Anlaşma sona erdiğinde, tarafların, birbirlerindeki dokümanları geri vermesi gerekir.

i) Kuruluş isminin halka yayınlanacak dokümanlarda kullanılabilmesi için üçüncü tarafların uygun kişiler tarafından yetkilendirilmesi gerekir.

j) Sadece yetkilendirilmiş tedarikçiler, kuruluşla çalışmakta olduklarını veya yapmakta oldukları işin doğasını halka yayabilirler.

k)Tedarikçiler kuruluşun sistemlerine erişmeden önce koşulların tanımlanmakta olduğu bir anlaşma imzalanmalıdır.

l) Gizli bilgilerin dağıtımını içeren kurallar belirlenmeli ve üçüncü taraflara bu bilgiler iletilmeden önce taraflarla bu kurallar hakkında anlaşılmalıdır.

m) Eğer bir gizlilik politikası, kuruluşun dezavantajlı olmasına neden oluyorsa, kuruluş bu dezavantajdan kurtulmak için bir üçüncü taraf kuruluşla anlaşma yapmamalıdır.

4- YAPTIRIM

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

P37 VARLIKLARA YÖNELİK SORUMLULUK POLİTİKASI

1- AMAÇ

Bu politikanın amacı CBÜ'nün, organizasyon el varlıklarını uygun koruma yöntemlerini belirlemektir.

2- SORUMLULAR:

Bu politikanın uygulanmasından Bilgi İşlem Daire Başkanlığı sorumludur.

3- UYGULAMA:

a) Her sene bir bilgi sistemleri envanteri yapılmalı ve bu konuda görevlendirilmiş kişiye bu liste verilmelidir. Bu çalışmanın amacı kuruluşun varlıklarını tespit etmek ve bu varlıkların kaybedilmesinin engellenmesini sağlamak.

b) Her bir bilgi sistemleri bileşenine okunabilir ve eşi olmayan bir kimlik numarası verilmelidir.

c) Rekabet avantajı sağlayabilmek için, kuruluş içinde geliştirilmiş sistem ve yazılımların da bu listeye eklenmesi gerekir. Bu liste her sene gözden geçirilecektir.

d) Herhangi bir yeni yaratılmış bilgi, her sene yenilenmekte olan veri bankasına girilmelidir.

e) Yeni üretilen bilginin bir sahibinin belirlenmesi ve bu bilginin uygun biçimde sınıflandırılması gerekir.

f) Organizasyonun sahip olduğu tüm sistemleri yönetebilecek, kullanıcı ayrıcalıklarını takip edecek ve erişim kontrol log' unu izleyecek bir güvenlik yöneticisi belirlenmelidir. Güvenlik

yöneticisinin kuruluşta bulunamayacağı durumlarda, bu görevi yerine getirebilmesi için bir çalışanın yetiştirilmesi gerekir.

g) Satın alınacak herhangi bir yazılım veya donanımın Satın Alma Bölümü aracılığı ile satın alınması ve bilgi güvenliği standartları ile uyumlu olması gerekir.

4- YAPTIRIM

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

P38 BASILI ÇIKTI VE DAĞITIM POLİTİKASI

1- AMAÇ

Bu politikanın amacı CBÜ'de basılı bilgisayar çıktısı ve dağıtılması ile ilgili kuralları tanımlamaktır.

2- SORUMLULAR:

Bu politikanın uygulanmasından Bilgi İşlem Daire Başkanlığı sorumludur.

3- UYGULAMA:

a) Tüm kritik bilgisayar raporlarının; bilginin hassasiyet seviyesine göre bir güvenlik sınıflandırma değeri olacaktır. Sınıflandırmayı bilgi sahibi kendisi yapacaktır.

b) Kâğıt ortamında basılı "Gizli" tanımlı raporların sadece hitap edilen kullanıcıya ulaştırılmasını güvence altına alacak metotlar belirlenecektir.

c) Kritik raporların dökümünü alan kullanıcı, rapor içeriğindeki bilginin uygun bir şekilde korunmasından sorumludur.

d) Herhangi bir kişi kendine ait olmayan kritik bir rapor bulur ise bu durumu CBÜ Bilgi İşlem Daire Başkanlığına bildirecektir.

e) "Gizli" kâğıt belgeleri kilitli dolap ve kasalarda muhafaza edilecektir.

f) "Gizli" kâğıt bilgileri FAKS ile iletilmeyecektir.

g) "Gizli" bilgi içeren dökümler ağ ortamında paylaşılmış yazıcılardan dökülüyor ise; dökümü başlatan kullanıcı beklemeden dökülen belgenin bulunduğu mahalle gidecek ve dökümün başkaları tarafından görülmesine imkân verilmeyecektir.

4- YAPTIRIM

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

P39 BİLGİ SINIFLANDIRMA VE ETİKETLEME POLİTİKASI

1- AMAÇ

Bu politikanın amacı CBÜ'nün bilgi varlıkları uygun koruma altına alınmasını sağlamaktır.

2- SORUMLULAR:

Bu politikanın uygulanmasından Bilgi İşlem Daire Başkanlığı sorumludur.

3- UYGULAMA:

a) Tüketicilere veya kuruluşun personeline yönelik tehlike arz eden herhangi bir ürün veya hizmet, bu tehlikenin doğasını açıklayacak biçimde tanımlanmalıdır.

b) Tüm bilgiler, aksi onaylanmadığı sürece gizli bilgi olarak nitelendirilmelidir.

c) Bir depolama ortamının çeşitli seviyelerde gizlilik içermesi durumunda, en yüksek gizlilik seviyesi içeren bilgiler öncelikli olarak kabul edilir.

d) Bilginin gizliliği hangi seviyede olursa olsun, ilgili yöneticilerin bu bilgiye ulaşımı mutlaka olmalıdır.

e) Ticari sırların neler olduğunu belirleyecek olan kişi mali müşavirdir.

f) Her bir bilgi parçası için bir elden çıkartma tarihi belirlenmelidir. Gerekirse bu tarihin uzatılması söz konusu olabilir.

g) Kullanıcılar, server'da belirlenmiş olan dosyalara kendi bilgisayarlarının yedeklerini kayıt etmelidir.

h) Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.

i) Sistemlere log-on olan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve yetki ihlalleri kontrol edilmelidir. Kullanıcı haklarını izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.

j) Gizlilik içeren bilgilerin iletişimi hakkındaki her türlü bilgi taahhütlü yollanmalıdır. Tüm bilgisayar sistemleri, alıcıya bizzat teslim edilmelidir.

k) Alıcılar, gizli bir bilgi alır almaz kendilerine bu konuda bilgi veren bir yazı iletilmelidir.

l) Gizli bilgiler, sadece yetkili bilgi sahibi tarafından kopyalanmalı ve bu kopyalama log book'ta belirtilmelidir. Kopyalama işlemini yürüten kullanıcı, fotokopide bırakmış olduğu dokümanlardan sorumludur.

m) Üçüncü taraflara açıklanan bilgileri içeren herhangi bir gizli belge gelecekte kopyalanmasını engelleyebilecek özel bir kağıt türüne basılmalıdır.

n) Kişiler tarafından yazılmış herhangi bir resmi dokümanın silinmez mürekkeple yazılması ve uygun şekilde işaretlenmesi gerekir. Yapılacak herhangi bir değişikliğin altı çizilmeli, tarihlenmeli ve yeniden onaylanmalıdır.

o) Gizli dokümanların tüm sayfaları numaralandırılmalıdır.

4- YAPTIRIM

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

P40 OLAY İHLAL BİLDİRİM VE YÖNETİM POLİTİKASI

1- AMAÇ
Bu politikanın amacı CBÜ'nün bilgi güvenliği olay ihlal süreçlerini belirler.

2- SORUMLULAR:
Bu politikanın uygulanmasından tüm personel sorumludur.

3- UYGULAMA:

a) Bilginin gizlilik, bütünlük ve kullanılabilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumlarında mutlaka kayıt altına alınmalıdır.

b) Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci oluşturulmalıdır.

c) Bilgi güvenliği ihlâli oluşması durumunda kişilerin tüm gerekli faaliyetleri hatırlamasını sağlamak maksadıyla bilgi güvenliği olayı rapor formatı hazırlanmalıdır.

d) Güvenlik olayının oluşması durumunda olay anında raporlanmalıdır.

e) İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.

f) Güvenlik ihlaline neden olan çalışanlar, üçüncü taraflarla ilgili resmi bir disiplin sürecine başvurulur.

g) Tüm çalışanlar, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği olayını önlemek maksadıyla güvenlik zayıflıklarını doğrudan kendi yönetimlerine veya hizmet sağlayıcılarına mümkün olan en kısa sürede rapor edilir.

h) Bilgi sistemi arızaları ve hizmet kayıpları, zararlı kodlar, dos atakları, tamamlanmamış veya yanlış iş verisinden kaynaklanan hatalar, gizlilik ve bütünlük ihlâlleri, bilgi sistemlerinin yanlış kullanımı gibi farklı bilgi güvenliği olaylarını bertaraf edecek tedbirler

alınır.

i) Normal olasılık planlarına ilave olarak olayın tanımı ve sebebinin analizi, önleme, tekrarı önlemek maksadıyla düzeltici tedbirlerin planlanması ve uygulanması, olaylardan etkilenen veya olaylardan kurtulanlarla iletişim, eylemin ilgili otoritelere raporlanması konuları göz önüne alınır.

j) İç problem analizi, adli incelemeler veya üretici firmadan zararın telafi edilmesi için aynı türdeki olayların izleme kayıtları (log) toplanır ve korunur.

k) Güvenlik ihlallerinden kurtulmak için gereken eylemler, sistem hatalarının düzeltilmesi hususları dikkate alınır.

l) Bilgi güvenliği olaylarının değerlendirilmesi sonucunda edinilen bilgi ile edinilen tecrübe ve yeni kontrollerin oluşturulması, aynı olayın tekrar etmesini önleyecek veya yüksek etkili olayların oluşmasını engelleyecektir.

m) Kanıt toplama; kuruluş içerisinde disiplin faaliyeti için delil toplanırken uygulanacak genel kurallar şunlardır;

- Kanıtın mahkemede kullanılıp kullanılamayacağı ile ilgili kabul edilebilirlik derecesi,
- Kanıtın niteliği ve tamlığını gösteren ağırlığı.

4- YAPTIRIM

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

P41 GÜVENLİ YAZILIM GELİŞTİRME POLİTİKASI

a) Mevcut sistem yazılımları üzerine kurulacak, kullanılacak yeni bir yazılım veya mevcut sisteme yapılacak olan güncellemeler ile etkisiz hale getirilmemelidir.

b) Yönetim sadece uygun yazılım projelerinin başlatıldığından ve proje altyapısının uygun olduğundan emin olmalıdır.

c) Uygulama yazılımlarının kurum içerisinde mi hazırlanacağı yoksa satın mı alınacağının belirlenmesi, uygun bir şekilde tanımlanmalıdır.

d) Sistem geliştirmede, ihtiyaç analizi, fizibilite çalışması, tasarım, geliştirme, deneme ve onaylama safhalarını içeren sağlıklı bir iş planı kullanılmalıdır.

e) Kurum içinde geliştirilmiş yazılımlar ve seçilen paket sistemler ihtiyaçları karşılamalıdır.

f) Yazılım geliştirme ve temin politikalarına uygun olmayan, ulusal ve uluslararası yazılım geliştirme standartları çerçevesinde geliştirilmemiş ve kurum talebi olmaksızın üretilmiş olan yazılımların kurumsal sistemler üzerine entegre edilmesine izin verilmemelidir.

g) Hazırlanan sistemler mevcut prosedürler dâhilinde, işin gerekliliklerini yerine getirdiklerinden ve iç kontrol yapıldığından emin olunması açısından test edilmeli, yapılan testler ve test sonuçları belgelenerek onaylanmalıdır.

h) Yeni alınmış veya revize edilmiş bütün yazılımlar test edilmeli ve onaylanmalıdır.

i) Eski sistemlerdeki veriler tamamen, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılmalıdır.

j) Uygulama ortamına aktarılma kararı uygun bilgilere dayalı olarak, ilgili yönetim tarafından verilmelidir.

k) Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.

l) Yazılımlar sınıflandırılmalı/etiketlenmeli ve envanterleri çıkarılarak bir yazılım kütüğünde muhafaza edilmelidir.

m) İlgili yazılım denetim süreçlerine göre yazılım geliştirme sureci politikasının gözden geçirilmesini önerilmektedir.

n) Taraflarca geliştirilen yazılımın proje yönetimi, yazılım geliştirme, test ve kabul esasları tanımlanmalıdır.

o) Kurumsal yazılım geliştirme esasları yayınlanmışsa ona uygun geliştirme talep edilmelidir. Fonksiyon isimlendirme, yorum kullanımı, kullanılan yazılım dili vb.

p) Sistem yazılımında mevcut olan kontroller, kullanılacak yeni bir yazılım veya mevcut sistem yazılımına yapılacak olan güncellemeler ile etkisiz hale getirilmemelidir.

q) Sistem geliştirmede, ihtiyaç analizi, fizibilite çalışması, tasarım, geliştirme, deneme ve onaylama safhalarını içeren sağlıklı bir iş planı kullanılmalıdır.

r) Kurum içinde geliştirilmiş yazılımlar ve seçilen paket sistemler ihtiyaçları karşılamalıdır.

s) Kurumda kişisel olarak geliştirilmiş yazılımların kullanılması engellenmelidir.

t) Hazırlanan sistemler mevcut prosedürler dâhilinde, işin gerekliliklerini yerine getirdiklerinden ve iç kontrol yapıldığından emin olunması açısından test edilmeli, yapılan testler ve test sonuçları belgelenerek onaylanmalıdır.

u) Yeni alınmış veya revize edilmiş bütün yazılımlar test edilmeli ve onaylanmalıdır.

v) Eski sistemlerdeki veriler tamamen, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılmalıdır.

w) Uygulama ortamına aktarılma kararı uygun bilgilere dayalı olarak, ilgili yönetim tarafından verilmelidir.

x) Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.

y) Yazılımlar sınıflandırılmalı/etiketlenmeli ve envanterleri çıkarılarak bir yazılım kütüğünde muhafaza edilmelidir.

BİLGİ GÜVENLİĞİ POLİTİKASI ONAYI

4.0 Amaç

Bu form CBÜ Bilgi Güvenliği Politikasının okunduğu, anlaşıldığı ve kabul edildiğinin onaylandığı bir dokümandır.
Bu formu Bilgi işlemden sorumlu çalışanlar ve yöneticiler onaylayacaktır. Kurumun en üst yöneticisi bu politikanın uygulanabilirliğinden sorumludur.

İzlenecek Prosedür

Aşağıdaki adımlar takip edilmelidir.

1- Bilgi Güvenliği politikasını okuyunuz.
2- Aşağıda belirtilen bölümlere tarih atınız ve imzalayınız.
3- Bu sayfayı ilgili birim amirine iletiniz.

Anlaşma

Bu forma imza atarak aşağıda yazılanları kabul etmiş oluyorum.

CBÜ bilgi güvenliği politikasının bir kopyasını teslim aldım, okudum ve anladım.

Çalışanın imzası: _____

Çalışanın Adı Ve Soyadı: _____

Tarih:_____

Çalıştığı Birim:_____

	HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
ÜNVANI	BGYS EKİP LİDERİ	BGYS YÖNETİM TEMSİLCİSİ	REKTÖR
İMZA			