Bilgi Güvenliği Yönetim Sistemi Politikalarının amacı, Kapadokya Üniversitesi personeli ve öğrencilerinin, bilgi ve varlıklarının; gizlilik, bütünlük ve erişilebilirlik kapsamında bilgi güvenliğini, uyulması gereken kurallarını belirlemek ve bu sınırlar doğrultusunda iş sürekliliğini sağlamaktır.

Üniversitemiz bilgi güvenliği gereksinimleri sağlamak için değişime açık, iyi eğitim almış, konusunda yetkin personel istihdamını sağlayacaktır. Ayrıca bilgi güvenliğinin sağlanması amacıyla gerekli olan alt yapısını oluşturmak ve sürekliliğini sağlamak için finansmanı, yeterli donanım ve altyapıyı bulunduracaktır.

Bilgi güvenliği sistemi faaliyetlerimiz, acil durum planları, veri yedekleme prosedürleri, virüslerden ve bilgisayar korsanlarından sakınma, erişim kontrol sistemleri ve bilgi güvenliği ihlal bildirimi gibi konulardan oluşmaktadır.

Risk değerlendirmeleri sonucunda amaçlarımızı belirleyip bu amaçlarım başarılması için gerekli olan kaynaklar ve şartlar sağlanacaktır. Yapılan risk değerlendirmeleri sonucunda sistemde tespit edilen açıklar ve tehditler bertaraf edilerek öğretim elemanlarımızın, idari personellerimizin, öğrencilerimizin ve üniversiteye gelecek misafirlerimizin bilgilerinin bilgi güvenliği politikamız gereği korunması sağlanacaktır.

Bilgi Güvenliği politikalarımızı yerine getirmek için başta çalışanlarımızın Bilgi Güvenliği Yönetim Sistemi şartlarını çalışma biçimi haline getirmeleri sağlanacaktır. Tüm personel ve belirli üçüncü tarafların Bilgi Güvenliği Yönetim Sistemi ile ilgili uygun eğitimleri alması sağlanacaktır.

Bilgi güvenliği ile ilgili uygulanabilir şartlar ve bu şartların getirdiği fırsatlar ve gereklilikler yerine getirilecek ve bu şartlar sürekli iyileştirilecektir. Akademik ve idari personelimizin (tedarikçilerimizin personelleri dahil) ve tüm ilgili tarafların bu sisteme adaptasyonu sağlanacaktır.

Politikalar:

Bİ.BGP.002 Erişim Kontrolü Politikası: Üniversitemizde üretilen verinin bütünlüğünün sağlanması için:

- Oryantasyon aşamasında personele gerekli bilgiler aktarılmış,
- Gerekli altyapı ve donanım belirlenmiş,
- Gerekli altyapı ve donanımın kesintisiz olarak sağlanması için, gerekli kaynaklar ayrılmış,
- Üniversitemizin, akademik ve idari personelleri, öğrencileri, üniversitemize gelen misafirler, hastanemizde tedavi olan hastaların bilgilerinin korunması açısından yapılması gerekenler

personellerle çeşitli eğitimlerle (ISO 27001 Temel Eğitimi, KVKK Eğitim vb.) aktarılmış, üniversite çalışanlarına "iş sözleşmeleri" ile sorumlulukları yazılı hale getirilmiş,

- Tüm verilerin yedeklenmesi amacıyla gerekli alt yapı belirlenip, sorumlular tanımlanmış,
- Network üzerinde gerekli erişim işlemleri sınırlandırılmıştır.

❖ Bilgi güvenliği konusundaki 3 temel prensip gizlilik, bütünlük ve erişilebilirlik olarak belirlenmiştir.
❖ Üniversite politikaları doğrultusunda içerik filtreleme sistemleri kullanılır. İstenilmeyen siteler (zararlı yazılım, oyun, kumar, şiddet içeren vs.) Bilgi İşlem Dairesi tarafından engellenir.
❖ Üniversitenin ihtiyacı doğrultusunda Saldırı Tespit ve Önleme Sistemleri kullanılır.
❖ Bilgi güvenliğinin tesis edilmesi amacıyla antivirüs yazılımları kullanılır. İnternetten gelen/giden bütün trafik virüslere karşı taranır.
❖ Kullanıcıların internet erişimlerinde firewall, antivirüs, içerik kontrol vs. güvenlik önlemleri mevcuttur.
❖ Ancak yetkilendirilmiş kişiler internete çıkarken, normal kullanıcılarının bulunduğu ağdan farklı bir ağda olmak kaydıyla, bütün servisleri kullanma hakkına sahiptir.
❖ 5651 sayılı kanun (İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun) gereği kurum internet erişim kayıtları en az iki yıl arşivlenir.
❖ Tunnel platformları, VPN (Kurum Dışı VPN), PROXY ve DNS değişiklikleri yapılarak internete bağlanılması yasaktır.
❖ ICQ, GTALK, SKYP vb. mesajlaşma yazılımları kullanılamaz.
❖ Başkalarının fikri haklarını ihlal edici (copyright) materyalin (yazı, makale, kitap, film, müzik eserleri vb.) dağıtımı yasaktır.
❖ Sistem ve ağ güvenliğinin ihlal edilmesi yasaktır, cezai ve hukuki mesuliyetle sonuçlanabilir. Kurum bu tür ihlallerin söz konusu olduğu durumları inceler ve bir suç oluştuğundan şüphe duyulursa Disiplin Talimatına göre karar alınır veya yasa uygulayıcısı ile iş birliği yapabilir.

Bİ.BLP.008 Güvenlik Politikası:

Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binada ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanmış ve erişim izinleri bu doğrultuda belirlenmiştir.

Tanımlanan farklı güvenlik bölgelerine erişim yetkileri düzenli aralıklar ile kontrol edilir.

Bina girişleri ve kampüs içi güvenlik amacıyla kamera ile kayıt altına alınmakta ve izlenmektedir.

Kritik sistemler sunucu kabininde tutulmaktadır.

Kritik sistemler elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmaktadır.

Açık ofislerde bulunan gizli bilgi varlıklarının olduğu dolaplar ve çekmeceler kilitli ve kontrol altında tutulmalıdır.

Ekipmanların kullanımı zimmetlenen kişiye aittir, bu ekipmanların güvenliğini sağlanması kişinin sorumluluğundadır. Teslim edilen ekipmanlara gelecek zararlar zimmet edilen kişiden tahsil edilecektir.

Kritik veya hassas iş faaliyetlerini desteklediği belirlenen tüm bilgi teknolojisi araçları, kilitli veya benzeri girişlerle korunan, fiziksel erişim kontrolü gerektiren alanlarda bulundurulmaktadır.

Koruma altındaki bölgelere alınacak ziyaretçilere atanmış kurum personeli eşlik eder ve ziyaretleri süresince yalnız bırakılmaz.

Bilgi Teknolojisi araçlarının, herhangi bir elektrik kesintisinde çalışmalarına devam etmeleri için kullanılan UPS, jeneratör gibi güç kaynakları yılda 1 defa periyodik olarak kontrol edilir.

Tüm donanımların düzenli periyotlarla bakımları yapılır.

Dizüstü bilgisayar, belge, CD ve taşınabilir bellek gibi varlıkların korunması için gerekli önlemlerin alınmasından varlık sahibi olarak kaydedilmiş kişi sorumludur.

Üniversite içerisinde kullanılan yazılım ve donanımlara ait sistemleri kullanımı eğitimler ile sağlanır.

Yazılı prosedürler ihtiyaç duyulduğunda ilgili birim yöneticisi tarafından hazırlanır ve onaylanarak güncellenir.

Üniversite genelinde tüm işlerin prosedürleri yazılı olarak bulunur ve ihtiyaç duyulduğunda kalite.kapadokya.edu.tr web adresinden erişim sağlanabilir.

Kurum bünyesindeki bütün sunucuların yönetiminden sadece yetkilendirilmiş sistem yöneticileri sorumludur.

Bütün sunucular (kurumun sahip olduğu) ilgili envanter yönetim sistemine kayıtlıdır.

Dış ortamdan (Firmalar, yöneticiler vb.) sisteme bağlanan kullanıcıların erişim logları firewall, analyser üzerinde kayıt altına alınmaktadır.

Sunucular fiziksel olarak güvenlik önlemi alınmış kabinetlerde bulundurulur.

Sunucu kabinindeki ekipmanların bakımları düzenli olarak yapılır, bakım kayıtları tutulur.

Elektrik ve data kabloları kurum içerisinde kanallardan geçirilir.

Elektrik kesintilerinden sunucu ve diğer ekipmanların etkilenmemesi için UPS sistemine bağlantısı mevcuttur ve sistem jeneratör ile desteklenmektedir.

Tüm sistem ve ağ ekipmanları yılda en az 1 defa tarama testlerinden geçirilerek güvenli hale getirilmelidir.

Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için orijinal kayıt ortamları ve birer adet kopyası yetkili kimselerin erişebileceği güvenilir yerlerde muhafaza edilir.

Ağ ekipmanları sadece yetkilendirilmiş kişiler tarafından erişilebilir ve yönetilebilir olmalıdır. Yetkisiz erişime karşı korunmalıdır.

Kurum ağına sadece kurum bilgisayarları bağlanabilir. Kurum dışında bir bilgisayar bağlanacak ise yetkili kişinin izni ve gözetiminde bağlanabilir.

Kurum internet ağı misafirler kullanıcılara kapalıdır.

Uzaktan bağlantı için kullanılacak portların güvenliği Bilgi İşlem Dairesi tarafından sağlanmaktadır.

Ağ cihazları üzerinde yapılan her işlemin logları firewall, analyser üzerinde kayıt altına alınmaktadır.

Günde iki defa bir transaction backup olarak usb hard diske ve merkez sunucuya yedeklenmesi sağlanır. Veriler offline ortamda süresiz olarak saklanır.

Alınan yedeklere yılda 1 olmak üzere veri kurtarma testi yapılır, sonuçlar mailerle kayıt altına alınır. Test sonuçlarına göre var ise açıklıkların kapamaları takip edilerek kapatılır.

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

Dış firma çalışanları ile yapılan sözleşmelere göre verilerin korunması sağlanır.

Bilginin gizlilik, bütünlük ve erişilebilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumları mutlaka kayıt altına alınmalıdır. İhlal bildirimleri Bilgi Güvenliği Yönetim Temsilcisine mail ile yapılmalıdır.

Bilgi Güvenliği Olay Bildirim Formunda olaylara müdahale süreci detaylı olarak belirlenmiştir.

Yaşanan Bilgi güvenliği ihlâli olayları Bilgi Güvenliği Yönetim Temsilcisi ile birlikte değerlendirilmelidir.

İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru olup olmadığı Disiplin Talimatına uygun şekilde yönetilmelidir.

Kanıt toplama faaliyetinde aşağıdaki süreçler takip edilmelidir;

Kanıtın niteliği ve tamlığını gösteren içerik.

İhlale neden olan olayların kanıtları için kamera kayıtları, giriş çıkış kayıtları, sunucu/program ve bilgisayar logları, firewall logları ve internet loglarından faydalanılır.

Olay kanıtlarının korunması yetkili kişilerin dışında erişimi kapatarak veya yedekleme yaparak sağlanır.

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

Kurum sistemlerine erişim sağlayacak çalışanlar için bilgisayar erişim hesapları doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişim yapacağı Bilgi Güvenliği Yönetim Temsilcisi tarafından belirlenir.

Kurum sistemlerine erişmesi gereken tedarikçilere yönelik kullanıcı hesabı Bilgi İşlem Birimi tarafından ilgili yetkiler verilerek tanımlanır.

Kurum bünyesinde kullanılan ve merkezi olarak erişilen uygulama yazılımları, paket llar, veri tabanları, işletim sistemleri üzerindeki kullanıcı yetkileri denetim altında tutulmalıdır.

Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.

Bİ.BGP.005 Tedarikçi İlişkileri Politikası:

Tedarikçilerimizin, Kapadokya Üniversitesinde uygulanan Bilgi Güvenliği Yönetim Sistemi Şartlarına uygun olarak faaliyet göstermesi gerekir.

Malzeme ve hizmet tedarikçileri bilgi sistemlerimize veya bilgi varlıklarımıza bakım vb. amaç ile geldiklerinde Gizlilik Sözleşmesi yapılması gerekmektedir.

Tedarikçilerimizin özellikle yapılacak tedarikçi sözleşmelerine uyum sağlaması önemlidir. Bu sözleşmeler verilerini korumakla yükümlü olduğumuz akademik personel, idari personel, öğrencilerimiz ve hizmet alıcıları için ayrı önem taşımaktadır.

Tedarikçilerimizin yasal gereklilikleri yerine getiren ve bu politika ve kurallar ile beraber iş etiği ile bağlantılı olan diğer tüm dokümanlardaki gerekliliklere bağlı tedarikçiler olması gerekmektedir.

Tedarikçi seçiminde; mali performans, tecrübe, teknik yeterlilik vb. kriterlerin yanında bu alanda olumlu bir geçmişe sahip olmaları ve önceki yıllara ait değerlendirme sonuçları dikkate alınır.

Tedarikçi seçimi ve yönetimi için ilgili daire başkanları onaylı tedarikçi listesi hazırlama, yönetme ve takip sistemlerinin kurulmasından sorumludur.

Birlikte çalışmaya karar verdiğimiz tedarikçilerimizi seçerken objektif kriterlere göre değerlendiriyoruz. Kapadokya Üniversitesi olarak tedarikçilerimiz ile iş ilişkilerimizde karşılıklı değer yaratmayı hedeflemekteyiz.

Kapadokya Üniversitesi olarak tedarikçilerimizin yasalara, kurallara, düzenlemelere bağlı kalmasını hedefleriz. Tedarikçilerin, birlikte çalıştıkları tedarikçilerin ve taşeronlarının işle ilgili uygulamalar konusunda bilgi sahibi olmasını bekleriz.

Kapadokya Üniversitesi, bu kurallara uymayan tedarikçilerle ilişkilerini sonlandırma hakkını saklı tutar.

Üçüncü taraflar kurum içerisinde bulundukları sürece kurum politikalarına uygun hareket etmekle yükümlüdür.

Malzeme ve hizmet tedarikçileri kurumun bilgi sistemlerine kendilerine verilen yetki kapsamında erişim sağlayabilirler.

Verilen erişim yetkileri, erişim amaçlarına uygun olacak şekilde kısıtlı olup, logları saklı tutulur ve çalışma bittikten sonra verilen yetkiler geri alınır.

Kapadokya Üniversitesi , tedarikçi, bakım firmaları veya üçüncü taraflara herhangi bir uyarıda bulunmadan ağa olan erişimlerini kesebilir.

Bİ.BGP.006 Kişisel Verilerin Korunması ve İşlenmesi Politikası:

Bİ.BGP.003 Temiz Masa Temiz Ekran Politikası:

Temiz Masa Temiz Ekran Politikamızın amacı, normal çalışma saatleri süresince ve dışında bilgiye yetkisiz erişim, bilgi kaybı ve hasarı risklerini azaltmak amacıyla kâğıtlar, kaldırılabilir depolama ortamları ve kişisel bilgisayarlar için gerekli şartları tanımlamaktır.

Personel; bilgisayar, USB bellek, harici disk vb. veri depolamanın mümkün olduğu ortamlardaki gizlilik içeren her türlü belgenin güvenliğini sağlamakla yükümlüdür.

Akademik ve idari personelin aşağıdaki şartlara uygun davranmaları gerekmektedir.

1. Çalışma saatleri dışında bilgisayarlar kapalı ya da kilitli şekilde bırakılmalıdır. Çalışma saatleri içerisinde başından ayrıldığında mutlaka bilgisayar kilitli bırakılmalıdır. (Ekran koruyucu 5-10 dk arasında devreye girmelidir ve şifre koruması olmalıdır.)

2. Yazıcıların üzerinde kişisel bilgileri ve gizli bilgileri içeren dokümanlar (müsvedde olsalar bile) bırakılmamalıdır.

3. Mesai bitiminde çalışma masası üzerinde kurum veya kişisel bilgileri içeren bir evrak bırakılmamalıdır.

4. Kuruma ait dokümante edilmiş gizli bilgiler kilitli ortamda tutulmalıdır.

5. Gizlilik dereceli evraklar, işlevini tamamladıktan sonra imha edilmelidir.

6. Bilgisayarların masaüstlerinde kuruma ait özel bilgiler içeren dokümanlar bulundurulmamalıdır.

7. Bilgisayarlara ait olan şifreler kesinlikle kâğıt ortamlara yazılı bir şekilde bırakılmamalıdır.

8. Personel, gizli bilgi içeren evrakı ağ üzerinden paylaşamaz, gizli bilgi içeren evrak imha edilmesi gerekiyorsa kağıt kırpma makinası veya elle parçalanarak imha edilir.

9. USB veya harici diske gizli/önemli verilerin konulması gerekiyorsa şifrelenerek saklanır.

10. Masa çekmecelerinin anahtarları, kasa anahtarları masa üzerinde bırakılmamalıdır.

Bİ.BGP.007 Mobil Cihaz Politikası

Kontrol: Mobil cihazların kullanımı ile ortaya çıkan risklerin yönetilmesi amacı ile bir politika ve destekleyici güvenlik önlemleri belirlenmelidir.

Uygulama Kılavuzu: Mobil cihazlar kullanılırken, is bilgilerinin ele geçirilmemesini temin için özel bir önem gösterilmelidir. Mobil cihaz politikası, korumasız ortamlarda mobil cihazların çalışması riskini hesaba katmalıdır.

Mobil cihaz politikası aşağıdaki hususları dikkate almalıdır:

a) Mobil cihazların kaydı,

b) Fiziksel koruma için gereksinimler,

c) Yazılım kurulum kısıtlaması,

d) Mobil cihaz yazılım sürümleri ve yamaların uygulanması için gereksinimler,

e) Bilgi hizmetlerine bağlantı kısıtlaması,

f) Erişim kontrolleri,

g) Kripto grafik teknikler,

h) Kötücül yazılım koruması,

i) Uzaktan devre dışı bırakma, silme ya da kilitleme,

j) Yedekleme,

k) Web servislerinin ve web uygulamalarının kullanımı.

Halka açık yerlerde, toplantı odalarında ve diğer korumasız alanlarda mobil cihazların kullanımına dikkat edilmelidir. Bu cihazlar tarafından saklanan ve islenen bilginin, açıklanmasına ya da yetkisiz erişimine karsı koruma bulunmalıdır. Örneğin; kartografi teknikleri kullanmak (bk. Madde 10) ve gizli kimlik doğrulama bilgisinin kullanımını zorlamak (bk. Madde 9.2.4).

Mobil cihazlar; araba ve diğer ulaşım araçları, otel odaları, konferans merkezleri ve toplantı salonları gibi yerlerde hırsızlığa karsı fiziksel olarak da korunmalıdır. Mobil cihazların çalınması ya da kaybolması durumları için yasal, sigorta ve kurulusun diğer güvenlik gereksinimleri dikkate alınarak özel bir prosedür oluşturulmalıdır.

Önemli, hassas ya da kritik is bilgilerini taşıyan cihazlar sahipsiz bırakılmamalı, mümkünse fiziksel olarak kilitlenmeli ya da cihazı güvenli hale getirmek için özel kilitler kullanılmalıdır.

Mobil cihaz kullanan personeller için, bu şekilde çalışmalardan kaynaklanan riskler ve uygulanması gereken kontroller ile ilgili olarak farkındalıklarının arttırılması amacıyla eğitim düzenlenmelidir.

Mobil cihaz politikası kişisel mobil cihazların kullanımına izin veriyorsa, politika ve diğer güvenlik önlemlerinde aşağıdaki hususlara dikkat edilmelidir:

a) Cihazların özel ve is kullanımının ayrılması. Bu ayrım özel cihazda bulunan iş verisinin ayrılması ve korunması gibi yazılımların kullanılmasını içerir,

b) Kullanıcıların görevlerini kabul ettikleri son kullanıcı anlaşmasını imzalamalarından sonra iş bilgilerine erişim sağlanması (fiziksel koruma, yazılım güncelleme vb.), is verilerinin sahipliğinden feragat, cihazın çalınması ya da kaybolması ya da hizmetin kullanımı

yetkilendirmesi için vakit olmadığında kuruluş tarafından verilerin uzaktan silinmesine izin verilmesi. Bu politikada mahremiyet mevzuatının dikkate alınması gerekmektedir.

Diğer Bilgiler: Mobil cihazların kablosuz ağ bağlantıları (wi-fi) diğer ağ bağlantısı türlerine benzer, ancak; kontrollerin tanımlanmasında önemli farklılıklara dikkat edilmelidir. Tipik farklılıklar şunlardır:

a) Bazı kablosuz güvenlik protokolleri olgunlaşmamıştır ve bilinen açıklıklara sahiptir,

b) Mobil cihazlarda depolanan bilgiler, kısıtlı ağ bant genişliği ya da yedeklemelerin planlandığı zamanlarda mobil cihazların bağlanamaması nedeniyle yedeklenemeyebilir. Mobil cihazlar sabit kullanım cihazları ile genellikle ağ, internet erişimi, e-posta ve dosya isleme gibi ortak fonksiyonları paylaşır. Bilgi güvenliği kontrolleri mobil cihazlar için genellikle sabit kullanım cihazlarında kabul edilen kontrollerden ve bu cihazların kurulusun tesisi dışındaki kullanımı ile gündeme gelen tehditleri ele alan kontrollerden oluşur.

Kuruluşa ait bilgi içeren taşınabilir cihazlar ilgili kişiye zimmetlenerek teslim edilmelidir.

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

Etki alanı dâhilindeki bilgisayarlar istisnalar dışında admin yetkisi sınırlandırılarak yalnızca User yetkilendirmesi ile ilgili kişiye teslim edilmelidir. Etki alanından bağımsız olan bilgisayarların sorumluluğu personele aittir.

Mobil cihazlara yetkisiz erişime karşı şifre tanımlanmalıdır.

Cep telefonları veya tablet bilgisayarlara kurum e-postası kurulması halinde cihazın güvenliğinin sağlanması adına şifre koruması olması zorunludur.

Etki alanı dâhilindeki bilgisayarlar üzerinde yapılan çalışmalar ve oluşturulan dosyalar birimlere ait ilgili ortak alana kaydedilmelidir.

Mobil cihazların (Dizüstü Bilgisayar, Tablet vb.) aile bireyleri dâhil zimmetlenen kişiler dışında kullanılması yasaktır.

Kaybolması ve çalınması kolay olduğundan mobil cihazlar başıboş bırakılmamalıdır.

Verilerin yedekleri alınmalı ve güncel bir kopyası farklı bir yerde saklanmalıdır.

Mobil cihazların uzaktan devre dışı bırakma ve silme özellikleri mutlaka kullanılmalıdır.