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.

- 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.