PO.02 Bilgi Güvenliği ve Yönetim Sistemi Politikası

1. Amaç

Kahramanmaraş Sütçü İmam Üniversitesi(KSÜ), verdiği hizmetlerinin veri güvenliğini ve sürdürülebilirliğini en üst düzeyde tutmak ve olası bilgi kayıplarını en aza indirgemek için fiziksel ve yazılımsal erişimlerin sınırlandırılmasına ihtiyaç duyar.

Bu doğrultuda üst yönetim tarafından onaylanmış olan BGYS Politikasının amacı,

1.1. Gelen ziyaretçilerin kayıt ve denetim altına alınmasını sağlamak,
1.2. Sistem Odası erişimleri sınırlandırmak,
1.3. Sunuculara ve Ağ donanımlarına erişimleri sınırlandırmak,
1.4. Sistem Yönetim yazılımlarına yetkisiz erişimleri engellemek,
1.5. Sistemde mevcut bilgilerin gizliliğini, bütünlüğünü ve devamlılığını sağlamak ve bununla ilgili önlemleri almaktır.

2. Kapsam

Bu politika;

2.1. KSÜ yerleşkelerinde yer alan personel, öğrenci, misafir kullanıcıları ve dış paydaşların kurum ağ ve sistemlerine erişimini,
2.2. Bilgi İşlem altyapısını kullanmakta olan tüm birimleri ve çalışanları,
2.3. Ağ ve sisteme dahil olan tüm kullanıcı ve personelin ağ erişim kural ve sorumluluklarını kapsamaktadır.

3. Kısaltmalar ve Açıklamalar

3.1. **KSÜ:** Kahramanmaraş Sütçü İmam Üniversitesi
3.2. **BGYS:** Bilgi Güvenliği Yönetim Sistemi
3.3. **CDDO:** Cumhurbaşkanlığı Dijital Dönüşüm Ofisi
3.4. **Dış Kaynaklı Belgeler Tablosu:** Bilgi İşlem Daire Başkanlığının kayıt altına aldığı dış kaynaklı belgelerin tablosu.
3.5. **Kayıtların Denetimi Prosedürü:** Bilgi İşlem Daire Başkanlığı tarafından hazırlanan kayıtların arşiv sürelerinin güncellenmesiyle ilgili bilgileri içeren prosedür.
3.6. **İlişik Kesme Formu:** Personel Daire Başkanlığı tarafından hazırlanan kurumdan ayrılacak olan personel için ilişik kesme formu.
3.7. **MERNİS:** Merkezi Nüfus İdaresi Sistemi.

3.8. **SMS:** Kısa Mesaj Servisi.

3.9. **Dış Paydaş:** Kurumdan etkilenen veya kurumu etkileyen kurum dışındaki kişi, grup veya kurum/ kuruluşlardır.

3.10. **GEM (Genel Erişim Matrisi):** Kurumumuz tarafından kullanılan bilgi varlıklarına, hangi kullanıcıların hangi yetki düzeyinde eriştiğini gösteren tablodur.

3.11. **Kullanıcılar:** KSÜ ağ ve sistem yapılarını kullanan tüm kişiler

3.12. **Personeller:** KSÜ bünyesinde çalışan tüm personeller

3.13. **Sistem/ Ağ /Uygulama Yöneticileri:** KSÜ Ağ, sistem ve uygulamalar yapısının işleyişinde görevli yöneticiler.

3.14. **Bilgi İşlem Personeli:** Bilgi İşlem Daire Başkanlığında görevli yetkili personel.

3.15. **Varlık Envanteri:** KSÜ Bilgi varlıklarının durumunu gösteren çizelge

3.16. **Birim / Bölüm Yöneticisi:** KSÜ bünyesindeki birim ya da bölümün yetkili yöneticisi.

4. Politika Konuları

4.1. Genel Bilgiler

4.1.1. İş uygulamalarıyla ilgili güvenlik gereksinimleri karşılayabilmek için ekip kurulur. Gerekli denetimler yapılarak gözden geçirilir ve yaptırım kararı alınır.

4.1.2. Bilgi sınıflandırmayla ilgili olarak CDDO tarafından hazırlanan Bilgi ve İletişim Güvenliği Rehberinde "2.1.1 Varlık Gruplarının Belirlenmesi" prosedürü bilgileri sınıflandırmak için ve GEM yetkilendirme için kullanılır.

4.1.3. Sistemler ve ağlara erişim hakları ile ilgili işlemler CDDO tarafından hazırlanan Bilgi ve İletişim Güvenliği Rehberinde yer alan "2. Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci" prosedürleri dikkate alınarak uygulanmaktadır.

4.1.4. "Dış Kaynaklı Belgeler Tablosu" takip edilip ve kayıtların arşiv sürelerinin güncellenmesiyle ilgili bilgiler "Kayıtların Denetimi Prosedürü" ile denetim altına alınmaktadır.

4.1.5. E-posta yoluyla Bilgi İşlem Yöneticisi aracılığıyla erişim talepleri toplanır. Bilgi İşlem Daire Başkanı tarafından e-posta yoluyla talepler onaylanır veya reddedilir.

4.1.6. Erişim haklarının kaldırılması talebi e-posta yoluyla Bilgi İşlem Yöneticisine iletilir. Bilgi İşlem Daire Başkanı tarafından talep onaylanır veya reddedilir. İlgili birimlere "İlişik Kesme Formu" doldurularak herhangi bir yetkisinin ve erişim hakkının kalmadığı, ilişkinin kesildiği beyan edilir.

4.2. Ağlara ve Ağ Hizmetlerine Erişim

4.2.1. Kurum ağ ve ağ kaynaklarına erişim yetkisi, personelin görev ve sorumluluklarını yerine getirebilmesi için "gerektiği kadar" yetkiye sahip olması ilkesine göre verilir ve erişim verilmeden önce ilgili yöneticilerden onay alınır. Her bir iş fonksiyonu ve görevi için gerekli olan ağ ve ağ hizmetleri önceden belirlenir ve belgelenir.

4.2.2. Kullanıcıların ağ üzerinden bağlantı yetkileri güvenlik duvarı erişim-denetim listeleri vasıtasıyla kısıtlanır. İş tanımlarının gerektirdiğinden daha fazla ağ hizmeti erişimine, ancak Bilgi İşlem Daire Başkanlığı tarafından onay alındığı ve ağ hizmeti kurumun genel güvenlik ilkelerine uygun olduğu takdirde izin verilir.

4.2.3. Sistem yöneticileri işletim sistemini, ağ erişimine izin vermeden önce her bir kullanıcının kimliğini doğrulayacak şekilde yapılandırır. Yapılandırma işlemi sonrası, sistem yöneticisi ilgili işlemi Bilgi İşlem Daire Başkanına rapor olarak sunar.

4.2.4. Uzaktan erişim ancak sınırlı olarak sağlanır ve uzaktan erişime ilgili bölüm yöneticisinin ve Bilgi İşlem Daire Başkanı onayı alındıktan sonra izin verilir.

4.2.5. Yönlendirici ve güvenlik duvarı gibi kritik cihazlara erişim yetkisi yalnızca kurum Bilgi İşlem ağına bağlı terminallere verilir. Cihazlar yalnızca yetki onaylı terminallerden yönetilirler.

4.2.6. Denetim ve ayarlar için kullanılan bağlantı noktalarına (port) fiziksel ve mantıksal erişim, sistem yöneticisi tarafından sınırlandırılır ve Bilgi İşlem Yöneticisi tarafından denetlenir.

4.2.7. Ağ ve ağ hizmetlerini içeriden ya da dışarıdan yapılan tüm erişimler yasal düzenleme gereği kayıt altına alınır. Bu kayıtlar düzenli olarak gözden geçirilir ve yetkisiz bir şekilde ağ hizmetlerinin kullanılmaması ya da ağ hizmetlerine yetkisiz personelin erişmemesi sağlanır. Bilgi İşlem Yöneticisi, sistem ve ağ yönetmeni ile birlikte düzenli olarak hazırladığı bu kayıtları periyodik olarak Bilgi İşlem Daire Başkanına sunar.

4.2.8. Ağlar, içerdikleri bilginin kritikliğine göre mantıksal veya fiziksel olarak ayrılır. Ağ mantıksal olarak ayrılmışsa, uygun bölgesel güvenlik cihazları kullanılır. Ağ fiziksel olarak ayrılmışsa, tüm ağ giriş noktalarına fiziksel erişimi korumak için gerekli denetimler bulundurulur.

4.2.9. Tüm ağ donanımı (yönlendirici, switch, vs.) ilk şifreleri, yönetici görevine sahip personel tarafından Bilgi İşlem Daire Başkanının onayına istinaden kurulum aşamasında değiştirilir. Ve bütün bu şifreler özel ve güvenlikli bir yerde saklanır.

4.2.10. Kuruma ait bilginin gizliliğini korumak için, kurum ağları işletmeyle ilgisi olmayan özel ve/veya kişisel bilginin iletimi için kullanılamaz.

4.2.11. Bir uzaktan erişim yazılımıyla doğrudan kişisel bilgisayarlara bağlanmış kişisel haberleşme ekipmanlarının (modem, ISDN kart vb.) kullanımına izin verilmez.

4.2.12. Üçüncü kişilere erişim, bu gereksinimin detaylı bir analizi yapılıp içerdiği riskler değerlendirildikten sonra sağlanır.

4.2.13. İnternet erişimi, iş tanımından ötürü bu erişime gereksinim duyan ve birim yöneticisi tarafından onaylandığı takdirde tüm çalışanlara görevleri kapsamına göre sağlanır.

4.2.14. Misafirlerin internete girebilmesi için ayrıca bir misafir ağı üzerinden internet erişimi sağlanır.

4.3. Kullanıcı Erişim Yönetimi

4.3.1. Kullanıcı kimlik bilgileri şifrelenerek saklanır ve doğrulamasıyla ilgili kayıtlar günlüklerde tutulur.

4.3.2. Ayrıcalıklı erişim hakkı (admin yetkisi) Bilgi İşlem Daire Başkanındadır. Ayrılmış olan tüm ayrıcalıkların kayıtları tutulmaktadır. Ayrıcalıklı erişim hakkının sona ermesi için uygulanacak işlemler erişim haklarının sona erdirilmesi için uygulanacak işlemlerle aynıdır.

4.3.3. Kurum bilgilerine ve bilişim sistemlerine (işletim sistemleri, uygulamalar, veritabanları, ağ donanımları ve diğerleri) erişim hakkı "en düşük erişim hakkı" ve "bilmesi gereken" ilkelerine bağlı kalınarak verilir. Her bir uygulama veya sistemin yetkisiz erişim, değişiklik, gizliliğinin ihlali veya zarar görmeye karşı korunması için uygun seviyede erişim denetimi içeren prosedürler uygulanır. Bu şekilde, bilginin doğru, gizli ve erişilebilir olması sağlanır. İşletim sistemi, iş uygulamaları, veritabanları ve ağ donanımları gibi her tip bilişim sistemine erişim yetkileri tanımlanır ve belgelendirilir.

4.3.4. Erişim yetkileri, kişilerin iş tanımlarına ve görevlerine göre ve gerekli onayların ardından verilir. Kişinin iş tanımının gerektirdiği erişim yetkilerinin dışındaki ek erişimler için ilgili birim amirinin ve Bilgi İşlem Daire Başkanının onayı alınır.

4.3.5. Bilişim sistemlerine ve hizmetlerine erişimlerin kaldırılmasına yönelik otomatik veya zamanında bildirmeyi de sağlayacak resmi bir erişim silme süreci izlenir.

4.3.6. İki durum için bir kullanıcıya erişim hakkı tanımlanır. Birinci durum, kullanıcı hesabının oluşturulmasıdır. Diğeri ise bir kullanıcının, görev değişikliği ya da sorumluluklarının değişmesinden ötürü ek erişim hakları talep etmesidir. Özel bir nedenden ötürü yüksek erişim yetkisine sahip kullanıcılar, normal işleri için ayrı bir kullanıcı hesabı kullanır (örn. bir uygulama çalıştırmak için sorumlu personel kendi kullanıcı hesabı ile sisteme giriş yaptıktan sonra bu hesabı

üzerinden "sistem yöneticisi- System Administrator" kullanıcı hesabına geçiş yapar).

4.3.7. Yeni bir kullanıcı yaratıldığında, erişim hakları, onay ve yetkinin alınmasının ardından talebe göre verilir.

4.3.8. Bir kullanıcının ek erişim haklarına ihtiyaç duyması durumunda, bu kişi ilgili Bölüm ya da Birim Yöneticisinin onayı alındıktan sonra Bilgi İşlem yöneticisine talepte bulunur ve eğer Bilgi İşlem Daire Başkanı tarafından uygun görülürse ek erişim yetkisi kullanıcıya tanımlanır.

4.3.9. Kullanıcılara erişim hakkı verilmeden önce, erişim hakkı talebinin, bölüm ya da birim yöneticisi tarafından onaylanması gerekir. Bölüm yöneticisi bu kişinin, verilecek ek erişim hakkına sorumluluklarını yerine getirmek için gereksinim duyduğunu denetler ve talep edilen erişim yetkisinin, o kişinin görevlerini yapabilmesi için minimum yeterliliğe sahip olup olmadığı inceledikten sonra talebi onaylar.

4.3.10. Sistem/Ağ/Uygulama Yöneticileri herhangi bir olumsuz durum ortaya çıkmayacağını ön görmeleri halinde ve gerekli onayların alındığını denetleyerek sistem, ağ ve uygulamalarda talep edilen erişim haklarını Bilgi İşlem Daire Başkanın onayına istinaden tanımlar. Kurum bünyesinde çalışan personelin görev tanımlarına istinaden, erişim sağlanan sistemlerde roller ve yetkiler tanımlıdır.

4.3.11. İşe yeni başlayan personelin seçme ve yerleştirme süreci Personel Daire Başkanlığı sürecinde tamamlandıktan sonra, Personel Daire Başkanlığı bölümünden gelen talebe istinaden sistem yöneticisini bilgilendirir.

4.3.12. Bir çalışanın iş tanımının gerektirdiği sistemler dışında bir sisteme erişimi gerektiğinde, bu çalışanın yöneticisi ya da kendisi, yöneticisini de bilgilendirerek, sistem yöneticisi yolu ile erişim talebinde bulunur. İlgili sistem yöneticisi iş uygulamaları arayüzleri üzerinden çalışanın iş tanımına uygun önceden belirlenmiş ya da çalışanın yöneticisi tarafından talep edilen sistemlere erişimini tanımlar.

4.3.13. Kullanıcılara verilecek bilgisayarlara kişinin rol ve sorumluluklarına göre opsiyonel izinli uygulamalar kurulur.

4.3.14. Üçüncü tarafların kurum bilgi sistemlerine erişmesi gerektiği durumlarda, üçüncü taraf ile koordinasyonu sistem yöneticisi sağlar.

4.3.15. Sözleşmeli çalışanlar ve danışmanlar için kullanıcı hesapları projenin bitiş tarihine kadar geçerli olacak şekilde yaratılır. Bu tarih sonrasında da bu kullanıcı hesabına ihtiyaç duyulması halinde, proje yöneticisinin onayıyla kullanıcı hesabı aktif hale getirilir.

4.3.16. Üçüncü taraflar için kullanıcı hesabı yaratılmasında Sistem Yöneticisinin ve Proje Yöneticisinin onayı gereklidir.

4.3.17. İşletim sisteminde açılacak yeni kullanıcı hesaplarını Bilgi İşlem Daire Başkanı, uygulamalarda açılacak yeni kullanıcı hesapları ilgili bölüm ya da birim yöneticisi ve veritabanında açılacak yeni kullanıcı hesaplarını Bilgi İşlem Daire Başkanı onaylar.

4.3.18. Ağ donanımları veya ağ hizmetlerine erişim talebinde bulunan yeni kullanıcılar sistem yöneticisinden erişim talebi ister.

4.3.19. Ortak kullanıcı hesaplarına erişim hakkı, bireysel hesapların yaratılmasının teknik olarak elverişli olduğu durumlarda, birden fazla kişiye verilemez.

4.3.20. Ortak bir kullanıcı hesabının kullanımını gerektiren durumlarda, bu erişimin verildiği kullanıcıların ve erişim gereksiniminin detayları sunularak, Bilgi İşlem yöneticisinden ve Bölüm Yöneticisinden özel izin ve onay alınır.

4.3.21. Ortak kullanıcı hesabı kullanımı, kayıt altına alınır. Bilgi İşlem Yöneticisi ayda bir defa erişim denetim izlerini (günlükler) gözden geçirir. Yapılan incelemede ortak kullanıcı hesaplarına hangi terminallerden girildiği ve bu terminallerin sahibi olan çalışanlar değerlendirilir. Eğer ortak kullanıcı hesabı, bu hesaba ulaşmasına onay verilmeyen bir çalışan tarafından kullanılıyorsa, önce şifresi değiştirilir. Daha sonra bu durum ilgili birimin Yöneticisine bildirilir.

4.3.22. Sistem yöneticisi, kullanıcıların aynı anda, birden fazla terminalden sisteme giriş yapamaması için gerekli parametreleri uygun şekilde ayarlar.

4.3.23. Bilgi İşlem Yöneticisi erişim yetkilerini kendi bölümü için yılda en az iki defa gözden geçirir ve bunları Bilgi İşlem Daire Başkanına rapor olarak sunar.

4.3.24. Bilgi İşlem Yöneticisi çeşitli bilişim sistemlerindeki kullanıcıları, erişim yetkileriyle birlikte her sene gözden geçirir.

4.3.25. Bilgi İşlem Yöneticisi, bilişim sistemlerindeki kullanıcıların erişim yetkilerinin onaylarını ve belgelendirilen ile uygulamadaki yetkilerin aynı olduklarını denetler.

4.3.26. Bilgi İşlem Yöneticisi, geçerlilik tarihinden sonra erişim yetkilerinin kaldırıldığını denetler. Bilgi İşlem Yöneticisi, ayrıca onay olmadan erişim hakkı verilip verilmediğini denetler.

4.3.27. Bölüm yöneticileri, altı ayda bir uygulamalarda tanımlı kullanıcı yetkilerini gözden geçirir ve 60 günden fazla süredir aktif olmayan hesapların listesinin çıkarılmasını sağlar ve bunu rapor olarak Bilgi İşlem Yöneticisine sunar.

4.3.28. Eğer bir kullanıcı 60 günden fazla bir süre için ayrılacaksa, Personel Daire Başkanlığı veya bölüm sorumlusu Bilgi İşlem Yöneticisine bunu bildirir. Bilgi İşlem Yöneticisi ise bu bilgi üzerine kullanıcı hesabının bu süre zarfında sistemlerin kullanılması söz konusu değil ise bu süre için kapatılmasını sağlar.

4.3.29. Personel Daire Başkanlığı birimi aynı zamanda kuruluş ile ilişkisini kesen kullanıcıların listesini, erişim haklarının silinebilmesi için Bilgi İşlem Yöneticisine sunar.

4.3.30. Gözden geçirme sırasında ya da ilk defa yeni bir yazılım yükleneceği zaman, Bilgi İşlem Yöneticisi, kurulumla gelen tüm kullanıcı hesaplarının kaldırılmasını veya bu hesaplara tanınmayacak hesap isimleri verilmesini veya şifrelerinin karmaşık olacak şekilde değiştirilmesini sağlar.

4.3.31. Personel Daire Başkanlığı birimi veya işten ayrılan/transfer edilen çalışanın bölüm yöneticisi bu çalışan hakkında Bilgi İşlem Yöneticisini derhal bilgilendirir. Bilgi İşlem Yöneticisi, ilgili çalışanın kullanıcı hesaplarının kaldırılmasını veya erişim haklarının geri alınmasını onaylar ve bu talebi ilgili kimlik yöneticisine bildirir.

4.3.32. Kimlik yöneticileri, çalışanların işten ayrılmaları üzerine kimlik yönetim sistemi üzerinde kullanıcı hesabının pasif hale getirilmesini veya sorumluluklarının değişmesi durumunda erişim yetkilerinin uygun şekilde değiştirilmesini sağlar.

4.3.33. Bilgi İşlem Yöneticisi kullanıcı listelerini, kullanıcı hesaplarının işten ayrılma tarihinde kapatıldığına veya erişim yetkilerinin güncellendiğine dair gözden geçirir.

4.3.34. Ortak bir kullanıcı hesabının kullanılması ya da işten ayrılan çalışanın kullanıcı hesabının denetim amacıyla açık tutulması gerektiğinde veya uygulamanın kullanıcı hesabının kaldırılmasına imkan vermediği durumlarda, bu hesapların şifreleri, çalışanın son iş gününde değiştirilir.

4.3.35. Bölüm yöneticisi, işten ayrılan personelin tüm sorumlulukların başka bir çalışana aktarılmasını sağlar. Bölüm yöneticisi ayrıca işten ayrılan çalışanın, işten ayrılmak için başvurduğu andan itibaren faaliyetlerini yakın takipte izler.

4.3.36. Personel Daire Başkanlığı birimi, işten ayrılan çalışanın, üzerindeki bilgisayar, anahtar, kimlik kartı, geçiş kartı, yazılım, veri, belge, kılavuz gibi tüm donanımları kurum ilgili birim yöneticisine teslim edilmesini sağlar.

4.3.37. Çalışanın işten ayrılması sonrasında tesis dışına çıkarmak istediği tüm malzemeleri güvenlik personeli incelemeye alır ve Güvenlik personeli kurumla ilişiği kesilmesi esnasındaki tüm süreçte çalışana refakat eder.

4.3.38. Tüm kullanıcı faaliyetlerinin, işletim sistemi, uygulama, veritabanı ve ağ bileşenleri seviyesinde denetim izi tutulur. Eğer denetim izi alınması sistem performansını düşürüyorsa, sistem/ağ/uygulama yöneticileri, Bilgi İşlem yöneticisi ile beraber denetim izi tutulması gereken kritik komutlar veya faaliyetleri belirler veyahut ta performansı artırmak için gerekli ilave yatırım planı hazırlarlar. Bilgi İşlem Yöneticisi seçilen denetim izi kriterlerini onaylar.

4.3.39. Sistem, ağ ve uygulama yöneticileri, sistemler üzerinde raporlanması gereken kritik işlemleri ve bunlarla ilgili tanımlanması gereken alarmları) belirleyerek, bunları Bilgi İşlem yöneticisine onaylatır.

4.3.40. Sistem ve ağ yöneticileri, sistemden gelen alarmları inceler ve gerekli durumlarda vaka/olay kaydı açar.

4.3.41. Kullanıcıların kaydı onaylı bir şekilde MERNİS ve SMS doğrulama ile oluşturulmaktadır. Kayıt silme işlemleri Bilgi İşlem Daire Başkanlığı personeli tarafından yapılmaktadır.

4.3.42. MERNİS ve SMS doğrulama işlemlerinde hata yaptığı zamanlarda kullanıcılar taleplerini Bilgi İşlem Yöneticisine iletir onaylanır veya reddedilir.

4.3.43. İşletim sistemi, veri tabanı yönetim sistemi ve her uygulamada ayrıcalıklı erişim hakkı Bilgi İşlem Daire Başkanındadır.

4.3.44. Personeller Gizlilik Sözleşmesini imzalayarak gizli kimlik bilgilerini paylaşmayacaklarını taahhüt ederler.

4.3.45. Kullanıcıların gizli kimlik bilgilerini korumak için kullanıcılara ilk kullanımda değiştirmek zorunda olacakları geçici bir şifre temin edilecektir.

4.3.46. İç tetkiklerde GEM'e göre ve çalışanları terfi, rütbe değişikliği ve iş feshi gibi durumlara göre erişim haklarının gözden geçirilmesi yapılır. İç tetkik raporları tutulup periyodik gözden geçirilen kayıtlar belgelenir.

4.3.47. Erişim haklarının düzenlenmesi talebi e-posta yoluyla Bilgi İşlem Yöneticisine iletilir. Bilgi İşlem Daire Başkanı tarafından talep onaylanır veya reddedilir.

4.3.48. Kurumdan ayrılacak kişi İlişik Kesme Formu doldurularak ilgili birimlere herhangi bir yetkisinin ve erişim hakkının kalmadığı, ilişkinin kesildiğini beyan eder.

4.3.49. Kullanıcılar oturum açma başarıyla tamamlanana kadar, sistem ve uygulama tanımlayıcılarını görüntülememekle yükümlüdür.

4.3.50. Kullanıcılar, bilgisayara sadece yetkili kullanıcıların erişim sağlaması gerektiğini belirten genel bir uyarı mesajı görüntülemekle yükümlüdür.

4.3.51. Kullanıcılar oturum açma sırasında yetkisiz kullanıcılara yardım edebilecek hiçbir yardım mesajı sağlanmaması hususunda sorumludur.

4.3.52. Oturum açma bilgisini, sadece tüm girdi verilerinin tamamlanması üzerine geçerli kılınacak şekilde ayarlanacaktır. Eğer bir hata durumu ortaya çıkarsa, sistem verinin hangi kısmının doğru ve yanlış olduğunu belirtmeyecek şekilde düzenlenecektir.

4.3.53. Kullanıcıların sistem ve uygulama girişleri, kaba kuvvet oturum açma girişimlerine karşı korumalı olacaktır.

4.3.54. Sistem ve uygulamalara kullanıcıların girişlerinde başarılı ve başarısız girişimlerin kayıtları tutulacaktır.

4.3.55. Potansiyel girişimler ya da oturum açma denetimlerinin başarılı ihlali tespit edilirse bir güvenlik olayı başlatılacaktır.

4.3.56. Başarılı bir oturum açma işleminin tamamlanmasının ardından önceki başarılı oturum açmanın tarihi ve zamanı, en son başarılı oturum açmadan bu yana her başarısız oturum açma denemesinin detayları görüntülenecektir.

4.3.57. Girilen parolanın görüntülenmemesine dikkat edilecektir.

4.3.58. Bir ağ üzerinden parolalar açık metin olarak iletilmeyecektir.

4.3.59. Tanımlanan bir hareketsizlik süresi sonrasında aktif olmayan oturumlar sonlandırılacaktır (özellikle halka açık alanlar ya da kuruluş güvenlik yönetimi dışındaki dış alanlarda ya da mobil cihazlar gibi yüksek riskli yerlerde).

4.3.60. Yüksek riskli uygulamalar için ek güvenliği sağlamak ve yetkisiz erişim fırsatlarını azaltmak amacıyla bağlantı süreleri kısaltılacaktır.

4.3.61. Gizli kimlik bilgisi kâğıt yazılım dosyası ya da el cihazı gibi ortamlarda tutulması kaçınılacaktır. Herhangi bir ifşa durumunda doğrulama bilgileri değiştirilecektir.

4.3.62. Gizli kimlik bilgisiyle alakalı parola özellikleri hatırlanması kolay, kolayca tahmin edilemeyecek, kişiyle ilgili bilgiler kullanılmadan (isimler, telefon numaraları), ardışık, tümü sayısal ya da tümü alfabetik olmayan, geçici ise ilk oturum açmada değiştirilecek şekilde olacaktır.

4.4. Hizmet Alımlarında Sistem ve Uygulama Erişim Denetimi

4.4.1. İşletim sistemlerine erişim güvenli bir sistem giriş prosedürü ile denetlenir. Çeşitli sistemlere erişilmesi için gerekli kullanıcı bilgileri bir kullanıcı kimliğinden (ID) ve şifresinden veya kullanıcıya özel diğer bilgilerden (dijital sertifikalar, belirteç (token) vb.) oluşturulur.

4.4.2. Kullanıcıların aynı işlem ortamında birden fazla kullanıcı hesabı olmaz. Zorunlu bir durum değilse, ortak kullanıcı kimlikleri kullanılamaz.

4.4.3. Ortak kullanıcının gerekli olduğu durumlarda, erişim sağlanmadan önce ilgili yöneticilerden onay alınır. Ayrıca, kullanıcı kimlikleri kullanıcılar arasında hiçbir koşulda paylaşılmaz.

4.4.4. İşletim sistemi seviyesinde şifre gereksinimlerine bağlı kalınması için gerekli kısıtlamalar oluşturulur. Uygulanabilir yerlerde, sistemin üzerine yazma işlemi gerçekleştirebilecek sistem yardımcı programlarına ve uygulama denetimlerine erişim, kullanıcıların iş tanımlarını gerçekleştirebilmek için gerekli olandan daha fazla bilgi elde edemediklerinin denetimi yapılır.

4.4.5. Sistem programlarına erişim, son kullanıcıların problemlerini çözmeye yardımcı olmaları için yalnızca yönetici görevindeki (administrator) kullanıcılarla sınırlı tutulur.

4.4.6. İşletim sistemleri, uygulamalar, veritabanları ve terminaller veya sunucular inaktif kaldıkları durumlarda belirli bir süre sonra zaman aşımına uğrar ve/veya ekran koruyucusu otomatik olarak devreye girer.

4.4.7. Eğer yeni bir sistem veya uygulama canlıya alınacaksa, canlıya geçilmeden önce, Bilgi İşlem Daire Başkanı, gerek duyulduğunda sistem yöneticisinin uygun güvenlik eğitimlerini almasını sağlar.

4.4.8. Güvenlik yönetimi fonksiyonları tesis edilmeden sistemlere erişim hakkı verilemez.

4.4.9. Sistem, iş istasyonları ve üretim sistemlerine yüklenen işletim sistemleri için uygun lisanslar edinilir. İşletim sisteminin yüklenmesinden sonra, kullanıma geçilmeden önce, canlı sunucularında işletim sisteminin tam yedeği alınır.

4.4.10. Yapılan her değişiklik için uygun sürümün yedeği bulunmalıdır. İşletim sistemi komutlarına doğrudan ya da hassas programlar üzerinden erişim, iş tanımlarından dolayı bu erişime sahip olması gereken kullanıcılarla kısıtlanır.

4.4.11. Her sistem yöneticisi, kendi sorumluluğundaki veri dosyalarının ve temel programların bir kaydını tutmakla yükümlüdür. Sistem yöneticisi bu dosyalara erişimi ve bu dosyalardaki değişiklikleri takip eder.

4.4.12. Düzenli olarak işletim sistemi güncellenir, örneğin yeni çıkan bir sürümü ya da yamayı yüklemek için güncelleme yapılır. Değişiklikler meydana geldiğinde, operasyon veya güvenlik üzerinde zararlı bir etki oluşmaması için uygulama sistemleri gözden geçirilir ve test edilir. Değişiklikler, değişiklik yönetimi sürecine göre Bilgi İşlem Daire Başkanının onayıyla hayata geçirilir.

4.4.13. İşletim sistemi değişikliklerinin uygulama denetimlerine ve bütünlük prosedürlerine zarar vermediğini Bilgi İşlem Yöneticisi denetler.

4.4.14. İlgili sistem yöneticileri, uygulamaya geçilmeden önce uygun gözden geçirmelere imkân vermek için, Bilgi İşlem yöneticisini işletim sistemi değişikliklerinden zamanında haberdar eder.

4.4.15. Bilgi İşlem Daire Başkanı tüm güvenlik ve sistem denetim araçlarının ana sahibidir. Bu araçlar sadece Bilgi İşlem Daire Başkanı veya Bilgi İşlem Daire Başkanı tarafından atanmış Bilgi İşlem Yöneticisi veya Bilgi İşlem Yöneticisi tarafından atanmış kimseler tarafından kullanılır. Bu yazılımlara erişim, bu belgede açıklanan erişim denetimi prosedürlerine göre verilir.

4.4.16. Kullanıcıların ve destek personelinin bilgi ve uygulama sistem fonksiyonlarına erişimi, erişim denetimi politika ve prosedürlerine göre kısıtlanır.

4.4.17. Bilgi İşlem Yöneticisi veya onun bu görevi atayacağı kişi yılda en az bir defa uygulama güvenliğinin sağlanıp sağlanmadığını denetler.

4.4.18. Uygulamalar ve hassas sistemler varlık envanterinde belirlenmiştir ve gerekli görülen kritik uygulamalar normal bilgi işlem ortamlarından ayrılmıştır.

4.4.19. Paylaşım ortamında hassas bir uygulama çalıştırılacağı zaman, uygulamanın sahibi ve Bilgi İşlem Yöneticisi ilgili uygulamanın kaynak paylaşımında bulunduğu uygulama sistemlerini belirler.

4.5. Parola Yönetim Sistemi

4.5.1. Tüm kullanıcı şifreleri (kullanıcı şifreleri ya da yönetici – "administrator"-şifreleri) gizli tutulur, kesinlikle paylaşılmaz, e-posta yoluyla bir başkasına iletilmez ya da herhangi bir şekilde deşifre edilemez.

4.5.2. Kullanıcı oluşturma süreci esnasında kullanıcıya güvenli yollardan bir ilk şifre sunulacaktır. Ayrıca sistem, kullanıcının ilk girişinde kullanıcıyı hemen şifresini değiştirmeye zorlayacak şekilde yapılandırılacaktır.

4.5.3. Kritik bilişim sistemleri için yönetici (administrator) şifrelerinin saklanması ve yönetilmesine yönelik uygun prosedürler uygulanacaktır.

4.5.4. Sistem kısıtları ya da iş gereksinimlerinden ötürü herhangi bir şifre ya da kullanıcı hesap politikası uygulanamıyorsa, bu duruma özel onay mekanizmaları ve bu durumdan kaynaklanacak riskin azaltılması için özel denetimler oluşturulacaktır.

4.5.5. Kişiye özel kullanıcı kimliği ve şifresinin oluşturulamadığı uygulamalar için, erişim yetkilerinin kısıtlanması ve denetlenmesi için alternatif çözümler uygulanacaktır.

4.5.6. Hesap verilebilirliği arttırmak için bireysel kullanıcı kimliklerinin ve parolalarının kullanımı zorunlu tutulacaktır.

4.5.7. Uygun olan yerlerde, kullanıcılara kendi parolalarını seçme ve değiştirme hakkının tanınması ve girdi hataları için teyit prosedürü içermesi sağlanacaktır.

4.5.8. Kullanıcılar, nitelikli parola seçimine ve kendi parolalarını ilk oturum açmada değiştirmeye zorlanacaktır.

4.5.9. Sistem ya da uygulamalara giriş yapılırken kullanıcı parolaları ekranda görüntülenmeyecek şekilde ayarlanacaktır.

4.5.10. Kullanıcı parola bilgileri, uygulama ya da sistem verilerinden ayrı bir yerde saklanacaktır.

4.5.11. Bölüm yöneticisinin veya Bilgi İşlem Daire Başkanının özel onayı olmadığı müddetçe okunabilir gizli ve çok gizli bilgi e-posta yoluyla gönderilmeyecektir.

4.5.12. Gizli veya çok gizli bilgi, ancak Kurumun uyguladığı şifreleme yöntemlerinden biriyle şifrelendiğinde ve şifreleme gönderen tarafta yapılıp yalnızca alınan tarafta çözülebildiği durumda elektronik posta sistemi üzerinden gönderilebilecektir.

4.5.13. Hassas kurum bilgisini içeren tüm taşınabilir cihazları, dizüstü bilgisayarları ve diğer taşınabilir bilgisayarları kullanan Kurum personeli, eğer cihazlardaki hassas bilgiler şifrelenmemişse, bu cihazları hiçbir koşulda gözetimsiz bırakmayacaktır.

4.5.14. Bilgi İşlem Daire Başkanlığı, kimlik doğrulama bilgilerinin elektronik herhangi bir ortamda saklanması veya ağ üzerinden iletilmesi durumlarında şifrelenmesini sağlayacaktır. Bu şekilde, yetkisiz tarafların bu şifreleri ele geçirmeleri durumunda şifreleri kullanamamaları sağlanacaktır.

4.5.15. Eğer şifreler veya Kişisel Kimlik Numaraları (Personal Identification Numbers - PIN) bir bilgisayar sistemi tarafından üretiliyorsa, formül, algoritma ve sürece ait diğer bilgileri içeren tüm yazılım ve dosyalar ilgili bilgisayar sisteminin desteklediği en sıkı güvenlik önlemleri ile kontrol edilecektir.

4.5.16. Şifreleme ihtiyaçlarının, yönteminin, gerekli iş alanlarının ve kullanımının belirlenmesi için risk değerlendirmeleri gerçekleştirilir.

4.5.17. Çok gizli ve gizli bilgilerin güvenliğinin sağlanması için uygun şifreleme kontrollerinin kullanılması sağlanır.

4.5.18. Çok gizli ve gizli bilginin tanımı, ilgili bilginin sahibinin bilgi sınıflandırma sürecine göre vereceği karara bağlıdır(Varlık Envanteri).

4.5.19. Aktif olarak kullanılmayan gizli bilginin, elektronik saklama ortamlarında (sunucular, manyetik teypler, CD veya taşınabilir bellekler gibi) muhafaza edildiğinde ya da taşındığında, mümkün olan her durumda şifrelenmesi esastır.

4.5.20. Statik ya da yeniden kullanılabilir kimlik doğrulama bilgisi, saklanması ya da ağ üzerinden iletilmesi gerektiğinde şifreleme yazılımı ya da donanımı kullanılarak şifrelenmesi tercih edilecektir.

4.5.21. İşletim Sistemi, uygulama, veri tabanı ve ağ donanımlarının şifre parametreleri asgari şekilde yapılandırılacaktır.

4.5.22. Minimum şifre uzunluğu: 8 karakter olacaktır.

4.5.23. Şifre bileşimi: alfa, nümerik, büyük ve küçük harfler ve en az bir özel karakter (bunlardan en az üçü sağlanacak şekilde) olacaktır.

4.5.24. Maksimum şifre ömrü: 180 gün olacaktır.

4.5.25. İzin verilen hatalı giriş sayısı: 3 kez olacaktır.

4.5.26. Aşağıdaki tablo hangi tip şifrelerin kritik şifre olduğunu göstermektedir. Bu şifreler, kaybolma ve unutulma riskine karşı dikkatli bir şekilde muhafaza edilecektir. Kritik şifreler kriptolanarak Bilgi İşlem Daire Başkanı ve sistem üst yetkilileri tarafından saklanacaktır.

İşletim Sistemi	Yönetici (Administrator) Şifresi/Şifreleri
Bilgi İşlem Sistemi / İş Uygulaması	Super User Şifresi (mevcut olduğu durumlarda) Yönetici (Administrator) Şifresi/Şifreleri Sistem Şifresi (Veritabanı bağlantısı için) mevcut olduğu durumda
Veritabanı	Veritabanı Super User Şifresi Veritabanı Yönetici (Administrator) Şifresi

	Veritabanı Security Officer Şifresi

4.5.27. Şifreleme algoritmasının tipi ve seviyesi, üzerinde çalışılan kurum bilgisinin kritikliğine göre tayin edilecektir.

4.5.28. Şifreleme anahtarları ağ üzerinden iletilmeyecektir. Şifreleme sürecinin yönetilmesi için kullanılan anahtarların ağ üzerinden iletilmesi gerekiyorsa, iletim güvenli haberleşme kanalları üzerinden gerçekleştirilecektir.

4.5.29. Sistemler üzerinde şifreli olarak bulunan verilerin şifreleme anahtarları güvenli alanlarda muhafaza edilecek ve şifreleme yapan personel haricinde bir personel ya da yöneticinin gereken durumlarda anahtara erişimi sağlanacaktır.

4.5.30. Yetkisiz girişleri engellemek için tüm elektronik ticaret sunucuları (ağ, veritabanı, ödeme, güvenlik sunucuları vs.) özgün dijital sertifika kullanılacak ve bilginin bu sunuculara ya da bu sunuculardan iletimi için şifreleme kullanılacaktır. Ağ sunucuları, FTP sunucuları ve paydaşlar, olası paydaşlar veya diğer kamu üyeleriyle iletişimi destekleyen herhangi bir Kamu sunucusu için bu yönteme başvurulmayabilir.

4.5.31. Kullanıcı şifre veya şifreleme anahtarını ilk kez tanımladığında, bu bilgiler iki kere girilir ve yazılan bilgilerin başkaları tarafından görülmemesi için gizlenir. Girilen bu bilgilerin ikisi de sistem tarafından kabul edilmesi için aynı olmalıdır. Bu kontrol yanlış yazımdan (tuşlama) kaynaklanacak kullanıcı kilitlenmelerine ya da sistemlere erişememeye karşı önlem alır.

4.5.32. Kurumumuzda AES şifreleme kullanılmaktadır. AES (Advanced Encryption Standard) Gelişmiş Şifreleme Standardı, elektronik verilerin şifrelemesinde kullanılan, modern bir şifreleme standardıdır. Modern kriptoloji simetrik ve asimetrik şifreleme yöntemleri olmak üzere ikiye ayrılır. Asimetrik şifrelemede açık mesaj (plain text), herkesçe bilinen bir anahtar (key) ile şifrelenir ve karşı tarafın şifreyi çözmek için gizli anahtarı kullanır. Simetrik yöntemde ise şifrelemede de (encrytion) şifre çözmede de (decryption) aynı ve tek bir anahtar kullanılır. AES, simetrik bir blok şifreleme standardıdır.

4.5.33. Tüm simetrik şifreleme anahtarları endüstriyel standartlara göre rastgele seçilir.

4.5.34. Asgari bir standart olarak 128 bit şifreleme kullanılır.

4.5.35. Şifreleme anahtarları kurum tarafından geliştirilmiş olan projelerin ilgili sabit değerler sınıflarında saklanmaktadır.

4.5.36. Şifreleme anahtarları, kullanımdan kaldırıldıklarında veya zarara uğratıldıklarında ve bir anahtar saklama programının bir parçası olmadıkları durumda silinir ya da imha edilir.

4.5.37. Şifreleme anahtarları gizli bilgidir ve bu anahtarlara erişim iş tanımı nedeniyle bu gereksinimde olan kişilerle sınırlandırılır. Şifrelemeyle korunan verinin sahipleri bu veriyi korumak için kullanılan şifreleme anahtar yönetimine dair sorumluluğunu imzalar. Şifreleme anahtarları haberleşme hatları üzerinden aktarılacaksa, şifrelenerek yollanır. Anahtarlar, iletilecek anahtarların şifreleme için kullanıldığı gizli bilginin şifrelenmesinde kullanılan algoritmadan daha güçlü bir algoritmayla şifrelenir.

4.5.38. Zarar gören şifreleme anahtarları derhal Bilgi İşlem Daire Başkanlığına ve korunan verinin bilgi sahibine raporlanacaktır. Ayrıca, anahtar değiştirilecek

ve/veya imha edilecek ve yeni bir anahtar üretilecektir. Yeni anahtar oluşturulur oluşturulmaz, zarar gören anahtarla şifrelenen veri yeni anahtar ile yeniden şifrelenecektir.

4.6. Ayrıcalıklı Destek Programlarının Kullanımı

4.6.1. Sistem ve ağ yöneticileri, uygulama yöneticileri ve kimlik yöneticileri, Bilgi İşlem Yöneticisi ve bölüm yöneticilerinin yardımıyla her bir iş birimi için işletim sistemi, uygulama, veritabanı ve ağ elemanları üzerinde tanımlı tüm erişim haklarını belirleyecektir.

4.6.2. GEM'in oluşturulması ve belgelendirilmesi için, 4.6.1 de belirtilen erişim hakları göz önünde bulundurularak kurumun personel iş tanımlarıyla (rol ve sorumlulukları) eşleştirilecektir. İş sorumluluğu için gereken çoğu uygulama, işletim sistemi ve veritabanı erişim hakları belirlenerek, erişim haklarının etkin ve güvenli yönetimi için bir uygulama rolüne atanacaktır. Mümkün olduğu durumda, birim içerisindeki ilgili her bir iş tanımı için ayrı bir uygulama rolü oluşturulacaktır.

4.6.3. Bilgi İşlem Daire Başkanı, bu rollerin ve bunlara sağlanacak yetkilerin yönetimi için oluşturulan GEM'i gözden geçirir, inceler ve herhangi bir olumsuz durum oluşturmadığında gerekli onayı verir. Bu işlem, bir uygulama, işletim sistemi, veritabanı veya ağ donanımının ilk kullanımında gerçekleştirilecektir.

4.6.4. Bilgi İşlem Daire Başkanı, bir uygulama, İşletim Sistemi, Veritabanı veya ağ donanımında önemli bir değişiklik gerçekleştiğinde veya yeni bir modül veya fonksiyon eklendiğinde, yeni bir iş tanımı veya rol oluşturulduğunda, iş tanımında veya rolde değişiklik yapıldığında, söz konusu durumu sistem yöneticileri / uygulama yöneticileri / ağ yöneticileri ile istişare ederek GEM'i değiştirecektir.

4.6.5. Bilgi İşlem Daire Başkanı, Bilgi İşlem Yöneticisinin ya da GEM'in görevler ayrılığı ilkesini ihlal etmediğini denetleyecek ve görev ayrılıklarının yılda bir gözden geçirilmesini sağlayacaktır.

4.6.6. İlgili Birim yöneticisi GEM'in eksiksiz ve gereksinimlere uygun olduğunu denetleyecektir.

4.7. Program Kaynak Kodu ve Veri tabanı erişimi

4.7.1. Mümkün olduğu sürece, program kaynak kütüphanesi işletimdeki sistemler içinde tutulmamalıdır.

4.7.2. Program kaynak kodu ve program kaynak kütüphanesi oluşturulmuş prosedürler ile yönetilmelidir.

4.7.3. Destek personeli, program kaynak kütüphanesine sınırsız erişim yetkisine sahip olmamalıdır.

4.7.4. Programcılar, program kaynak kütüphanesinin ve ilişkili öğelerin güncellenmesi ve program kaynaklarının yayınlanmasını sadece uygun yetki alındıktan sonra yapmalıdır.

4.7.5. Program listeleri güvenli bir ortamda saklanmalıdır.

4.7.6. Program kaynak kütüphanelerine yapılan tüm erişimlerin denetim günlüğü tutulmalıdır.

4.7.7. Program kaynak kütüphanelerinin sürdürülmesi ve kopyalanması sıkı değişim denetim prosedürlerine tabi olmalıdır.

4.8. E-Posta Kullanımı ve Erişimi

4.8.1. Kurumun e-posta sistemi, taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz. Bu tür özelliklere sahip bir mesaj alındığında hemen Bilgi İşlem Daire Başkanlığına haber verilecektir.

4.8.2. E-posta kullanıcıları mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterecektir.

4.8.3. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında kesinlikle başkalarına iletilmeyecek ve Bilgi İşlem Daire Başkanlığına bilgi verilecektir.

4.8.4. Kişisel kullanım için internet sitelerine üye olunması durumunda kurum e-posta adresleri kullanılmayacaktır.

4.8.5. Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmayacaktır ve konuyla ilgili Bilgi İşlem Daire Başkanlığına bilgi verilecektir.

4.8.6. Kullanıcıların kullanıcı kodu / şifresini girmesini isteyen e-postaların sahte eposta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinecek ve konuyla ilgili Bilgi İşlem Daire Başkanlığına bilgi verilecektir.

4.8.7. Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, fikri mülkiyet içeren malzeme vb.) göndermeyeceklerdir.

4.8.8. Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemekle yükümlüdür. Bu yüzden e-posta erişimi için donanım /yazılım sistemleri yetkisiz erişimlere karşı korunacaktır.

4.8.9. Kurum çalışanları mesajlarını düzenli olarak denetlemek ve kurumsal mesajları cevaplandırmakla yükümlüdür.

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

4.8.11. E-posta adresine sahip kullanıcının herhangi bir sebepten (emekli olma, işten ayrılma gibi nedenlerle) kurumdaki değişikliğinin Personel Daire Başkanlığı tarafından Bilgi İşlem Daire Başkanlığı'na bildirilmesi gereklidir.

4.8.12. Kurumumuza ait alan adları üzerinden çalışanların ismi üzerine açılmış elektronik posta adresleri kişisel e-posta olarak kullanılmayacaktır.

4.8.13. Söz konusu elektronik posta adresleri kuruma ait işlerin ve faaliyetlerin gereği gibi, aksamadan, zamanında gerçekleştirilmesi adına kişilere tanımlanarak sadece zilyetliği teslim edilmiş olup mülkiyet hakkı her zaman alan adı sahibine aittir.

4.8.14. Kuruma ait alan adı üzerinden yapılan elektronik gönderilerin Kurum'u temsil ettiği göz önünde bulundurulacak ve amacı dışında kullanılmayacaktır.

4.8.15. Kurum, e-postaların kurum bünyesinde güvenli ve başarılı bir şekilde iletilmesi için gerekli yönetim ve altyapıyı sağlamakla yükümlüdür. Kurumda bu sürecin başarılı bir şekilde çalışmasından da Bilgi İşlem Daire Başkanlığı sorumludur.

4.8.16. Virüs, solucan, truva atı veya diğer zararlı kodlar bulaşmış olan bir e-posta kullanıcıya zarar verebilir. Bu tür virüslere bulaşmış e-postalar anti-virüs sistemleri tarafından analiz edilip temizlenecektir. Bilgi İşlem Daire Başkanlığı bu sistemden sorumludur.

4.9. Fiziksel Güvenlik

4.9.1. Kurumsal bilgi varlıklarının fiziksel olarak korunması, farklı koruma mekanizmaları ile donatılması temin edilecektir.

4.9.2. Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binada ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanacak ve erişim izinleri bu doğrultuda belirlenerek gerekli denetim altyapıları teşkil edilecektir.

4.9.3. Kurum dışı ziyaretçilerin ve yetkisiz personelin Kurumun güvenlik alanlarına girişi yetkili görevliler gözetiminde gerçekleştirilecektir.

4.9.4. Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin güncelliği sağlanacaktır.

4.9.5. Kritik sistemler erişim yetkisi ile belirlenmiş alanlarda bulundurulacaktır.

4.9.6. Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunacak, yangın ve benzer felaketlere karşı koruma altına alınacaktır.

4.9.7. Kuruma giriş yapacak ziyaretçi veya kurye teslimatları yetkili görevliler gözetiminde gerçekleştirilecektir.

4.9.8. Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve denetim altında tutulması temin edilecektir.

4.9.9. Fotoğraf, video, ses vb. kayıt cihazlarının yetki verilmeyen kişiler tarafından güvenli alanlara sokulması yasaklanacaktır.

4.10. Uzaktan Erişim

4.10.1. Uzaktan erişim ancak sınırlı olarak sağlanacak ve uzaktan erişime ilgili birim yöneticisinin onayı alındıktan sonra izin verilecektir.

4.10.2. Internet üzerinden kurumun herhangi bir yerindeki bilgisayar ağına erişen kişi veya kurumlar VPN teknolojisini kullanmaktadır. VPN teknolojisinde IpSec, SSL, PPTP, L2TP vb. protokollerden herhangi biri kullanılacaktır.

4.10.3. Uzaktan erişim güvenliği sıkı bir şekilde denetlenecektir.

4.10.4. Kurum çalışanları hiçbir şekilde kendilerinin oturum açma ve e-posta şifrelerini hiç kimseye vermemelidirler.

4.10.5. Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya diğer kişiler bağlantı esnasında aynı anda başka bir ağa bağlı olmadıklarını denetleyeceklerdir. Tamamıyla kullanıcının denetiminde olan ağlar için bu kural geçerli değildir.

4.10.6. Uzaktan erişim ile kuruma erişen bütün bilgisayarlar en son güncellenmiş antivirüs yazılımına sahip gerekmektedir.

4.10.7. Kurum ağına standart dışı erişim isteğinde bulunan kurumlar veya kişiler Bilgi İşlem Daire Başkanının özel izni ile geçici olarak erişim sağlanacaktır.

4.10.8. Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların kimlikleri ve hesapları kapatılacaktır.

4.10.9. Uzaktan erişim yetkisi e-posta yoluyla talep edilecektir.

5. Yaptırım Uygulamaları

5.1.1. Politika uygulama sürecin işletilmesinden BGYS Komisyonu ve KSÜ makamı sorumludur.

5.1.2. Fiziksel Çevre, Sistem Odası Kullanımı, Personel Görev Tanımları ve Yetkileri bu politikanın bir parçasıdır.

5.1.3. YS Temsilcisi politikanın sürdürülmesinden ve politikanın gerçekleştirilmesi konusunda tavsiyelerde bulunmaktan ve yol göstermekten doğrudan sorumludur.

5.1.4. Tüm personel, BGYS Politikasına bağlı kalmakla sorumludur.