|  |  |  |  |
| --- | --- | --- | --- |
| **SIRA NO** | **YÖNETİM SİSTEMLERİ STANDARDININ ŞARTLARI** | **İNCELENEN KAYITLAR VE DOKÜMANLAR** | **UYGUN (U) /** **UYGUN DEĞİL (UD)** |
| ***BÖLÜM/BİRİM: Tüm Birimler*** | |  | |
| ***TARİH: 01.07.2022*** | |  | |
| 1 | Görev tanımı olmayan çalışan var mı? |  |  |
| 2 | Disiplin prosedürü var mı? BGYS ile ilgili hususlar bulunmakta mıdır? |  |  |
| 3 | Personel disiplin prosedürü hakkında bilgi sahibi mi? |  |  |
| 4 | Bilgi güvenliği farkındalık eğitimi verilmiş/alınmış mı? |  |  |
| 5 | İşten ayrılan personel hakkında BGYS kapsamında gerekli süreçler işletilmiş mi? |  |  |
| 6 | İşten ayrılan personelin zimmetleri teslim alınmış mı? |  |  |
| 7 | BGYS kapsamında tanımlanmış dokümanlar (politika, prosedür, talimat vb.) personel tarafından biliniyor mu? Dokümanların yayın, revizyon tarihleri takip ediliyor mu? Doküman takip listesine mevcut mu? Revizyon olan dokümanlar hakkında personel bilgilendiriliyor mu? |  |  |
| 8 | Birimlerde gerçekleştirilen süreçler, yapılan değişiklikler ve karşılaşılan ihlal olayları için yeni riskler tanımlanmış mı? |  |  |
| 9 | BGYS farkındalık/oryantasyon eğtimini almamış personel var mı? |  |  |
| 10 | Politikalar tüm personellere deklare edilmiş mi? Yeni giren personellere beyan edilmiş mi? |  |  |
| 11 | Çalışanlar BG politikalarından bilgi sahibi mi? |  |  |
| 12 | Politikalara hangi kaynaktan erişeceklerini biliyorlar mı? |  |  |
| 13 | Birimlerin/şirketin varlık envanteri oluşturulmuş mu? |  |  |
| 14 | Çalışanlar bilgi varlıklarının etiketleme prosedürünü biliyor mu? Uygulanması gerekenlere etiketlemeler belirtilen şekilde yapılmış mı? |  |  |
| 15 | Varlıklar bilgi sınıfına göre tasniflenmiş ve uygun şekilde korunuyor mu? |  |  |
| 16 | Etrafta kontrolsüz kıymetli evrak bırakılmış mı? |  |  |
| 17 | Personelin program yükleme ve kaldırma yetkisi var mı?  Var ise Ayrıcalıklı Hakları Listesi/Yetki Tablosunda gösterilmiş mi? Bu listenin son gözden geçirme tarihi nedir? |  |  |
| 18 | Çalışanlar arasında şifre paylaşımı, şifrelerin bir yerlere yazılması gibi uygulamalar var mı? |  |  |
| 19 | Şifre/parola politikasından herkes biliyor mu? |  |  |
| 20 | Temiz masa temiz ekran politikası oluşturulmuş mu? Personel bu politikayı biliyor mu? Uyguluyor mu? |  |  |
| 21 | Çalışma ortamları için tanımlanmış güvenlikli alanları mevcut mu?  Ağ ve yedekleme cihazlarını nasıl korunuyor? Bilgi güvenliğinin sağlanmasına yönelik risk değerlendirmeleri yaptınız mı? |  |  |
| 22 | Genel bir bilgi güvenliği politikası mevcut mu? |  |  |
| 23 | Bilgi sistemlerinin güvenliği için teknik açıklık testleri yapılıyor mu? Teknik açıklık testleri sonuçları değerlendiriliyor mu? Çıkan teknik açıklıklar plan dahilinde kapatılıyor mu? |  |  |
| 24 | Onaylı Tedarikçi listesi oluşturulmuş mu? (özellikle BT için) Onaylı tedarikçi listesindeki firmalar ile gizlilik sözleşmesi/taahhütnamesi yapılmış mı? Onaylı tedarikçi listesindeki firmalar düzenli olarak hizmet alanına göre değerlendiriliyor mu? |  |  |
| 25 | Kurum yerleşkesine ve binalara fiziksel giriş çıkış kontrolleri yapılıyor mu? |  |  |
| 26 | Ziyaretçilerin giriş kayıtları tutuluyor mu? |  |  |
| 27 | Bina ve tesisler, yangın sel deprem gibi afetlere karşı fiziksel koruma önlemleri alınmış mı? Sistemlerde alınan yedekler felaket durumuna karşı ofis dışında tutuluyor mu? |  |  |
| 28 | Enerji kesintilerine karşı Jeneratör ve KGK gibi altyapı ile destekleniyor mu?  Kesintilere karşı testler yapılıyor mu? (KGK devreye alma gibi) Güç ve iletişim kablolarına müdahaleye karşı koruma yapılmış mı? Güç ve iletişim kabloları yedekli olarak mı alt yapı kurulmuş? Güç ve iletişim kablolarında karışıklık olmaması için etiketleme yapılmış mı? |  |  |
| 29 | Yedekleme Prosedürü/planı var mı? Yedekleme alınırken plana uygun mu hareket ediliyor? Alınan yedekler düzenli olarak test ediliyor mu? |  |  |
| 30 | İş Sürekliliğinin sağlanması için politika mevcut mu?  İş sürekliliği için kritik süreçler tanımlanmış mı?  İş sürekliliği için tatbikatlar yapılıyor mu?  İş sürekliliğinin sağlanması için yedek teçhizat bulunduruyor mu? |  |  |
| 31 | Hangi cihazın kimde olduğuna yönelik varlık envanter takibi yapılıyor mu? |  |  |
| 32 | Erişim ve kullanım yetki matrisi var mı? Güncel mi? |  |  |
| 33 | Bilgi işlem işletimi için yazılı prosedür/politika mevcut mu?  (Yedekleme, kullanımı hesap açma kapama, cihaz bakım vb.) Değişiklik yönetimi ile ilgili prosedürünüz var mı? |  |  |
| 34 | Virüs saldırılarına karşı sistemler nasıl korunuyor, personel bilgisayarlarında virüs programları yüklü ve güncel mi? Programı kaldırma/devre dışı bırakma yetkileri var mı? |  |  |
| 35 | Yazılım ve sistemler üzerinde yapılan işlemlerin logları tutuluyor mu? (Programlarda yapılan işlemler, dosya sunucu üzerinde yapılan işlemler, ağ bağlantılarındaki değişiklikler vb.) |  |  |
| 36 | İşletim sistemleri üzerindeki yazılımların kurulum yetkileri kimlerde? Tüm sistemi etkileyecek yazılım güncellemelerini nasıl yapıyorsunuz?  (Değişiklik yönetimi uygulanıyor mu, eski sürümler saklanıyor mu?) |  |  |
| 37 | Bilgi Güvenliği olay yönetimi prosedürü/politikası mevcut mu? Bilgi güvenliği olaylarını kayıt altına alınıyor mu? Yaşanmış olayları kontrol ediyor musunuz? |  |  |
| 38 | Uyulmakta olan yasal, düzenleyici, mevzuat, standartlar tanımlanmış mı?  Tanımlanan mevzuat ve standartların kimin takibinde olduğu belirtilmiş mi? |  |  |
| 39 | Fikri mülkiyet haklarının korunması için nasıl bir çalışma yapıyorsunuz? (Lisanssız yazılım yükleniyor mu? lisans sayıları aşılıyor mu? lisans süreleri kontrol ediliyor mu?) |  |  |
| 40 | Tüm ilgili bilgi işleme sistemlerinin saatleri tek bir referans zaman kaynağına göre senkronize ediliyor mu? |  |  |
| 41 | Bilginin korunması için kriptografik kontrollerin kullanımına ilişkin bir politika geliştirilmiş ve gerçekleştirilmiş mi? |  |  |
| 42 | Geliştirme, test ve işletim ortamlar, yetkisiz erişim veya işletim ortamlarında değişiklik risklerinin azaltılması için birbirinden ayrılmış mı? |  |  |
| 43 | Misafir internet ağı mevcut ise kurum ağından ayrı şekilde yapılandırılmış mı?  Kurum içinde ayrıca VLAN konfigürasyonları yapılmış mı? |  |  |
| 44 | Bir bilgi güvenliği politika dokümanı, yönetim tarafından onaylanmış, yayınlanmış ve tüm çalışanlar ve ilgili dış taraflara bildirilmiş mi? |  |  |
| 45 | Kayıtlar kaybedilmeye, yok edilmeye, sahteciliğe, yetkisiz erişime ve yetkisiz yayımlamaya karşı yasal, düzenleyici, sözleşmeden doğan şartlar ve iş şartlarına uygun olarak korunuyor mu? |  |  |
| 46 | Kötücül yazılımlardan korunmak için tespit etme, engelleme ve kurtarma kontrolleri uygun kullanıcı farkındalığı ile birlikte uygulanıyor mu? |  |  |
| 47 | Bilgi, yasal şartlar, değeri, kritikliği ve yetkisiz ifşa veya değiştirilmeye karşı hassasiyetine göre sınıflandırılmış mı? |  |  |
| 48 | Riskler belirlenmiş mi? |  |  |
| 49 | Tedarikçiler ile yapılan anlaşmalar, bilgi ve iletişim teknolojileri hizmetleri ve ürün tedarik zinciri ile ilgili bilgi güvenliği risklerini ifade eden şartları içeriyor mu? |  |  |
| 50 | Kuruluş mevcut bilgi güvenliği politikalarını, prosedürlerini ve kontrollerini sürdürme ve iyileştirmeyi içeren tedarikçilerin hizmet tedariki değişiklikleri, ilgili iş bilgi, sistem ve dâhil edilen süreçlerin kritikliğini ve risklerin yeniden değerlendirmesini hesaba katarak yönetiyor mu? |  |  |
| 51 | Kullanıcılar, gözetimsiz teçhizatın uygun şekilde korunmasını temin ediyor mu? |  |  |
| 52 | Bilgi, yasal şartlar, değeri, kritikliği ve yetkisiz ifşa veya değiştirilmeye karşı hassasiyetine göre sınıflandırılmış mı? |  |  |

|  |  |  |
| --- | --- | --- |
| **BÖLÜM/BİRİM** | **TARİH** | **DENETİMDE KARŞILAŞILAN KİŞİLER VE GÖREVLERİ** |
|  |  | **Bkz.: Katılım Tutanağı** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **TESPİT EDİLEN UYGUNSUZLUKLAR** | | | | | | | | | | |
| **MAJOR BULGU SAYISI** |  | **Madde No'ları:** |  |  |  |  |  |  |  |  |
| **MİNÖR BULGU SAYISI** |  | **Madde No'ları:** |  |  |  |  |  |  |  |  |

|  |  |
| --- | --- |
| **İYİLEŞTİRİLMESİ GEREKEN YÖNLER-GÖZLEMLER** | |
| **Madde No** | **Gözlem Tanımı** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| **KUVVETLİ YÖNLER** | |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **KATILIM TUTANAĞI** | | | | |
| **SIRA** | **İSİM SOYİSİM** | **ÜNVAN** | **GÖREV** | **İMZA** |
| **1** |  |  |  |  |
| **2** |  |  |  |  |
| **3** |  |  |  |  |
| **4** |  |  |  |  |
| **5** |  |  |  |  |
| **6** |  |  |  |  |
| **7** |  |  |  |  |
| **8** |  |  |  |  |
| **9** |  |  |  |  |
| **10** |  |  |  |  |
| **11** |  |  |  |  |
| **12** |  |  |  |  |
| **13** |  |  |  |  |
| **14** |  |  |  |  |
| **15** |  |  |  |  |
| **16** |  |  |  |  |
| **17** |  |  |  |  |
| **18** |  |  |  |  |
| **19** |  |  |  |  |