1. AMAÇ

Bilgi Güvenliği Yönetim Sistemi'nin **ETIQA iç**erisinde sürdürülebilirliğin sağlanabilmesi için Bilgi İşlem Birimi personelleri başta olmak üzere ilgili çalışan ve üçüncü taraf kişi/kurumların yapması gereken çalışmaların temel kurallarını belirlemeyi amaçlamaktır.

2. KAPSAM

Bu politika **ETIQA** bilgi varlıklarının gizliliği, bütünlüğü ve erişilebilirliğini etkileyen tüm unsurları ve çalışma ortamlarını kapsamaktadır.

3. SORUMLULUK

BGYS politikalarının, gözden geçirilmesi ve güncellenmesinden BGYS Yönetim Temsilcisi ve BGYS Ekibi sorumludur. Bu politikalara uyulmasından iç ve dış tüm personeller sorumludur.

4. TANIMLAR

BGYS: Bilgi Güvenliği Yönetim Sistemi

5. POLİTİKA

5.1. Antivirüs Programı Uygulama Kuralları

a) Kurumun bütün bilgisayarları ve sunucuları anti-virüs yazılımına sahip olmalıdır.

b) Düzenli aralıklarla anti-virüs yazılımı otomatik veya manuel olarak güncellenecektir.

c) Virüs bulaşan makineler tam olarak temizleninceye kadar ağa bağlanmamalıdır.

d) Hiçbir kullanıcının herhangi bir sebepten dolayı anti-virüs programını sistemden kaldırması veya durdurmasını engelleyecek kısıtlamalar yapılmalıdır.

e) Bilinmeyen ve şüpheli bir kaynaktan gelen e-postalar Bilgi İşlem Birimi tarafından kontrol edilmelidir. Yapılan kontroller kurum ağından izole edilmiş bir ortamda yapılmalıdır.

f) Bilgisayarlarda kullanılan CD, USB vb. depolama aygıtları erişimleri virüs buluşma ihtimaline karşı kapatılmalıdır.

g) Ayrıcalıklı erişim yetkisi olan bilgisayarlarda kurum dışı CD, USB vb. materyaller kurum bilgisayarlarına takılmayacak şekilde önlem alınmalıdır.

h) Kurum ağına anti-virüs programı güncel olmayan bilgisayarlar dâhil edilmemelidir

5.2. Sunucu Güvenlik Kuralları

a) Kurum bünyesindeki bütün sunucuların yönetiminden sadece yetkilendirilmiş sistem yöneticileri sorumludur.

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

c) Kullanılmayan sunucular güvenlik ve elektrik tasarrufu açısından kapalı tutulmalıdır.

d) Sunucular üzerinde yapılan işlemlerin log kayıtları en az 1 hafta saklanacak şekilde ayarlanmalıdır.

e) İşletim sistemleri, uygulamalar, veri tabanları, ağ donanımları yetkili erişim logları tutulmalıdır.

f) Sunucuların yönetimi için her sunucunun kendi hesabı ile bağlantı yapılmalıdır. Sunuculara dışarıdan yapılan bağlantılar uzak bağlantıya ilişkin belirlenen kurallara göre yapılmalıdır.

g) Sunucular fiziksel olarak güvenlik önlemi alınmış sistem odalarında bulunmalıdırlar.

h) Sistem odaları sıcaklık, nem değerleri ve su basmasına karşı denetlenmelidir.

i) Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve kayıt altına alınmalıdır. Sistem odası sunucu bakımları refakatçi kontrolünde olmalıdır.

j) Elektrik ve data kabloları sunucu odaları dahil kurum içerisinde kanallardan geçmelidir.

k) Sistem odalarındaki ekipmanların bakımları düzenli olarak yapılmalı ve bakımlar kayıt altına alınmalıdır.

5.3. Ağ Yönetim Kuralları

a) Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için yedekli ekipman bulundurulmalı veya bakım anlaşmaları yapılmalıdır.

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

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

d) Kurum internet ağına misafirler alınmamalı, misafir ağı kurum ağından bağımsız tasarlanmalıdır.

e) Kamera, santral, kablosuz ağ, kullanıcı ağları vb. ağlar birbirinden ayrı olmalıdır.

f) Uzaktan bağlantı, kamera vb. için kabul görmüş varsayılan portlar kullanılmamalı ve portların güvenliği sağlanmalıdır.

g) Ağ cihazları yılda en az 1 defa açıklık tarama testlerinden geçirilerek güvenli hale getirilmelidir.

h) Ağ cihazlarının konfigürasyonları kritik değişikliklerden sonra veya belirli periyotlarda yedeği alınarak saklanmalıdır.

5.4. Uzak Bağlantı VPN Kuralları

a) Uzaktan bağlantılar sadece güvenli uygulamalar ile yapılmalıdır.

b) Üçüncü taraflar kendi sunucularına, tanımlanmış IP adresleri üzerinden RDP ile bağlantı kuracak şekilde ayarlanmalıdır.

c) VPN kullanım hakkı verilen kişiler firewall üzerinde listelenmeli ve düzenli olarak kontrol edilmelidir.

d) Uzak bağlantı yapan kurum dışı bilgisayarlar, Antivirüs Politikasına uygun bir şekilde cihazların antivirüs yazılımları kurulu ve güncel olmalıdır.

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

f) Kurum personeli dışında üçüncü taraflara verilecek erişimler için gizlilik anlaşması yapılmış olmalıdır.

g) Uzak bağlantı yetkileri sadece gizlilik taahhüdü alınmış üçüncü taraf kişi/kurumlara verilmelidir.

5.5. Tedarikçi ve Üçüncü Taraf Güvenlik Kuralları

a) Tedarikçiler, bakım firmaları veya üçüncü taraflar (müşteriler) bilgi sistemlerimize veya bilgi varlıklarımıza bakım vb. amaç ile geldiklerinde gizlilik anlaşması yapılması gerekmektedir.

b) Üçüncü taraflar kurum içerisinde bulundukları sürece kurum politikalarına uygun hareket etmekle yükümlüdürler.

c) Tedarikçiler, bakım firmaları veya üçüncü taraflar bilgi sistemlerinde veya bilgi varlıkları üzerinde yapacakları çalışmaları Bilgi İşlem Yöneticisine bildirilmelidir.

d) Tedarikçiler, bakım firmaları veya üçüncü taraflar kurumun bilgi sistemlerine kendilerine verilen yetki kapsamında erişim sağlayabilirler.

e) Tedarikçiler, bakım firmaları veya üçüncü taraflara verilen erişim yetkileri, erişim amaçlarına uygun olarak sadece çalışma alanlarında olacak şekilde kısıtlı verilmeli, logları saklı tutulmalı ve çalışma bittikten sonra verilen yetkiler hemen geri alınmalıdır.

f) Tedarikçiler, bakım firmaları veya üçüncü taraflar bilgi sistemlerine ve bilgi varlıklarına eriştikleri süre boyunca refakatçisiz bırakılmamalıdır.

g) Üçüncü taraflara erişim izni verilecek donanımlar *(bilgisayar, sunucu vb.)* için uzak bağlantı VPN kuralları uygulanacaktır. **ETIQA**, bilgi güvenliğine etki edebilecek bir risk görmesi durumunda tedarikçi, bakım firmaları veya üçüncü tarafların erişimlerini herhangi bir uyarıda bulunmadan kesebilir.

5.6. Mobil ve Taşınabilir Cihaz Yönetim Kuralları

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

b) Etki alanındaki bilgisayarların admin yetkileri sınırlandırılarak yalnızca user yetkilendirmesi ile ilgili kişiye teslim edilmelidir.

c) Taşınabilir cihazlar (tablet, laptop) teslim edilmeden önce şifre belirlenmelidir. Şifreler sadece kullanıcının kendisine teslim edilmelidir. Kullanıcı ilk oturum açmasında şifre değiştirmeye zorlanacak şekilde kural oluşturulmalıdır.

d) Etki alanı dâhilindeki bilgisayarlar üzerinde yapılan çalışmalar ve oluşturulan dosyalar ilgili kişiye yetki verilmiş ortak alana kaydedilmelidir.

e) Taşınabilir cihazlara kurum dışında meydana gelecek bilgi güvenliği zafiyetlerine karşı *(hırsızlık, bakım ve onarım faaliyetleri vb.)* şifreleme güvenliği *(encrypt)* kullanılmalıdır.

5.7. Veritabanı Güvenlik Kuralları

a) Veri tabanında bulunan kişisel ve kritik verilere her türlü erişim işlemleri *(okuma, değiştirme, silme, ekleme)* kaydedilmelidir. Log kayıtlarına yetkisiz erişimlere karşı kısıtlama yapılmalıdır.

b) Veri tabanı sunucusuna sadece yetki hakkına sahip olanlar bağlanmalıdır.

c) Veri tabanı bulunan sistemlere erişim yetkileri kayıt altına alınmalı ve bu yetkiler kontrol edilmelidir.

d) Veri tabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme kuralları oluşturulmalıdır. Yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli alınması sağlanmalıdır.

e) Bilgilerin saklandığı sistemler, fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.

f) Veri tabanı sistemlerinde yapılacak bakım onarım, yama ve güncelleme çalışmalarından önce ilgili birimlere duyuru yapılmalıdır.

g) Veri tabanına acil erişim gerekmesi durumunda aksiyon öncesinde ve sonrasında ilgili birimlere veya personellere bilgilendirme yapılmalıdır.

h) Veri tabanı aksiyonlarında destek firmasına talepler yazılı olarak bildirilmelidir.

i) Veri tabanları yedekleme listesine göre düzenli olarak yedeklenmelidir.

j) Veri tabanı bulunan medyalar kurum dışına çıkarılmamalıdır.

k) Veri tabanlarının bulunduğu medyaların doluluk oranları düzenli olarak kontrol edilmelidir.

l) Veri tabanı raporları düzenli olarak ilgili firma tarafından verilmelidir.

m) Veri tabanı erişimlerinde üreticinin belirlemiş olduğu default şifreler kullanılmamalıdır.

n) Veri tabanına erişimlerde en az yetki prensibine göre kullanıcının ihtiyacından fazla veriyi görmesi engellenmelidir.

5.8. Değişim Yönetimi Kuralları

a) Yazılımsal ve donanımsal değişiklik talepleri kayıt altında tutulmalıdır.

b) Değişiklik taleplerinin sözlü olarak alınmaması konusunda hassasiyet gösterilmelidir.

c) Bilgi sistemlerinde değişiklikler yetkilendirilmiş kişiler tarafından yapılmalıdır. Yazılımsal değişikliklerin yetkisiz kişiler tarafından gerçekleştirilmemesi için sistemlerde yetki sınırlaması yapılmalıdır.

d) Herhangi bir sistemde uzun süreli veya önemli değişiklik yapmadan önce bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenmelidir.

e) Mevcut sistemlerin kaynaklarının izlenmeli, sorun yaşanmaması adına gerekli önlem ve tedbirler alınmalıdır. Kapasite kullanımının yüksek olması durumlarında kapasite kullanımı düşürülmelidir. *(kullanılmayan servislerin kapatılması, gereksiz dosyaların silinmesi vb.)* Kapasite kullanımının düşürülememesi durumunda satın alma faaliyeti gündeme alınmalıdır.

f) Değişiklikler gerçekleştirilmeden önce ilgili birimlere / kişilere bilgi verilmelidir.

g) Yapılacak değişiklikten önce değişikliğin yapılacağı sistemlerin yedekleri alınmalıdır.

h) Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanmalı ve ilgili yöneticilere bilgi verilmelidir.

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

j) Yapılacak değişiklikler mümkün olduğunca test sunucuları üzerinde gerçekleştirilmelidir. Yapılan testlerin başarılı geçmesi halinde canlı sistemde değişiklikler gerçekleştirilmelidir.

k) Değişiklik yapılan donanımların sistem saatlerinin mevcut sistemler ile aynı olmasına dikkat edilmelidir.

l) Yazılımlar için yayınlanmış yamalar önce test edilmeli, sonra ilgili sistemlere yüklenmelidir.

m) Değişikliklere ilişkin kullanıcı ve yönetici log kayıtları alınmalı ve uygun koşullarda saklanmalıdır.

5.9. Kimlik Doğrulama ve Yetkilendirme Kuralları

a) Kullanıcı yetkileri, ilgili kullanıcın yöneticisinin talebiyle verilmeli veya kaldırılmalıdır.

b) Kimlik doğrulama bilgileri ilgili kullanıcının kendisine verilmelidir. İlk verilen kimlik doğrulama bilgileri kolay olmamalı ve ilk oturum açmada sistem tarafından değiştirilmeye zorlanmalıdır.

c) Kurum sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenmelidir.

d) Kurum sistemlerine erişmesi gereken firma kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanmalıdır.

e) Kurum bünyesinde kullanılan ve merkezi olarak erişilen uygulama yazılımları, paket programlar, veri tabanları, işletim sistemleri ve log-on olarak erişilen sistemler üzerindeki kullanıcı rolleri ve yetkiler belirlenmeli ve kontrol altında tutulmalıdır.

f) Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilmelidir.

g) Sistemlerin başarılı ve başarısız erişim logları düzenli olarak tutulmalıdır.

h) Sistemlere log-on olan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve kayıt alınmalıdır.

i) Kullanıcı hatalarını izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.

5.10. Kriptografik Kontroller

a) Kurum içerisinde tanımlanan gizli bilgi varlıkları kriptografik şifreleme yöntemleri ile saklanmalıdır.

b) Risk değerlendirmelerine göre yüksek düzeyde koruma gerektiren bilgi varlıklarının korunmasında güçlü şifreleme algoritması kullanılmalıdır.

c) Kritik ve kişisel veri barındıran donanımlar kullanıcıya zimmetlenmeden önce disk encrypt edilmelidir veya kurum dışına gönderilirken disk çıkarılmalıdır.

5.11. Olay İhlal Bildirim ve Yönetim Kuralları

a) 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 durumlarında mutlaka kayıt altına alınmalıdır.

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

c) Bilgi güvenliği ihlâli oluşması durumunda, kişilerin tüm gerekli faaliyetleri değerlendirmesi Bilgi Güvenliği Ekibi ile birlikte yapılmalıdır.

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

e) 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 alınmalıdır.

f) Adli incelemelerin yürütülebilmesi veya üretici firma kaynaklı zararların telafi edilmesi için ihlalin log kayıtları toplanmalı ve korunmalıdır.

g) Güvenlik ihlallerinden kurtulmak için gereken eylemler, sistem hatalarının düzeltilmesi hususları dikkate alınmalıdır.

h) Bilgi güvenliği olaylarının değerlendirilmesi sonucunda edinilen bilgi ile edinilen tecrübe, yeni kontrollerin oluşturulması, olayların kök nedenine inilmesi ve yazılı hale getirilmesi gerekmektedir.

i) 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 logları.
- Olay kanıtlarının korunması yetkili kişilerin dışında erişimi kapatarak veya yedekleme yaparak sağlanır.

5.12. Yazılım Geliştirme ve Taleplerin Karşılanması Kuralları

a) Kurumun ihtiyacını karşılayacak yazılım projelerinin başlatıldığından ve proje altyapısının uygun olduğundan emin olunmalıdır.

b) Yazılım talepleri değerlendirilirken mevcut yazılım envanteri dikkate alınarak yazılım ihtiyacı olup olmadığı değerlendirilmelidir.

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 kurallarına 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 ilgili personele yazılı olarak *(e-posta, mevcut kontrol formları vb.)* bilgilendirmesi yapılmalıdır.

h) Yeni alınmış veya revize edilmiş bütün yazılımlar test ortamında kontrol edilmelidir. Herhangi bir sorun görülmesi durumunda üretici firma ile iletişime geçilip çözüm arayışına girilmelidir.

i) Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.

j) Yazılımlar sınıflandırılmalı ve envanterleri çıkarılarak varlık envanteri güncellenmelidir.

k) Kurumda kişisel olarak geliştirilmiş yazılımların kullanılması engellenmelidir.

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

m) Üçüncü taraf yazılım desteği alınırken aşağıdaki hususlara dikkat edilmelidir;

- Lisans anlaşmaları, kodlara kimin sahip olacağı, fikri mülkiyet haklarına ilişkin çerçeve oluşturulmalıdır.
- Yazılım desteği esnasında, uzaktan erişimlerde güvenli bağlantı yöntemleri kullanılır.
- Güvenli tasarım, güvenli kodlama ve test yöntemleri belirlenmelidir.
- Sistem kalite ve güvenlik kabul gereksinimleri belirlenmelidir.
- Gerekli testlerin yapıldığına dair kayıt sunma yöntemleri belirlenmelidir.
- Açık kaynaklı yazılımlarda, kaynak kod güvenliğine ilişkin anlaşmalar yapılmalıdır.
- Geliştirme süreçlerinin denetleme hakkı belirlenmelidir
- Geliştirme esnasında yapılan güvenlik testleri, zararlı kod analizleri ve bu testlere ait sonuçların kayıtları istenmelidir.
- Yazılımın işletilmesi, yönetilmesi ve bakımı için gerekli işletim dokümanlarının gerekliliği belirlenmelidir.

n) Test ortamında gerçek veri kullanılmamalı ve hassas veriler maskelenmelidir.

o) Test ortamına erişimler kontrollü olmalı, test ortamında gerçek veri varsa erişim kontrolleri canlı ortamda uygulandığı şekilde uygulanmalıdır.

5.13. Erişim Kontrolleri

a) Kurum içerisinde giriş çıkışlar kamera sistemi ile kayıt altına alınmalıdır.

b) Aktif dizine bağlanan kullanıcı parolaları Parola Yönetim Kurallarına uygun tanımlanmalıdır.

c) Ağ üzerinde aktif dizin kullanıcıları için ortak alanlar oluşturulmalıdır. Bu ortak alanlar üzerindeki birimler ve kullanıcılara göre yetkilendirme yapılmalıdır.

d) Yetkilendirilen personel haricinde hiçbir personelin dosya silme yetkisi bulunmamalıdır.

e) Kurumda mümkün olduğunca SSL ya da benzeri güvenlik protokolleri kullanılmalıdır.

f) Erişim kontrolleri Erişim ve Kullanım Yetki Tablosunda belirtilen kontrol sorumluları tarafından tanımlanmış zaman dilimlerinde gözden geçirilmelidir.

g) Kullanıcılara erişim yetkilerinin verilmesi, hesap tanımlanması, yetkilerin düzenlenmesi veya yetkilerin kaldırılmasına ilişkin talepler ilgili personelin yöneticisi tarafından yazılı olarak alınmalıdır.

h) Ayrıcalıklı erişim yetkileri mümkün olduğunca süre sınırlı olmalıdır.

i) Bilgi İşlem birimin kullanmış olduğu uygulamaların yetkileri, Bilgi İşlem çalışanlarının yetki, rol ve sorumluluklarına göre verilmelidir.

j) Programların kaynak kodlarına erişim kısıtlanmalıdır.

5.14. Parola Yönetim Kuralları

a) Active Directory hesap şifreleri kolay tahmin edilmeyen karmaşık şifreler olmalıdır.

b) Kullanıcı bilgisayar şifreleri 90 günde bir değiştirilmeye zorlanmalıdır.

c) Oluşturulacak şifre son 3 parola ile aynı olmayacak şekilde kural belirlenmelidir. Bir parola değiştirildikten sonra 24 saat içerisinde tekrar değiştirilmesi engellenmelidir.

d) Bilgisayar kullanıcı hesaplarının parolaları en az 8 karakter olacak şekilde kural belirlenmelidir. Parola; büyük harf, küçük harf, rakam ve özel karakterden oluşmalıdır.

e) Kullanıcı bilgisayarları kullanılmadığı zaman otomatik olarak 10 dakika içerisinde şifreli ekran korumasına girecek şekilde kural belirlenmelidir.

f) Parolanın 5 kez üst üste yanlış girilmesiyle sistem kilitlenmelidir.

g) Kullanıcılara tahsis edilen ilk parola, Parola Yönetim Kurallarına uygun olarak oluşturulmalı ve kullanıcının ilk oturumu açmasıyla yeni parola oluşturmaya zorlamalıdır.

h) ETIQAçalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının parolaları da kolayca kırılamayacak güçlü bir şifreye sahip olmalıdır.

i) Kişisel Verilerin Korunması Kanunu 'na istinaden **ETIQA** personelinin bizzat kendi talebi olmaksızın parolası sıfırlanamaz veya değiştirilemez. Olağanüstü durumlarda güvenlik açığı oluşması durumunda parola Bilgi İşlem Birimi tarafından değiştirilebilir ya da sıfırlanabilir.

5.15. Konfigürasyon Yönetim Kuralları

a) Kural yazımlarında kaynak, hedef, port, zaman bilgileri spesifik şekilde belirtilmelidir.

b) Birbiri ile eşleşen kurallar hem yönetim açısından karmaşıklık hem cihazın işlemci gücünü gereksiz yere kullanacağından dolayı tespit edilip silinmelidir.

c) Hit almayan kurallar hem yönetim açısından karmaşıklık hem cihazın işlemci gücünü gereksiz yere kullanacağından dolayı tespit edilip silinmelidir.

d) İnternet üzerinden firewall cihazına erişim olmamalıdır.

e) Any olarak adlandırılan her şey güvenlik açığı oluşturacağından dolayı bu kurallar var ise silinip, silinemiyor ise revize edilmesi gerekmektedir.

f) İnternet üzerinden gelebilecek saldırı, virüs gibi durumlardan iç networkünüzün etkilenmemesi için bu erişimlerin kapalı olması gerekmektedir.

g) Site to Site VPN konfigürasyonlarında karşı firmanın sizin local IP'lerinizi öğrenmesi güvenlik açığı doğuracağından dolayı NAT işlemi yapmalıdır.

5.16. Veri Sızıntısı Önleme Yöntemleri Kuralları

a) Hassas verilerin işlendiği, depolandığı veya iletilen sistemler, ağlar ve diğer cihazlar, veri sızıntısı önleme tedbirlerine tabi tutulmalıdır.

b) Güvenli e-posta alışverişi için SPF, DMARC ve DİKM kayıtları e-posta servis sağlayıcı ve DNS üzerinde konfigüre edilmelidir.

c) Kurumun onay vermediği dosya transfer ortamları kullanılmamalıdır. Veri paylaşımında (dosya transferi vb.) MS 365 OneDrive ve E-Posta harici herhangi bir dosya transfer ya da paylaşım platformu kullanılamayacaktır.

d) Çalışanlar, veri sızıntısı önleme politikaları ve prosedürleri konusunda eğitilmeli ve bilinçlendirilmelidir.

e) Kritik ve hassas veriler, kurum veri güvenliği politikasına uygun olarak daha yüksek koruma önlemleri alınarak ayrıştırılmalıdır.

f) Hassas verilerin depolandığı ve taşındığı yerlerde şifreleme kullanılmalı, yetkisiz kişilerin şifresiz verilere erişmesi engellenmelidir.

g) Veri sızıntısı izleme araçları ve sistemleri kullanarak şirket verilerinin dışarıya sızması engellenmelidir.

5.17. Tehdit İstihbaratı Yönetim Kuralları

a) Hizmet alınan üretici (MS 365) tarafından yayınlanan güvenlik bültenleri gereklilikleri kapsamında tehdit istihbaratlarına uygun önlemler alınmalıdır.

b) Sistem yöneticileri tarafından takip edilen güvenlik açıklarının yayınlandığı bültenlere uygun kurum içerisinde gerekli önlemler alınmalıdır.

c) Bilgi Teknolojileri Kurumu (BTK) tarafından yayınlanan siber güvenlik dokümanlarına uygun olarak gerekli tedbirler alınmalıdır

5.18. Konfigürasyon Yönetimi Politikası

- Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümante edilmelidir.
- Yazılım ve donanım envanteri oluşturularak güncel tutulmalıdır.
- Herhangi bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenmelidir.
- Değişiklikler gerçekleştirilmeden önce Bilgi İşlem Birimi tepe yöneticisinden onay alınmalıdır. Tüm sistemlere yönelik yapılandırma dokümantasyonu oluşturulmalı, yapılan her değişikliğin bu dokümantasyonda güncellenmesi sağlanarak kurumsal değişiklik yönetimi ve takibi temin edilmelidir.
- Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik bir çalışma hazırlanmalı ve ilgili yöneticiler tarafından onaylanması sağlanmalıdır.
- Teknoloji değişikliklerinin kurumun sistemlerine etkileri belirli aralıklarla gözden geçirilmelidir

5.19. VERİ MASKELEME POLİTİKASI

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI İLE DÜZENLENEN KAYIT ORTAMLARI

- Kâğıt ortamlar
- Manuel veri kayıt sistemleri (formlar ziyaretçi giriş defteri)
- Yazılı, basılı, görsel ortamlar

- Elektronik ortamlar
- Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.)
- Yazılımlar Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.)
- Kişisel bilgisayarlar (Masaüstü, dizüstü)
- Mobil cihazlar (telefon, tablet vb.)
- Optik diskler (CD, DVD vb.)
- Çıkartılabilir bellekler (USB, Hafıza Kart vb.)
- Yazıcı, tarayıcı, fotokopi makinesi

SAKLAMAYI GEREKTİREN FİRMA AMAÇLARI

- Acil Durum Yönetimi Süreçlerinin Yürütülmesi
- Bilgi Güvenliği Süreçlerinin Yürütülmesi
- Çalışan Adayı / Stajyer / Öğrenci Seçme ve Yerleştirme Süreçlerinin Yürütülmesi
- Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi
- Çalışan Memnuniyeti ve Bağlılığı Süreçlerinin Yürütülmesi
- Çalışanlar İçin İş Akdi ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi
- Çalışanlar İçin Yan Haklar ve Menfaatleri Süreçlerinin Yürütülmesi
- Denetim / Etik Faaliyetlerinin Yürütülmesi
- Eğitim Faaliyetlerinin Yürütülmesi
- Erişim Yetkilerinin Yürütülmesi

5.20. VERİ SIZINTISI ÖNLEME POLİTİKASI

Hassas bilgileri işleyen, depolayan ve ileten sistem, ağ ve tüm cihazlara erişimi olan herkes bu politikadan sorumludur.

UYGULAMA

- **Veri sızıntısı önleme (DLP) yazılımlarını tüm sistemlere uygun şekilde kurmak.**
- **Kriptolu disk ortamları oluşturarak bu alanlarda verilerinizi şifreleyerek gizleyebilir, yetkili kullanıcılara erişim verebilirsiniz.**
- **Penetrasyon testinin düzenli aralıklarla yapılması.**
- **Önemli ve hassas bilgileri kriptolu bir şifre ile tutmak.**

5.21. WEB FİLTRELEME POLİTİKASI

Bu politikanın uygulanmasından firma ağları veya iletişim kanalları üzerinden internet erişimi sağlayan herkes sorumludur.

UYGULAMA

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

- **Antivirüs programlarına ek olarak sadece URL filtreleme yapmak üzere tasarlanan yazılımlar da sıklıkla kullanılmalıdır.**
- **Spam, zincir ve junk e-mailleri silinmelidir.**
- **Bilinmeyen ve şüpheli kaynaklardan asla dosya indirilmemelidir.**

5.22. BULUT HİZMETLERİ KULLANIM POLİTİKASI

Bu politika Kurum özelinde bazı hizmetlerin bulut hizmet kapsamında alınmasını ve kullanımı faaliyetlerini kapsar.

UYGULAMA

- **Bulut hizmet alınacak servisler belirlenir.**
- **Bulut hizmetler nesne depolama, sunucular, bulut devops gibi servisleri kapsar.**
- **Kullanılan ya da satın alınan bulut hizmetler firmalar arası imzalanan sözleşmelerle hukuki değer kazanır.**
- **Bulut hizmetlerin bakım ve geliştirme süreçleri hizmet alımının gerçekleştirildiği firmaca yerine getirilir.**

YAPTIRIM

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