İçindekiler:

1. E-Posta Politikası
2. Parola Politikası
3. Anti-Virüs Politikası
4. İnternet Erişim ve Kullanım Politikası
5. Sunucu Güvenlik Politikası
6. Ağ Cihazları Güvenlik Politikası
7. Ağ Yönetimi Politikası
8. Uzaktan Erişim Politikası
9. Kablosuz İletişim Politikası
10. İş Sürekliliği Yönetimi Politikası
11. Kimlik Doğrulama ve Yetkilendirme Politikası
12. Veri Tabanı Güvenlik Politikası
13. Teknik Açıklık Yönetimi Politikası
14. Görevler Ayırımı
15. Değişim Yönetimi Politikası
16. Bilgi Sistemleri Yedekleme Politikası
17. Kişisel ve Harici Ekipmanların Kullanımı Politikası
18. Veri Transfer Politikası
19. Risk Yönetimi Politikası
20. Kriptografik Kontroller ve Anahtar Yönetimi Politikası
21. Bilgi Sistemleri Kabul Edilebilir Denetim Koşulları Politikası
22. Fikri Mülkiyet Hakları Politikası

1. **AMAÇ:** KÖKSAN'in kurumsal olarak yürüteceği faaliyetleri kapsamında bilginin toplanması, değerlendirilmesi, raporlanması ve paylaşılması süreçlerinde güvenliğin sağlanmasına yönelik tedbir almak, bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek içeriden veya dışarıdan kasıtlı ya da kazayla oluşabilecek tüm tehditlerden korunmasını sağlamak, son kullanıcı, idareci, sistem ve veri tabanı yöneticileri ve teknik personelin bilgi sistem ve ağları üzerinde yapacakları çalışmalarda bilgi güvenliği farkındalık, duyarlılık ve teknik bilgi düzeylerinin artırılması ile sistemsel güvenlik açıklarının ortadan kaldırılmasını sağlayarak, insan kaynaklı zafiyetlerin önlenmesi ve gizliliği, bütünlüğü ve erişilebilirliği sağlanmış bilişim alt yapısının kullanılması ve sürdürebilirliğinin temin edilmesi sureti ile; veri ve bilgi kayıplarının önlenmesi bu yolla ekonomik zarara uğranılmaması ve kurumsal prestij kaybı yaşanmaması ana ilke ve amaçlar olarak öngörülmektedir.
   - KÖKSAN, bilgi güvenliği yönetim sistemini sürekli iyileştirmeyi, kendisine uygulanabilir yasal ve diğer şartlara uymayı ve ilgili tarafların uygulanabilir beklentilerini karşılamayı taahhüt eder.
   - KÖKSAN zaman içerisinde gelişimini güvence altına almak üzere politikasını ve bilgi güvenliği performansını sürekli gözden geçirecektir.
   - KÖKSAN, yalnızca yetkili bireylerin ve ortakların hassas bilgiyi görebilmesi için erişimi kontrol edebilecek veya sınırlayacaktır.Müşteri bilgilerine erişim, yalnızca bu bilgileri görmeye veya kullanmaya özellikle ihtiyaç duyan bireyler ve ortaklar ile sınırlandırılmıştır. Bilgiler bilgi sahiplerinin yazılı izinleri olmaksızın dış tarafların kullanımına sunulmayacaktır.
   - Kurum faaliyetlerinin, düzenleyici kurumların beklentilerini karşılayacak şekilde gerçekleştirilebilmesi, bilgi güvenliği ile ilgili kaygılara yönelik gerekli önlemlerin alınması ve güvenlik ihlallerinin önüne geçilmesinde çalışanların sorumluluklarının belirlenmesi ve dolayısıyla Kurum'un korunması amacıyla, bir Bilgi Güvenliği Politikası oluşturulmuştur. Bu politika, ilgili prosedür ve diğer eklerde belirtilen ilkeler ve önlemler, KÖKSAN için tanımlanmış ve geçerli hedefleri temsil etmektedirler.

2. KAPSAM: Bu doküman KÖKSAN içerisinde çalışan her personeli bağlayıcı niteliktedir. Politikaların ihlali durumunda **İnsan Kaynakları Disiplin Yönetmeliği** kapsamında gerektiğinde kurum içinde ihlalde bulunan adına yasal işlem yapılabilir.

Bu politika bilgi güvenliğinin sağlanması için ve bilgi sistemleri tasarlarken veya işletirken asgari uyulması gereken kuralları açıklamaktadır. Ayrıca KÖKSAN'da bu amaca yönelik olarak yayınlanmış tüm Bilgi güvenliği politikaları için şemsiye oluşturmaktadır. Bu politikalar temel olarak aşağıda belirtilen hedefleri amaçlamaktadır.

- Bilgi Sistemlerinde paylaşılmakta olan her türlü verinin güvenliğini sağlamak
- İş devamlılığını sağlamak ve güvenlik ihlalinden kaynaklanabilecek kanuni riskleri en aza indirmek
- Kurumun itibarını ve yatırımlarını korumak
- Hizmet performansını ve müşteri memnuniyetini artırma, verimliliği yükseltme ve sektörün gelişen ihtiyaçlarını dikkate alan dinamik yatırım planlarıyla sürekli gelişme ve iyileştirme hedefleriyle KÖKSAN faaliyetlerini tarafsız olarak sürdürmektedir.

3. TANIMLAR:

BGYK: Bilgi Güvenliği Yönetim Kurulu.

BGYS: Bilgi Güvenliği Yönetim Sistemi.

4. SORUMLULAR: KÖKSAN Organizasyon Şemasına bağlı personel.

5. UYGULAMA:

5.1. E-Posta Politikası: Bu politika şirket içerisinde e-posta altyapısına yönelik kuralları içermektedir. Kurum içerisinde kullanılan e-posta hesapları kurum kimliği taşımaktadır.

Kurum bünyesinde oluşturulan e-posta hesaplarının tüm personeller için doğru kullanımını kapsamaktadır.

Kullanıcılar İçin E-posta Kullanımında Dikkat Edilmesi Gerekli Hususlar:.

- ✓ Şirketin e-posta sistemi, taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajlar gönderilmek için kullanılamaz
- ✓ Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir. Örneğin, “Tümünü Yanıtla” seçeneğinin dikkatli kullanılması gerekmektedir.
- ✓ Şirket ile ilgili olan hiçbir gizli bilgi, gönderilen mesajlarda yer alamaz. Bunun kapsamı içerisine eklenen her türlü dosya dahildir.
- ✓ Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren epostalar alındığında BT ye bilgi verilmeli ve BT nin verdiği bilgiler doğrultusunda hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.
- ✓ Kişisel kullanım için internetteki listelere eve sosyal medyalara üye olunurken kurum e-posta adresleri kullanılmamalıdır.
- ✓ Spam, zincir e-posta, şüpheli e-posta vb. zararlı e-postalara yanıt verilmemeli ve BT haber verilmelidir.
- ✓ Kullanıcıların kullanıcı kodu ve parola girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal BT haber verilmelidir.
- ✓ Çalışanlar e-posta ile uygun olmayan içerikler (ırkçılık, siyasi propaganda vb.) gönderemezler.
- ✓ Şirket içerisinde kişisel amaçlar için e-posta kullanımı mümkün olduğunca makul seviyede olmalıdır.
- ✓ Çalışanlar kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesi ve okunmasını engellemekle sorumludurlar. Bu nedenle kullanıcılar ancak kendi özel şifreleri ile mail sistemini kullanabilir ve e-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı Bilgi Teknolojileri Bölümü tarafından korunur.

- ✓ Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal BT ye haber verilmelidir.
- ✓ Gönderilen e-postalara eklenecek dosyaların boyutlarına dikkat edilerek ekli dosyanın sıkıştırılıp gönderilmesine özen gösterilmelidir. Gönderilecek olan ekli dosyanın boyutu 20 mb ile sınırlandırılmıştır.
- ✓ E-posta adresine sahip kullanıcının herhangi bir sebepten birim değiştirmesi durumunda unvan yada diğer departman bilgileri KÖKSAN Bilgi Teknolojileri Bölümü'ne bildirilmelidir.
- ✓ Kullanıcılar sunucu üzerinde 5 GB kullanım kotasına sahiptirler. Bu sınır, müdür, yönetim kurulu üyeleri ve Genel Müdür'ün onay verdiği diğer personeller için gerektiğinde arttırılabilir. Kota dolduğu zaman kullanıcı mail atamaz ve alamaz. Kullanıcıların belirli zamanlarda gereksiz maillerini silmeleri ve arşiv yapmaları gerekmektedir.
- ✓ KÖKSAN mail duyuru sistemi sadece genel duyurular (İnsan Kaynakları duyuruları, Kalite Yönetim Sistemi duyuruları, Bilgi Güvenliği Yönetim Sistemi duyuruları, İSG duyuruları, Proje duyuruları vb.) yapmak amacıyla ve yetkili kişiler tarafından kullanılabilir

Mail Oluşturmada Dikkat Edilmesi Gereken Hususlar:

- ✓ Genel olarak e-posta ortamında uzun ve karışık cümleler kurmaktan kaçınmalı, mümkün olduğunca basit, kesin, açık ve yanlış anlaşılmalara neden olmayacak bir dil kullanılmaya gayret edilmelidir. Araştırmalara göre, kısa cümlelerin uzun cümlelere göre daha çabuk ve net anlaşıldığı kanıtlanmıştır.
- ✓ Dilbilgisi kurallarına ve noktalama işaretlerine uygun, yalın bir dil kullanılmaya gayret edilmelidir. Hitap edilen alıcının kimliğine göre bir dil ve ifade tonu belirlenmelidir. Uygun bir selamlama ve kapanış dili kullanmak oldukça önemlidir.
- ✓ Yazım tarzı olarak pozitif bir tarz benimsenmelidir. Caps Lock düğmesi kapalı tutulmalıdır, çünkü büyük harfle yazdığınız yazılar sizin kızgın veya BAĞIRIYOR olduğunuz anlamına gelir ve kaba bir davranış olarak algılanabilir.
- ✓ Kısaltmaları yazarken küçük harf kullanılmamalıdır. Cümlelere başlarken büyük harfle başlanılması ihmal edilmemelidir. SMS yazarken kullanılan kısaltma ve ikon

kullanılması profesyonel bir yaklaşım değildir.

- ✓ Mesaj gönderilmeden önce yazım hatalarına karşı kontrol edilmelidir.
- ✓ Metin içerisindeki bazı kısımlara dikkat çekmek için, bu kısımları kalın (bold) karakterlerle, altını çizerek, başka renk vb. şekilde yazmak uygun bir davranış değildir. Örneğin kalın (bold) karakterle ayrıştırılmış cümle veya sözcükler, yüz yüze konuşmada muhatabınıza bağırarak konuştuğunuz durumlara benzer etki oluşturabilir. Bir cümlenin altını çizmek, muhatabınızın anlayış kabiliyeti ile ilgili bir hakaret olarak değerlendirilebilir. Ancak mail içeriğinde tarih ve yer belirtiliyorsa sadece bu bilgilerin kalın karakterlerle yazılması söz konusu olabilir. Mutlak ayrıştırılması ve vurgulanması gereken bir bölüm varsa, bunu diğer yazılı dokümanlardaki uygulamalara benzer olarak yapmaya özen gösterilmelidir. Örneğin, alıntı cümlelerini iki tırnak arasında, eğik (italik) harflerle veya ayrı bir paragrafta eğik harflerle yazılabilir.
- ✓ E-postalar, “konu” kısmı mutlaka doldurularak gönderilmelidir. İçeriğin ne hakkında olduğunu bildiren bir konu başlığı, gönderilere tekrar bakmak gerektiğinde, hem göndericinin hem de alıcının isini kolaylaştırır. Konu baslığı, içeriğe uygun anahtar kelimelerden oluşan kısa bir tanımlama seklinde olmalıdır.
- ✓ Elektronik postanın “kime” bölümü konunun direkt muhatabı olan kişi, “bilgi” ve “gizli bilgi” bölümleri ise, iletinin bilgi amaçlı gönderilmesi gereken kişiler için kullanılır. E-postanın “bilgi ve gizli” olarak yollandığı kişiler, mesajın doğrudan muhatabı değillerdir. İleti bu alıcılara sadece bilgi vermek amacıyla yollanmış demektir.
- ✓ Bir konu hakkında hatırlatma, uyarı, şikayet içeren mesajın “Bilgi” olarak asıl alıcının üstü pozisyonundaki kişilere de yollanması, alıcının yöneticisine şikayet edilmesi anlamı taşıyabilir. Mesaj alıcıları seçilirken alıcıyı diğer alıcılar önünde küçük düşürecek ifadelerden kaçınılmalıdır.
- ✓ Şikayet mesajları yazarken dikkatli bir tavır sergilenmeli, şikayet mailine her zaman kurum etiğine yakışır bir dil ile başlanılmalıdır.
- ✓ Mesajlar dikkatle kontrol edilmeli, gönder tuşuna basmadan önce son kontroller yapılmalıdır.

- ✓ Mesajların şirketin ve kişilerin adına bir izlenim verdiği unutulmamalıdır. Bunun iyi bir izlenim olması gerektiği dikkate alınmalıdır.
- ✓ Bazen tam olarak ne düşündüğünüzü ve ne hissettiğinizi söylemek uygun olmayabilir, özellikle de önemli müşteriler söz konusu olduğunda. Kurumsal bir dil kullanılması gereği unutulmamalıdır.

Gelen Mesajları Yanıtlamada Dikkat Edilecek Hususlar :

- ✓ Zincir veya toplu gönderilmiş mesajlara, gerekmediği sürece, “tümünü yanıtla” şeklinde cevap yazılmamalıdır. Eğer zincirleme olarak uzayan bir mesaja cevap veriliyorsa, bir önceki mesaj dışındaki mesajlar, çok gerekli değilseler silinmelidir. Aksi takdirde mesaj fazlasıyla uzayacak ve okunamaz hale gelecektir. Çok sayıda kişiye yazılmış olan maillere verilecek cevaplarda “tümünü yanıtla” seçeneği ile geri dönülmeden önce söz konusu cevabın ya da yazışmanın tüm alıcıları ilgilendirdiğinden emin olunmalı, gerekirse sadece maili yazan kişiye “yanıtla” seçeneği kullanılmalıdır.
- ✓ Elektronik ortamda, genel bilgilendirme maksadıyla yönetim tarafından yayınlanan duyurulara, bireysel olarak ve tüm alıcılara geri dönecek şekilde karşı mesaj yazılmamalıdır. Duyurulan konu ile ilgili herhangi bir sorun varsa sadece o mesajı yazan kişiye bir mail atılarak durum ile ilgili olarak bilgi temin edilebilir ya da bilgi verilebilir.

Bilgi Teknolojileri Sorumlulukları:

- ✓ Bir çalışanın işten ayrılma bilgisi alındığı anda, ilgili kullanıcının hesabı erişilemez hale getirilmesi amacıyla şifresi derhal değiştirilir.
- ✓ İşten ayrılma süreci tamamlandığında, söz konusu kullanıcı hesabı Bilgi Teknolojileri Bölümü tarafından pasif duruma getirilir.
- ✓ Kullanıcıya gelecek yeni e-postalar, ilgili bölüm yöneticisinin talebi doğrultusunda belirlenen kişilere yönlendirilerek bilgi akışının devamlılığı sağlanır.
- ✓ Ayrıca, kullanılmayan e-posta adresleri aylık olarak düzenli bir şekilde tespit edilmekte ve ilgili yöneticinin bilgisi dahilinde sistemden tamamen kaldırılmaktadır.
- ✓ Dışarıdan gelen mailler Antispam gateway tarafından spam-virus ve zararlı kodlar için kullanıcıya gelmeden önce otomatik olarak taranır. Aynı zamanda

kullanıcıların bilgisayarında kurulu olan anti virüs programı ek güvenlik sağlamaktadır.

5.2. **Parola Politikası:** Bu politikanın amacı güçlü bir parola ekleme oluşturulması, oluşturulan parolanın korunması ve parolanın değiştirilme sıklığı hakkında standartlar oluşturulmasıdır. Parolalar bilgisayar güvenliğinin en önemli unsurlarıdır. Kullanıcı hesaplarının korunmasında ilk sırada yer alan güvenlik önlemidir. Kötü seçilmiş bir parola bütün kurumsal ağı etkileyebilecek sonuçlar doğurabilir. Bunun gibi bir durumla karşılaşmamak için kurumsal ağa dahil olan bütün kullanıcılar (çalışanlar, danışmanlar, uzaktan destek veren firmalar vb.) parolalarını korumak için aşağıdaki gerekli önlemleri almakla sorumludurlar.

Genel Parola Kullanım Prensipleri:

- ✓ Tüm sistem düzeyinde parolalar (ERP, E-Posta ve Domain kullanıcıları vs.) en az 90 günde bir değiştirilmelidir.
- ✓ Kullanıcı parolalarının 90 günde bir değişmesini sistem zorunlu tutmaktadır.
- ✓ Yeni girilen parola son üç (3) parola farklı olmalıdır.
- ✓ Parolalar en az sekiz (8) karakter uzunluğunda olmalıdır. Parola içerisinde kullanılan karakterler “harf” , “rakam” ve “sembol” içerecek şekilde sistem tarafından kontrol edilir.
- ✓ Sistem yöneticisi tarafından verilen ilk parola, sistem değiştirmeyi zorunlu tutmaktadır, kişisel parola ile değiştirilir.
- ✓ Tüm kullanıcı düzeyi ve sistem düzeyinde parolalar aşağıda açıklanan kurallara uymak zorundadır.

Parola Koruma Kuralları – Yapılmayacaklar:

- ✓ KÖKSAN ’da tüm çalışanlar parolalarını herhangi bir kişiyle paylaşmamalıdır. Parolalar şirkete ait gizli bilgiler olarak düşünülmelidir.
  - ✓ Şirket çalışanları herhangi bir kişiye telefonda parola vermemelidir.

- ✓ E-posta mesajlarında parolalar paylaşılmamalıdır, yazılı, online olarak, lokal uygulamalarda yada elektronik ortamda saklanılmamalıdır.
- ✓ Parolaları yazılı olarak tutmaya, sadece **Acil Durum Eylem Planı** yaptırımları dikkate alınarak izin verilir. Bu durumda, yazılı parolalar kapalı bir zarfta güvenli bir biçimde saklanmalıdır.
- ✓ Başkalarının önünde parolalar hakkında konuşulmamalıdır.
- ✓ Parolalar aile bireyleri de dahil diğer kişilerle paylaşılmamalıdır.
- ✓ Görev devri (örneğin izin, hastalık) söz konusu olduğunda bile başkalarına verilmemelidir. Çalışanın işten uzakta olması durumunda iş arkadaşlarına dahi parolaları bildirmemelidir. Kişiye ulaşılamaması durumunda yönetici ve üstü seviyedeki bir yöneticinin destek sistemi veya yazılı olarak (e-mail) bildirdiğinde parola Bilgi Teknolojileri tarafından sıfırlanabilir.
- ✓ Parolanın üçüncü şahıslarca öğrenilmiş olması durumunda, parola derhal değiştirilmelidir.

Parola belirlerken kullanıcı tarafından dikkat edilmesi gerekli hususlar:

- ✓ Parola karışık olmalıdır (içinde “harf”, “rakam” ve “sembol” bulunmalıdır.)
- ✓ Aynı parolanın birden fazla uygulamada kullanılmaması tavsiye edilmektedir. Aksi taktirde uygulamalardan birine ait parola ele geçirilirse diğer uygulamalara da erişilmiş olur. Ancak bu durum kullanıcının kendi isteğine bırakılmıştır.
- ✓ Kullanıcı adı ve soyadının parola içinde bulunmamasına dikkat edilmelidir.
- ✓ Parolaların tahmin edilmesi kolay ve ardışık şekilde kullanılmaması önerilir (örn İstanbul , 1453 , Galatasaray)
- ✓ Parola girişi hızlı ve gizli yapılmalıdır. Parola girişi sırasında üçüncü şahısların klavyeyi izlemediğinden emin olunmalıdır. Kullanıcılar parolalarını akıllarında tutabilmelidir. Parolalar, takvime ya da not kağıtlarına yazılmamalı, bilgisayarda

saklanmamalıdır. Aksi takdirde kullanıcının güvenliği parolanın yazılı olduğu kağıda ya da bilgisayarda saklanan dosyaya bağlıdır.

- ✓ Parolayı bir yere not etmek durumunda kalmamak için kullanıcı kendisi için hatırlaması kolay, fakat yabancılar için tahmin edilmesi zor parola seçmelidir. Kullanıcı kendisine göre bir parola bicimi geliştirebilir. Böylece farklı sistemler için parola belirlerken ve parolasını hatırlarken zorlanmayacaktır.

5.3. **Anti-Virüs Politikası:** Bu politika kurum içindeki tüm son kullanıcı bilgisayarlarını kapsamaktadır.

- ✓ Anti virüs yazılımının sürekli olarak çalışır durumda olmasından ve güncellenmesinden Bilgi Teknolojileri Personelleri sorumludur.
- ✓ Tüm bilgisayarlarda standart ve tek anti-virüs yazılımı yüklüdür. Güncellemeleri otomatik olarak kullanıcı müdahalesi olmadan merkezi sunucu üzerinden yapılmaktadır.
- ✓ Kullanıcıların bilgisayarından anti virüs yazılımını kaldırmaları uzun ve kırılması güç parolayla engellenmiştir.
- ✓ Virüs bulaşan bilgisayar tam olarak temizlenmeden ağa eklenmez.
- ✓ Anti-Virüs konusunda şirket standartları ve kullanıcıların uyması gereken kurallar **Bilişim Kaynakları Kullanım Standartları Politikası**'nda *Anti-Virüs Yazılımı Kullanımı* başlığında detaylıca verilmiştir.

5.4. **İnternet Erişim ve Kullanım Politikası:** Bu politikanın amacı internet kullanıcılarının güvenli internet erişimi için gerekli olan kuralları kapsamaktadır.

İnternet Erişim ve Kullanımı Genel Prensipleri:

- ✓ Şirket çalışanları, danışmanlar, destek hizmeti veren kişi ve kurumlar (Denetim firmaları, donanım ve yazılım destek firmaları vb.) görev tanımları ve sözleşmelerde yer alan görevlerini yerine getirebilmek için çalışmalarına destek olacak şekilde kendilerine sağlanacak şirket kaynaklarını kullanarak internete erişebilirler.
- ✓ Bilgi Teknolojileri Bölümü, şirketin merkez ofisi ve dışındaki tüm lokasyonlarda (depolar, aktarma merkezleri, lojistik şubeler vb.) uygun programlar kurularak kullanıcıların internet erişimlerini sağlamaktadır.
- ✓ Bilgi Teknolojileri Bölümü, gerekli durumlarda şirket bünyesindeki birimlerde kurulu olan sistemlerin hızlandırılması vb. gerekli nedenlerle internet trafiği üzerinde kısıtlamalara gidebilir ve kullanıcıların kullanım kapasitelerini belirleyebilir.

Bilgi Teknolojileri Bölümü Sorumlulukları:

- ✓ Şirketin bilgisayar ağı internet sağlayıcı aracılığıyla METRO ETHERNET yedekliliği 4,5g , Radyolink olarak konuk interneti ise Fiber ADSL üzerinden internete çıkış yapacaktır.
- ✓ Ağ güvenlik duvarı (Firewall), şirketin ağı ve dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında şirketin karşılaşabileceği sorunları önlemek üzere tasarlanmıştır. Dışarıdan şirket içerisine olan bağlantılar, (şubeler, depolar,aktarma merkezleri, mobil kullanıcılar ve anlaşmalı destek firmaları) ağ güvenlik duvarına tanımlanmış KÖKSAN IP adresleri ve Global VPN client ile sağlanır.
- ✓ Şirket bilgisayarlarının internete çıkışları, Firewall un içerik filtreleme özelliği kullanılarak, belirlenen seviyelerde gruplar oluşturulup kullanıcı tanımları bu gruplara atanarak sağlanır. İstenilmeyen (kumar, yetişkin içerik, uyuşturucu, şiddet içeren siteler vb.) internet siteleri yasaklanır. (İnternetten bulaşan virüsler, çoğunlukla bu tür siteler aracılığıyla sisteme zarar vermektedir).
- ✓ İstemci ve sunucularda anti virüs programı kuruludur. Gelen mailler antispam ve antivirüs kontrolünden geçerek istemcilere ulaştırılır. İnternet üzerinden (http, https v.s. kontrolü) gelebilecek zararlı kodlar vb. Firewall içerik filtreleme sistemi tarafından kontrol edilerek girişine izin verilmez.Ancak sistem yöneticisi tarafından yetkilendirilmiş kişiler internete çıkarken uygun içerikli servisleri kullanma hakkına sahiptir.

- ✓ 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna göre tüm KÖKSAN internet erişim kayıtları arşivlenir.

Kullanıcının Sorumlulukları:

- ✓ KÖKSAN internet kullanım hakkı genel olarak iş amaçlı verilmektedir. Bununla birlikte çalışanlar konuya sadece medya kullanım bilinci ve sorumluluğu ile yaklaştıkları sürece, ayrıca yasalar ve kurumun etik ilkeleri çerçevesinde diğer erişimlerine de izin verilebilir. Bu konudaki en önemli noktalar şirketin kendi bilgi birikimiyle ilgili kritik bilgilerinin, gizlilik kurallarının ve şirket imajının korunmasıdır.
- ✓ Her türlü anlık mesajlaşma programının kullanıcılar tarafından bilgisayarlarda kurulması, kullanılması veya internet siteleri üzerinden kullanılmasına izin verilmez. Ancak iş tanımına göre belirli kullanıcılara işin gerektirdiği ihtiyaç doğrultusunda Artık Risk Onay formu imzalatılarak Bilgi Teknolojileri Bölümü ve ilgili çalışanın yöneticisinin izni ile izin verilebilir.
- ✓ Çalışma saatleri içerisinde iş ile ilgili olmayan sitelerde çok fazla zaman geçirmek yasaktır.
- ✓ Şirket çalışanları, bilgi güvenliği politikası ve yürürlükteki Türkiye Cumhuriyeti yasaları ve yönetmeliklerine uygun hareket etmeli ve kesinlikle şirket internetini aykırı faaliyetlerde bulunmak için kullanmamalıdır.
- ✓ Bilgisayar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemeli ve dosya indirimi yapılmamalıdır.
- ✓ Sistemi gereksiz meşgul edecek, internet trafiğini gereksiz yere artıracak, müzik ve resim dosyaları, oyunlar, filmler ve benzeri programların (zip, rar, mpg, mpeg, avi, exe, com, mp3 vb. uzantılı dosyalar) internetten indirilmesi yasaktır.
- ✓ İnternet üzerinden Bilgi Teknolojileri Bölümü tarafından onaylanmamış yazılımlar indirilemez ve kurum sistemleri üzerine bu yazılımlar kurulamaz. Bu konuda kendi inisiyatifinizle yaptığınız her şey ciddi sonuçlara yol açabilir. Kurumsal işlevlere yönelik yazılım ihtiyaçlarının olması durumunda Bilgi Teknolojileri Bölümünden istenilmelidir.

- ✓ İnternete KÖKSAN bilgisayarları ile internete bağlanıyorsanız en güncel antivirüs yazılımının bilgisayarınızda yüklü ve çalışır durumda olduğundan emin olun.
- ✓ Üçüncü şahısların kurum internetini kullanmaları, Bilgi Teknoloji Bölümü sorumlularının izni ve bu konudaki politika dahilinde gerçekleştirilebilecektir.
- ✓ İnternet erişiminin tüm günlükleri (Log Kayıtları) saklanmaktadır. Bu kayıtlar her bir iş istasyonu bazında kaydedilir. Kurumumuzun bilgi birikimi ve ticari çıkarları her zaman için korunmalıdır.
- ✓ Internet kullanımı, ulusal ve uluslararası yasalara uygun olmalıdır. KÖKSAN bilgi güvenliği politikalarında belirtilen ihlalin ya da internet'in kötüye kullanımı durumunda insan kaynakları disiplin prosedürleri geçerlidir.
- ✓ Şirket çalışanları, görev tanımları ve sözleşmelerde tanımlı görevlerini yerine getirilebilmek için çalışmalarına destek olacak şekilde İnternet aracılığı ile dağıtılan bazı ücretsiz sürüm programlarını kullanmak istemeleri halinde, Bilgi Teknolojileri Bölümü yetkililerine başvurmaları ve yazılı onay almaları gerekmektedir. Bu tür programların internet üzerinden indirilmesi, kurulması sadece Bilgi Teknolojileri Bölümü personeli tarafından yapılacaktır. Bu tür programların işin yerine getirilmesine katkısı yoksa kullanılmamalıdır.
- ✓ Şirkete ait her türlü bilgi, doküman ve/veya yazılımın, iş amaçlı kullanım dışında, İnternet üzerinden satılması veya şirket dışındaki üçüncü kişilere herhangi bir sebeple gönderilmesi kesinlikle yasaktır.
- ✓ Şirket içi kullanımı için hazırlanmış, müşterileri ile ilişkilerini veya şirket imajını etkileyecek, herhangi bir bilgi, dosya veya duyurunun (iş potansiyelleri, birim maliyetleri, fiyatlar, yatırımlar, ihale bilgileri vb.) İnternet üzerinden açıklanması veya dağıtılması kesinlikle yasaktır.
- ✓ Şirkete ait önemli bilgilerin yetkisiz kişilere verildiği veya açıklandığı tespitedildiğinde veya bu konuda şüphe oluştuğunda konu Bilgi Teknolojileri Bölümü ile zaman geçirilmeden bildirilmelidir.

5.5. **Sunucu Güvenlik Politikası:** Bu politikanın amacı kurum bünyesindeki sunucuların

temel güvenlik konfigürasyonlarının nasıl olması gerektiğini belirtir. Bu temel güvenlik konfigürasyonların yapılmasından ve işletilmesinden Bilgi Teknolojileri Sistem Yöneticisi sorumludur.

✓ **Genel Konfigürasyon Kuralları:**

- Sunucular üzerindeki kullanılmayan servisler ve uygulamalar kapatılmaktadır.
- Sunuculara erişimler loglanmakta ve erişim kontrol logları incelenmektedir.
- Sunucu üstünde çalışan işletim sistemlerinin, hizmet sunucu yazılımlarının, yönetim yazılımlarının vb. koruma amaçlı yazılımların kontrollü sürekli güncellenmesi yapılmaktadır. Anti virüs güncellemeleri otomatik, yama güncellemeleri sistem yöneticileri tarafından kontrollü şekilde yapılmaktadır. Bu yama güncelleme işlemi, değişiklik yönetiminden sayılmamaktadır.
- Sistem ve uygulama yöneticileri gerekli olmadıkça “administrator”, “root” vb. kullanıcı hesaplarını kullanmamaktadırlar. Windows ortamında gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmaktadırlar. Önce kendi kullanıcı hesapları ile giriş yapıp daha sonra genel yönetici hesaplarına geçiş yapmaktadırlar.
- Ayrıcalıklı bağlantılar teknik olarak güvenli kanallar (ssh veya ssl, ipsec vpn gibi parolalenmiş ağ) üzerinden yapılmaktadır.
- Sunucular fiziksel olarak korunmuş sistem odalarında korunmaktadırlar.

5.6. **Ağ Cihazları Güvenlik Politikası:** Bu politika kurumun ağındaki yönlendirici (router) ve anahtarların (switch) sahip olması gereken minimum güvenlik konfigürasyonlarını tanımlamaktadır.

- Bilgisayar ağında bulunan tüm cihazların IP’leri ve mac adresleri aktif cihaz listesinde yer almaktadır.
- Yönlendirici ve anahtarlarda enable parolasi kodlanmış şekilde saklanmaktadır.
- Yönlendirici giriş portuna gelen IP adresleri kullanıcı parolasi ile kabul edilir.
- Yönlendirici ve anahtarlarda çalışan güvenli web servislerine erişim sadece Bilgi Teknolojileri çalışanlarına verilmektedir.

- Yönlendiricilerde ve anahtarlarda SNMP kullanıldığı durumlarda varsayılan olarak kullanılan "public", community string'e farklı değerler atanmaktadır.
- Yazılım ve firmware'ler ilk önce test ortamlarında denendikten sonra çalışma günlerinin veya saatlerinin dışında canlı ortama taşınmaktadır.
- Cihazlar üzerinde varsayılan servisler kapatılacaktır (telnet, http). Bunların yerine güvenli protokoller ile bağlanılmalıdır (SSH, https).

5.7. **Ağ Yönetimi Politikası:** Ağ yönetim politikası, ağın güvenliği ve sürekliliğini karşılayan kuralları belirlemekte, standartlaştırılmasını amaçlamaktadır.

- Bilgisayar ağlarının ve bağlı sistemlerinin iş sürekliliğini sağlamak için yedeklilik sağlanmaktadır.
- Ağ üzerinde kullanıcının erişebileceği servisler kısıtlanmaktadır.
- Sınırsız ağ dolaşımı engellenmiştir.
- İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden teknik önlemler alınmıştır (Firewall vb.).
- Ağ erişimi VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılmıştır.
- Ağ bağlantıları periyodik olarak kontrol edilmelidir.
- Ağ üzerindeki yönlendirme kontrol edilmektedir.
- Bilgisayar ağına bağlı bütün makinelerde kurulum ve konfigürasyon parametreleri kurumun güvenlik politika ve standartlarıyla uyumlu olarak yapılmaktadır.
- Bilgisayar ağındaki adresler, ağa ait konfigürasyon ve diğer tasarım bilgileri 3. şahıs ve sistemlerin ulaşamayacağı bir şekilde saklanmaktadır.
- Bilgisayar ağıyla ilgili ag topolojisi güncel olmalı ve ağ cihazlarının güncel konfigürasyon bilgileri saklanmaktadır.
- Bilgisayar ağı üzerinde gerçekleşen işlemler takip edilmektedir.

5.8. **Uzaktan Erişim Politikası:** Bu politikanın amacı herhangi bir yerden kurumun bilgisayar ağına erişilmesine ilişkin standartları saptamaktır. Bu standartlar yetkisiz kullanımdan dolayı kuruma gelebilecek potansiyel zararları en aza indirmek için tasarlanmış olup, **Erişim Politikası** dokümanı ile detaylandırılmıştır.

5.9. **Kablosuz İletişim Politikası:** Bu politika kurum bünyesinde kullanılabilecek bütün kablosuz haberleşme cihazlarını (dizüstü bilgisayar, akıllı cep telefonları, PDA, tablet vs.) kapsamaktadır. Kablosuz cihazların gerekli güvenlik tedbirleri alınmaksızın kurumun bilgisayar ağına erişimini engellemeyi amaçlamaktadır. **Erişim Politikası** içinde ele alınmış ve detaylandırılmıştır.

5.10. **İş Sürekliliği Yönetimi Politikası:** Bilgi güvenliği ve iş sürekliliğiyle ilgili standartlar belirlenmektedir.

Bu kapsamda;

- Bilgi sisteminin kesintisiz çalışması için gereken önlemler alınmıştır.
- Kurum bilişim sistemlerinin kesintisiz çalışmasını sağlanması için aynı ortamda kümeleme (cluster), uygulanmaktadır. Risk işleme planı ile ele alınmış ve değerlendirilmiştir.
- Acil durumlarda sistem logları yedeklenmektedir.
- Bir güvenlik ihlali yaşandığında BGYK acil olarak bilgilendirilmektedir.
- Acil durum kapsamında değerlendirilen olaylar aşağıda farklı seviyelerde tanımlanmıştır:
  - **Seviye A (Bilgi Kaybı):** Kurumsal değerli bilgilerin yetkisiz kişilerin eline geçmesi, bozulması, silinmesi.
  - **Seviye B (Servis Kesintisi):** Kurumsal servislerin kesintisi veya kesintiye yol açabilecek durumlar.
  - **Seviye C (Şüpheli Durumlar):** Yukarıda tanımlı iki seviyedeki durumlara sebebiyet verebileceğinden şüphe duyulan ancak gerçekliği ispatlanmamış durumlar.
- Her bir seviyede tanımlı acil durumlarda karşılaşılabilecek riskler, bu riskin kuruma

getireceği kayıplar ve bu risk oluşmadan önce ve oluştuktan sonra hareket planları **Risk İşleme Planı** ile dokümante edilmiştir.

- Acil durumlarda şirket çalışanları Bilgi Teknolojilerine rapor etmektedir, ihlal bildirimi doğrudan BGYK'ya raporlanmaktadır.
- Bu konuda **Bilgi Güvenliği İş Sürekliliği Yönetimi Prosedürü**, **Acil Durum Eylem Planı** ve **Bilgi Güvenliği İhlal Yönetimi Politikası** hazırlanarak yayınlanmıştır.

5.11. Kimlik Doğrulama ve Yetkilendirme Politikası: Bu politika kurumun bilgi sistemlerine erişimde kimlik doğrulaması ve yetkilendirme politikalarını tanımlamaktadır. Bilgi sistemlerine erişen kurum çalışanları ve kurum dışı kullanıcılar bu politika kapsamındadır.

- Kurum sistemlerine erişebilecek kurumdaki kullanıcıların ve kurum sistemlerine erişmesi gereken diğer firma kullanıcılarının hangi sistemlere, hangi kimlik doğrulama yönetimi ile erişebileceği belirlenmiş ve **Erişim Politikası** ile dokümante edilmiştir.
- Kurum bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veri tabanları, işletim sistemleri ve log-on olarak erişen tüm sistemler üzerindeki kullanıcı rolleri ve yetkileri belirlenerek denetim altında tutulmaktadır, periyodik olarak bu yetkiler gözden geçirilmektedir.
- Gerekli minimum yetkinin verilmesi prensibi benimsenmektedir.
- Erişim ve yetki seviyeleri belirli periyotlarda kontrol edilip gerekli durumlarda güncellenmektedir.
- Tüm kullanıcılar kurum tarafından kullanımlarına tahsis edilen sistemlerdeki bilgilerin güvenliğinden sorumludur.
- Sistemlere başarılı ve başarısız erişim logları düzenli olarak tutulmaktadır. Erişim Logları düzenli olarak incelenmektedir.
- Kullanıcı hareketlerini izleyebilmek için her kullanıcıya kendisine ait bir kullanıcı hesabı açılmaktadır.

5.12. **Veri Tabanı Güvenlik Politikası:** Kurumdaki veritabanı sistemlerinin kesintisiz ve güvenli şekilde işletilmesine yönelik standartları tanımlar. Tüm veritabanı sistemleri bu politikanın kapsamındadır.

- Veritabanı sistemleri envanteri ve bu envanterden sorumlu kişiler tanımlanmıştır.
- Veritabanı işletim kuralları belirlenmiştir.
- Veritabanı sistem logları tutulmakta, gerektiğinde Bilgi Teknolojileri Bölümü tarafından kontrol edilmektedir.
- Veritabanı yedekleme politikaları oluşturulmuş, yedeklemeden sorumlu sistem yöneticileri belirlenmiş ve yedeklerin düzenli olarak alındığı kontrol edilmektedir.
- Veritabanı erişim politikaları “kimlik doğrulama ve yetkilendirme” çerçevesinde oluşturulmuştur.
- Hatadan arındırma, bilgileri yedekten dönme kuralları “iş sürekliliğine” uygun, kurumun ihtiyaçlarına yönelik olarak oluşturulmuştur.
- Bilgilerin saklandığı sistemler, fiziksel güvenliği sağlanmış sistem odasında tutulmaktadır.
- Yama ve güncellemeler yapılmadan önce bildirimde bulunulmakta ve sonrasında ilgili uygulama kontrolleri gerçekleştirilmekte olup, değişim yönetiminden sayılmamaktadır.
- Veritabanı sunucularında sadece rdp, ssl ve orijinal veritabanı yönetim yazılımları kullanılmakta, bunun dışında ftp, telnet vb. clear text bağlantılara kapanmıştır.
- Veritabanı sunucusuna ancak zorunlu hallerde root ve administrator olarak bağlanılmaktadır. Root ve administrator parolasi yetkili kişilerde bulunmaktadır.
- Bütün kullanıcıların yaptıkları işlemler loglanmaktadır.
- Veritabanı sunucularına 3. tarafların destek amaçlı erişimleri VPN ile güvenli bağlantı sağlamaktadırlar.
- Veritabanı sunucularına ancak yetkili kişiler erişebilmektedir.
- Veritabanı sunucularında kod geliştiren kullanıcıların dışında hiçbir kullanıcı bağlanıp sorgu yapamamaktadır.
- Parolaler 90 günlük aralıklarla değiştirilmekte ve erişim parolaleri usb bellek içerisine yüklenip kurumun kasasında saklanmaktadır.

5.13. **Teknik Açıklık Yönetimi Politikası:** Bilgi sistemlerinde var olan teknik açıklıkların tespit edilmesi, açıklıkların değerlendirilip önlemlerin ortaya konması, uygun önlemlerin seçilerek uygulanması ve uygulama sonuçlarının gözlenmesine yönelik **Teknik Açıklık Yönetimi Politikası** yürürlüktedir. KÖKSAN'da ihtiyaç duyulduğu durumlarda Penetrasyon Testi yapılır.

5.14. **Görevler Ayırımı :** KÖKSAN'da varlıklarının yanlışlıkla ya da kasıtlı olarak yanlış kullanım riskini azaltmak için yetkilendirmeler kurallara bağlanmıştır.

Kuruluş varlıklarının yanlış kullanımını azaltmak amacıyla çelişen görevler ve sorumluluklar ayrılır.

Bir olayın başlatılması onun yetkilendirilmesinden ayrılır. Bununla birlikte faaliyetlerin izlenmesi, denetim kayıtları ve yönetimin gözetimi gibi diğer kontroller dikkate alınır.

Kullanıcıların yetki kuralları ve görevlerin ayrımı **Kullanıcı Yetki Kuralları ve Görevler Ayrımı Politikası**'nda kapsamlı olarak belirlenmiştir.

Kurumun bilgi varlıklarına erişim için **Erişim Politikası** ve standartlar içinse **Bilişim Kaynakları Kullanım Standartları Politikası** oluşturulmuş ve yayınlanmıştır.

5.15. **Değişim Yönetimi Politikası:** Kurum bilgi sistemlerinde yapılması gereken konfigürasyon değişikliklerinin güvenlik ve sistem sürekliliğini aksatmayacak şekilde yürütülmesine yönelik politikaları belirlemektedir. Değişim yönetimi için **Değişim Yönetimi Politikası** adında ayrı bir politika oluşturulmuştur.

5.16. **Bilgi Sistemleri Yedekleme Politikası:** Bu politika kurumun bilgi sistemleri yedekleme politikasının kurallarını tanımlamaktadır. Tüm kritik bilgi sistemleri ve bu sistemleri işletilmesinden sorumlu çalışanlar bu politika kapsamındadır. Ayrı bir Yedekleme Prosedürü belirlenmemiştir.

5.17. **Kişisel ve Harici Ekipmanların Kullanımı Politikası:** Bu politika kurum çalışanlarının ve üçüncü parti firmaların kendi bilgi işleme ekipmanlarını KÖKSAN bünyesinde yada uzaktan bağlantı yaparak iş amaçlı kullanmasındaki kuralları belirler.

- Prensip olarak KÖKSAN çalışanlarının kendi özel ekipmanlarını iş amaçlı kullanmalarına müsaade edilmez. İstisnai durumlarda bu türden ekipmanların iş amaçlı kullanımı yalnızca uzaktan bağlantı (VPN) altyapısıyla mümkündür.
- Tedarikçi firmaların ekipmanlarının kurum bünyesinde yada uzaktan iş amaçlı kullanılması durumunda BGYS güvenlik gereksinimleri dikkate alınır.
- Bu türden bağlantılarla ilgili tüm kayıt altına alınma gereksinimleri dikkatlice ve noksansız yerine getirilir, aktivite geçmişi (loglar) düzenli bir şekilde takip edilir.
- **Erişim Politikası**, **Bilgi Güvenliği Kullanıcı El Kitapçığı** ve **Bilişim Kaynakları Kullanım Standartları Politikası'**nda öngörülen BGYS gereksinimleri bu türden bağlantılarda aksatmadan uygulanır.

5.18. **Veri Transfer Politikası:** Bu politikanın amacı üçüncü parti kişi ve kuruluşlarla ve kurum içi çalışanlarla bilginin taşınması sürecinde izlenecek yöntemleri belirlemektir.

- Tüm bilgi varlıklarının taşınması ve aktarılması varlık sahibinin bilgisi ve onayıyla mümkündür.
- Taşıma ya da aktarma sürecinde bilgi güvenliği gereksinimleri yerine getirilmeli. Bilginin bütünlüğü, gizliliği ve erişilebilirliğini etkileyebilecek riskler tespit edilerek bu risklerin bertaraf edilmesi yoluna gidilmelidir.
- Aktarma ortamlarında, taşıma kanallarında ve haberleşme tesislerinde güvelik standartlarına uyulmalıdır.
- Kullanılması gereken elektronik bilgi taşıma kanallarının seçiminde (Ör: e-posta, FTP, wetransfer, Dropbox vb.) Bilgi Teknolojileri Bölümünün onayına başvurulmalıdır. Güvenliği onaylanmamış ve bilinmeyen transfer yöntemleri kesinlikle kullanılmamalıdır.
- Verinin güvenli ve istenen şartlarda aktarıldığını temin için İletim, sevk ve alındı kontrolü yapılmalıdır.
- Bilgi transferinde bilgi etiketleme kuralları göz önünde bulundurularak bilgi varlığının

paylaşımında “Genel”, “Dahili”, “Gizli” ve “Kişisel” bildirim etiketlerine göre dağıtımı yada aktarması yapılmalıdır. Örnek “Genel” etiketli bir bilginin dağıtımı yapılabilirken “Dahili” etiketli bilgi varlığının aktarılmasında mutlaka varlık sahibinin, “Gizli” ve “Kişisel” etiketli bilgi varlığı için Varlık Risk sahibinin onayı alınmalıdır. Bu konuda **Bilgi Etiketleme ve İşleme Prosedürü**’ne başvurulmalıdır.

- Bilginin gizlilik ve ifşa edilmemesi anlaşmaları kuruluşun çalışanları ve üçüncü parti firmalarla yapılarak yasal güvence altına alınmalıdır.
- Bilgi transfer sürecinde oluşabilecek her türlü bilgi güvenliği ihlal olayları anında BGYK’na bildirilmeli ve “Bilgi Güvenliği İhlal Bildirimi” kaydı açılmalıdır. Tespit edilen ihlaller **Düzeltici ve Önleyici Faaliyet Formu** ile kayıt altına alınır.
- Bilgi Transferlerinde oluşabilecek her türlü güvenlik ihlali BGYK tarafından hızla ele alınarak önleyici tedbirler acilen hayata geçirilmeli ve kayıt altına alınmalıdır.

5.19. **Risk Yönetimi Politikası:** KÖKSAN’da Risk Yönetimi; Kurumun Stratejik Hedeflerini gerçekleştirme sürecini olumsuz yönde etkileyebilecek risk faktörlerinin belirlenmesi, ölçülmesi ve en alt düzeye indirilmesi sürecidir.

Buna göre kurumun temel risk yaklaşımı;

- BGYS Risk Yönetim Sisteminin üretim tesisi ile iş sürekliğini temin etmek,
- İç ve dış mevzuata uygun olarak tesis edilen Risk Yönetim Sistemini, kurumsal yapının entegre bir parçası haline getirmek,
- Risk yönetimini kurum stratejileri doğrultusunda yapmak, proaktif aksiyonlarla riskleri kabul edilebilir seviyelerde tutmak,
- Riskleri, katılımcı yönetim anlayışı ile tanımlamak ve risk portföyünü devamlı güncellemek,
- Her tehditte fırsatlar, her fırsatta tehditler olabileceği anlayışı ile risklere yaklaşmak,
- Risk tutumunu, değişen şartlar doğrultusunda güncelleyerek, doğru risklerin doğru miktarda alınmasını sağlamak,
- Etkin iletişim ve raporlama ile paydaşlar nezdinde itibar ve güven ortamını tesis etmek,
- Risk yönetim sisteminin performansını ölçmek, risk yönetim sistemi ve riskleri sürekli

iyileştirerek, kurumsal yapıyı dinamik bir yapıda tutmak,

- Değişen ve gelişen şartlar doğrultusunda Risk Politikasını gözden geçirmek ve iyileştirmek.

Bu kapsamda Risk gerek varlık temelli ve gerekse de süreç bazlı olarak ele alınıp tehdit ve açıklıklardan hareketle risk değerlendirmesi yapılır.

Risk Değerlendirmesi yöntemi ve seçilen metodoloji **BGYS Risk Değerlendirme Prosedürü**'nde ele alınmıştır.

5.20. Kriptografik Kontroller ve Anahtar Yönetimi Politikası:

✓ **Giriş:** Veriyi korumanın yollarından biri de şifrelemedir. Hassas bilgiler bilinen ve test edilmiş şifreleme yöntemleri ile saklanmalıdır. Süreç içerisinde kırılması uzun zaman alan algoritmalar daha kısa zamanda çözülebilmektedir, bu nedenle uygulama içindeki algoritmalar zamanla gözden geçirilmeli ve güncellenmelidir.

KÖKSAN'da Kriptografik Kontroller aşağıdaki maksatlarla kullanılır;

- ❖ Gizlilik: Saklanan veya iletilen hassas veya kritik bilgiyi korumak için şifrelemenin kullanılması,
- ❖ Bütünlük/Güvenilirlik: Saklanan veya iletilen hassas veya kritik bilginin güvenilirlik veya bütünlüğünü korumak için sayısal imzaların veya mesaj doğrulama kodlarının kullanılması,
- ❖ İnkar edilemezlik: Bir olay veya faaliyetin oluşumu veya oluşmadığının kanıtını elde etmek için kriptografik tekniklerin kullanılması.

✓ **Uygulama:**

- Personelin gönderdiği maillerde, hiçbir şekilde yönetici, kullanıcı gibi hesap parolaları bulundurulmamalıdır.

- İşletim sistemi üzerinde saklanan kullanıcı ve yönetici hesabı parolalarının kriptolu olarak saklandığı belirli zaman aralıklarında kontrol edilmelidir.
- Sunuculara kriptolu bağlantı ile bağlanılmalı, kripto kullanmayan yöntemler tercih edilmemelidir. Düz metin kullanarak veri alışverişi yapan yöntemlerin kullandığı portlar gerekirse kapatılmalıdır.
- Kriptografik anahtarların korunması, şifrelenmiş bilginin kaybolması, tehlikeye düşmesi veya hasar görmesi durumunda tekrar geri alınması ile ilgili metotları içeren anahtar yönetimi uygulanmalıdır.
- Kriptografi iki adımlık kimlik doğrulama , E-imza ve Web uygulamaları SSL sertifikalarında kullanılmaktadır.

✓ **Anahtar Yönetimi:** Anahtar yönetiminde aşağıda belirtilen ve üzerinde mutabık kalınan standartlar, prosedürler ve güvenli yöntemler seti dikkate alınmalıdır;

- ❖ Web uygulamalarında kullanılan SSL sertifikaları sistem sorumlusu tarafından Muhafaza edilmektedir.
- ❖ SSL sertifikaları süresi dolmadan önce yenilenir ve güncelleme yapılır.
- ❖ Uzaktan şirket ağına bağlanmak için iki adımlık kimlik doğrulama kullanılmaktadır. İki adımlık kimlik doğrulama için fiziksel Token Cihazı veya Mobil Uygulama kullanılmaktadır. Sistem üzerinden kontrolleri ve takibi yapılmaktadır.
- ❖ Güvenli iletişim için gerekli olan yerlerde E-imza kullanılmaktadır. E-imza için kullanılan fiziksel anahtar takibi ve kontrolü varlık envanteri üzerinden yapılmalıdır.
- ❖ Kullanımdan kaldırıldıklarında veya zarara uğratıldığında ve bir anahtar saklama programının parçası olmadıkları durumunda silinir veya imha edilir .

5.21. Bilgi Sistemleri Kabul Edilebilir Denetim Koşulları Politikası:

Amaç: Kurum, bilgi sistemlerine yapılan denetimlerin süreçler üzerinde yapacağı bilgi güvenliği etkilerini azaltmak.

Kapsam: Kurum Bilgi sistemlerine yapılan iç ve dış denetimler.

- Sistemler ve veriye erişim için denetim gereksinimleri konusunda ilgili yönetim ile mutabık olunur.
- Teknik denetim testlerinin kapsamına karar verilir ve kontrol edilir.
- Denetim testleri, yazılım ve veriye sadece okunabilir erişim ile sınırlandırılır.
- Sadece okunabilir erişim dışında kalan erişim için, sistem dosyalarının ayrı bir ortamdaki kopyalarına izin verilir, bu kopyalar denetim tamamlandığında silinir veya denetim dokümantasyon şartları altında bu tür dosyaları tutmak için bir zorunluluk varsa uygun koruma sağlanır.
- Özel ve ek bir işleme için gerekler tanımlanır ve kararlaştırılır.
- Sistem erişilebilirliğini etkileyebilecek denetim testleri çalışma saatleri dışında çalıştırılır.
- Tüm erişimler izlenir ve referans kaydı oluşturmak için kaydedilir.

5.22. Fikri Mülkiyet Hakları Politikası:

Kapsam: Fikri mülkiyet hakları; yazılım veya belge telif haklarını, tasarım haklarını, markaları, patentleri ve kaynak kod lisanslarını kapsar.

Uygulama:

- Tüm çalışanların sorumluluğundadır. Kuruluşumuz ulusal ve uluslararası tüm yasa ve düzenlemelere uymayı taahhüt eder.
- Yazılım ve diğer ürünlerinin yasal kullanımını belirleyen fikri mülkiyet haklarına uyum İnsan Kaynakları **İş Etiği Kuralları Prosedürü**'nde ele alınmıştır.
- Yazılım ve lisanslar satınalmaları telif haklarının ihlal edilmemesini temin etmek için sadece bilinen ve seçilmiş tedarikçilerden alınır.
- Fikri mülkiyet hakları farkındalığını arttırmak için;

- BGYS Farkındalık Eğitimi en az beyaz yaka çalışanlarına anlatılır
- **BGYS Kullanıcı El Kitapçığı** tüm çalışanlara dağıtılır.
- **İnternet Erişim ve Kullanım Politikası**'nda, **E-Posta Kullanım Politikası**'nda ve **Bilişim Kaynakları Kullanım Standartları Politikası**'nda konu vurgulanır.

- Fikri Mülkiyet Hakkının çalışan tarafından ihlali İnsan Kaynaklarının İlgili Disiplin Yönetmeliği kapsamında ele alınır.
- Varlık envanterleri oluşturularak tüm lisanslar ve fikri mülkiyet hakkı kapsamındaki bilgi varlıkları kayıt altına alınır.
- Lisansların, ana disklerin, kılavuzların ve benzerlerinin sahipliğine dair ispat ve deliller muhafaza edilir.
- Kurum bilişim ekipmanlarına yazılım ve lisanslı ürünlerin kuruluşu yalnızca yetkili Bilgi Teknolojileri Ekibi tarafından yapılır.
- Yazılımların ve lisansların üçüncü taraflara transferi veya yok edilmesi **Ekipman İmha Bağış ve Kayıttan Düşme Prosedürü**'nde ele alınır.
- Telif hakkı yasası tarafından izin verilen dışında kitapların, makalelerin, raporların ve diğer belgelerin tam veya kısmen kopyalanmasına izin verilmez.

6. KURALLAR: -

7. KAYITLARIN SAKLANMASI:

7.1. Tüm kayıtlar, **Dökümante Edilmiş Bilgi prosedürü'** ne göre saklanır.

8. İLGİLİ DOKÜMANLAR:

8.1. Dökümante Edilmiş Bilgi prosedürü Prosedürü.

Onaylayan
SİSTEM SORUMLUSU

KONTROLLÜ KOPYADIR...