BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKALARI

İÇİNDEKİLER

P00 BİLGİ GÜVENLİĞİ POLİTİKASI
Genel Bakış

Bu politikanın amacı, hukuka, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklere ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemek için, üst yönetiminin yaklaşımını ve hedeflerini tanımlamak, tüm çalışanlara ve ilgili taraflara bu hedefleri bildirmektir.

2.0 Sorumluluk
Bilgi Güvenliği Politikasının hazırlanması, gözden geçirilmesi ve güncellenmesinden Bilgi Güvenliği Yönetim Temsilcisi (Yönetim Sistemleri Yöneticisi) ve/veya Bilgi Güvenliği Yönetici Yardımcısı olarak atanan Ekip Lideri (Genel Sekreter) sorumludur. Kırşehir Ticaret ve Sanayi Odası (KSTO) Yönetim Kurulu Bilgi Güvenliği Politikasını onaylar ve duyurulmasını sağlar.

3.0 Politika Detayları
3.1. Tanımlar
3.1.1. Bilgi Güvenliği Yönetim Sistemi - BGYS:
Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır.

3.1.2. Bilgi Güvenliği Yönetim Temsilcisi:
Bilgi Güvenliği Yönetim Sistemi'nin operasyonundan ve sürekli iyileştirilmesinden sorumludur. Bilgi Güvenliği Yönetim Temsilcisi, Yönetim Sistemleri Yöneticisidir.

3.1.3. Bilgi Güvenliği Yönetici Yardımcısı:
Bilgi Güvenliği Ekip Lideridir. Bilgi Güvenliği Yönetim Temsilcisi'ne destek olmak ve tüm bilgi güvenliği süreçlerinde Bilgi Güvenliği Yönetim Temsilcisi ile yer almaktan sorumludur. Bilgi Güvenliği Ekibi Toplantılarını düzenler Bilgi Güvenliği Yönetici Yardımcısı, Genel Sekreterdir.

3.1.4. Bilgi Varlığı:
KTSO'nun sahip olduğu, işlerini aksatmadan ve herhangi bir yasal yaptırıma uğramadan yürütebilmesi için önemli olan varlıklardır. Bu politikaya konu olan bilgi varlıkları şunlardır:

- ✓ Kağıt, elektronik, görsel veya işitsel ortamda sunulan her türlü bilgi ve veri
- ✓ Bilgiye erişmek ve bilgiyi değiştirmek için kullanılan her türlü yazılım ve donanım
- ✓ Bilginin transfer edilmesini sağlayan ağlar
- ✓ Bölümler, birimler, ekipler ve çalışanlar
- ✓ Tesis ve Özel alanlar
- ✓ Çözüm ortakları (TOBB, Gümrük ve Ticaret Bakanlığı)
- ✓ Üçüncü taraflardan sağlanan servis, hizmet veya ürün (Tedarikçiler)

3.1.5. Bilgi Varlığının İş Sahibi:

Bilgi varlıklarının üretimi, geliştirilmesi, bakımı, kullanımı ve güvenliğini kontrol etmek için onaylanmış yönetim sorumluluğu bulunan kişi veya varlıkları tanımlar. 'Sahip' terimi, gerçekten varlık üzerinde mülkiyet hakları olan kişi anlamına gelmez.

3.1.6. Bilgi Varlığının Teknik Sahibi:
Bilgi varlıklarının kurum içinde kullanılması için gerekli olan teknik operasyonda sorumluluğu bulunan (işi yapan) kişi veya ekipleri tanımlar.

3.2 Politika
Bilgi kaynakları, tesisler ve cihazlar gibi KTSO açısından büyük önem taşıyan varlıklardır. Bilgi varlıklarını ve kaynaklarını kullanan veya bilgi sağlayan herhangi bir kişi, bilgi varlıklarını korumakla yükümlüdür

Ortak bilgi varlıklarını kullanan tüm çalışanların, gereken duyarlılığı göstermesi ve diğer meslektaşlarını, kurum çalışanlarını ve kurumsal değerleri gözeterek hareket etmesi beklenir.

Kurumsal değerlerin gereği olarak gizliliğe önem verilir, her türlü kişisel bilgi en yüksek güvenlik standartlarına sahip sistemlerle korunur. Bilginin sahibi istemedikçe, yetki verilmedikçe veya yasal gereklilikler oluşmadıkça bilgi paylaşılmaz.

KTSO için tüm bu bilgi varlıkları ve kaynakları içerisinde en kritik olanı, özenle korunması, gizliliğinin sağlanması, ihtiyaç duyulduğu anda erişilmesi gereken bilgi varlıkları, müşteri mülkü ***(MM)***, yönetim kararlarını ***(YK)*** ve Kurum Mülkü ***(KM)***'dür. Bu varlıkları barındıran ***Arşiv ve Server***'dır. İnsan Kaynakları ***(İK)*** ise bilgi varlıklarını yönetir ve aynı zamanda kendisi de bilgi varlığıdır. İnsan kaynaklarına dışarıdan alınan hizmetler için görevli personel de dahildir ve Sistem Sorumlusu olarak tanımlanır. Kurum Mülkü olarak tanımlanan varlıklar, doküman ve bilişim sistemlerinin tamamıdır. Kurumun tüm bilgi varlıkları Bilgi Varlıkları Envanter Listesinde tanımlanır.

Önemli Not: *Server kurulumu ile birlikte tüm terminaller sadece işlem yapmak amacı ile kullanılır ve bilgi tutulmaz. Terminallerde ya da bilgi taşınabilir cihazlarda bilgi tutmak bilgi güvenliğinin ihlali sayılır ve Bilgi Güvenliği Disiplin Talimatı kapsamında yaptırım uygulanır. .*

Bilgi varlıkları ve kaynakları farklı konumlarda veya ortamlarda bulunabilir. Hangi konumda veya ortamda olursa olsun ***yasal şartlar, müşteri (Üye ve Diğer Yararlanıcılar) iletişim gereksinimleri ve kurumsal değerler*** bu varlıkların ve kaynakların kullanımını belirler.

Bilgi güvenliği, sadece bilginin gizliliğinin değil, bütünlüğünün ve kullanılabilirliğinin de sağlanması ile mümkündür. Bilginin gizlilik gerekliliği, sadece yetkilendirme dahilinde gereken bilgi varlıklarına erişim verilmesi anlamına gelir. ***Bilginin bütünlüğü, tüm bilgi varlıklarının tamlığını ve doğruluğunu sağlamayı gerektirir.*** Bilginin kullanılabilirliği, bilgi varlıklarının ihtiyaç duyulduğu anda ulaşılabilir ve kullanılabilir olması anlamına gelir.

Bilginin kullanımı, yerleşimi ve korunması ile ilgili ihtiyaçların karmaşıklığı ve çokluğu, kapsamlı ve geniş bilgi güvenliği süreçlerinin ve politikalarının tanımlanmasını zorunlu kılmaktadır. Bu nedenle

belirlenen süreçler doğrultusunda bilgi güvenliği riskleri, bilgi varlığından sorumlu olan kişiler tarafından değerlendirilir, risklerin önceliği belirlenir ve gereken önlemler alınır.

Arşiv ve Server sunucuların güvenliğinin sağlanması öncelikli olarak ele alınır. Varlık envanterinin ve bu envanterin olası risklerinin önceden belirlenerek müşterilerin güven içinde ve kesintisiz hizmet almaları için vardır.

Karar ve eylemlerde, güvenilir nesnel bilgiler ile teknolojinin tüm olanaklarının kullanılmasına önem ve öncelik verilir. Hareketler sezgilere, duygulara ya da doğru görünene göre değil; bilimsel ve teknolojik gerçeklerin ortaya koyduğu objektif esaslara göre düzenlenir. Bunu sağlamak için bilgi en ileri ve güvenilir kaynaklardan transfer edilir, benimsenir ve mesleki uygulamalar bu doğrultuda yapılır. Kaynaklar verimli kullanılarak teknolojiye ve bilgiye hızlı ve güvenilir erişim için yatırım yapılır, gelişim bu doğrultuda sürdürülür.

Bu nedenle bilgi güvenliği yönetim sisteminin planlama, uygulama, izleme ve iyileştirme adımları ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardına ve bu standardı destekleyen standartlara uygun olarak yürütülür.

3.2.1. Bilgi Varlıklarının ve Kaynaklarının Kullanımı

KTSO'da yürütülen üye ve diğer yararlanıcı hizmetlerinin doğası gereği ve bilgi güvenliği yasası kapsamı dışında kalan bilginin gizliliğinin korunması gerekir. Bilginin hassasiyeti ve güvenliği ile ilgili ihtiyaçlar gözetilirken, aynı zamanda bilgiye ihtiyaç anında hızla ulaşılması büyük önem taşımaktadır. O nedenle, bilgi kaynaklarının değerinin iyi tespit edilmesi, bilginin korunmasını sağlayacak çaba ve maliyetin bilginin hassasiyeti ile orantılı olması gerekir.

KTSO'nun bilgi kaynaklarını kullanarak etik dışı veya yasalara karşı faaliyetlerde bulunmak, hiç kimse için kabul edilemez ve cezai yaptırımları vardır.

Bu politikanın asgari gereği olarak,

- ✓ Verinin kasıtlı olarak değiştirilmesi,
- ✓ Kasıtlı olarak veride hataların oluşmasına veya veri kaybına neden olunması,
- ✓ Bilgi kaynaklarının yasaları ihlal eden bir faaliyet için kullanılması,
- ✓ Bilgi güvenliğinin ihlal edilmesi veya suiistimal edilmesi,
- ✓ Cihazların, yazılımların veya herhangi diğer bir bilgi kaynağının çalınması, tahrip edilmesi,
- ✓ Bilgi kaynaklarının bilişim sistemlerinin performans kaybına sebep olacak şekilde kullanılması,
- ✓ Tesislerin, fiziksel cihazların, ağların tahrip edilmesi kabul edilemez.

Bu ve benzeri faaliyetler ve teşebbüsler disiplin suçu olarak ele alınır, gereken disiplin süreçleri ve yasal süreçler Genel Sekreter ve Yönetim Kurulu tarafından uygulanır. Gerekli olması durumlarda Meclis kararı istenebilir.

Belirtilen tarzda bilgi güvenliği ihlallerinin, ihlal teşebbüslerinin veya bu tür ihlaller ile sonuçlanabilecek zafiyetlerin, tespit edildiği anda zaman kaybetmeden Bilgi Güvenliği Yönetim temsilcisi ve/veya Bilgi Güvenliği Ekip Liderine bildirilmesi gerekir.

3.2.1. Yasal Şartlara Uyumluluk

KTSO Türkiye Cumhuriyeti kanunlarına ve tüm uluslararası kanunlara uymayı kabul ve taahhüt eder. Bilginin saklanması, kullanılması ve ifşasında TCK 5846 ve TCK 5651 olmak üzere tüm kanunlara ve yönetmeliklere uygun hareket eder. KTSO yönetimi, bu kanun ve yönetmeliklere aykırı bir davranışta bulunan çalışanı veya tedarikçisi ile ilgili gerekli suç duyurusunda bulunmakla sorumludur.

4.2.1. Rol ve Sorumluluklar

Bilgi varlıklarının teknik sahipleri bilginin gizlilik bütünlük ve kullanılabilirliğini sağlamak için;

- ✓ Bilgi varlıklarına yetkisiz olarak erişilmesini; bilgi varlıklarının yetkisiz olarak değiştirilmesini veya tahribatını önlemek suretiyle, bilgi varlıklarını korurlar.
- ✓ Operasyonun mümkün olan en kısa hizmet kesintisi ile devam etmesini sağlamak için gerekli süreçlerin tanımlanmasını ve uygulanmasını sağlarlar.
- ✓ Bilgi güvenliği gerekliliklerini gözetirken, ihtiyaç duyulduğunda bilgiye hızla erişilebilmesi için karmaşıklığı ortadan kaldıracak dengeyi kurarlar.
- ✓ Çalışanlarını ve birlikte çalıştıkları üçüncü taraf çalışanlarını bilgi güvenliği gereklilikleri, rolleri ve sorumlulukları konusunda bilgilendirirler ve bilinçlendirirler.

Bütün bu faaliyetlerin kurumsal ISO/IEC 27001:2013 standardı ile uyumlu bir çerçevede ele alınması için, tüm kuruluşun süreç ve hizmetlerini kapsayan bir Bilgi Güvenliği Yönetim Sistemi kurulmuş ve Sistem Yetkilisi (Sözleşmeli Tedarikçi), "Bilgi Güvenliği Yönetim Temsilcisi", Bilgi Güvenliği Ekip Lideri atanmıştır.

4.2.1. Bilgi Güvenliği Ekibi (BGE)

Bilgi Güvenliği Ekibi (BGE) aşağıdaki kişilerden oluşur:

- ✓ Genel Sekreter (Bilgi Güvenliği Ekip Lideri)
- ✓ Yönetim Sistemleri Yöneticisi
- ✓ Üye (Muhasebe Yardımcı Personeli)
- ✓ Üye (Bilgi İşlem Sorumlusu)

Bilgi Güvenliği Ekibi (BGE), ayda bir, Bilgi Güvenliği Ekip Lideri'nin oluşturduğu gündem çerçevesinde periyodik Personel Toplantıları ile aynı zamanda toplanır.

Bunun dışında altı ayda bir Yönetim Kurulu ile toplantılar yapılır ve bu toplantılar aynı zamanda yönetim gözden geçirme toplantılarıdır.

Toplantılarda görüşülen konular aşağıda belirtilen maddeleri içerir, ancak bunlarla sınırlı kalmayabilir, ani gelişen olaylar muhakkak ilk toplantılının gündemine alınır:

- ✓ Bilgi Güvenliği Politikası'nın gözden geçirilmesi
- ✓ Risk Yönetim Metodolojisinin onaylanması

- ✓ Güncel risk raporunun değerlendirilmesi
- ✓ Kabul edilebilir risk seviyesinin üst yönetim tarafından onaylanması
- ✓ Artık risklerin üst yönetim tarafından onaylanması
- ✓ Risk işleme planının üst yönetim tarafından onaylanması
- ✓ Güvenlik ihlal olaylarının değerlendirilmesi
- ✓ İş süreklilik stratejisinin gözden geçirilmesi
- ✓ İş sürekliliği tatbikat sonuçlarının değerlendirilmesi
- ✓ Bilgi güvenliği bilinçlendirme çalışmalarının gözden geçirilmesi
- ✓ İç denetim raporlarının değerlendirilmesi
- ✓ Kurumu etkileyebilecek önemli değişiklikler.

Bu politika KTSO Yönetimi tarafından gözden geçirilmiş ve onaylanmıştır.

P01 BİLGİ SİSTEMLERİNİN GENEL KULLANIM POLİTİKASI

1.0 Genel Bakış

Kurumun amacı, herhangi bir şahıs üzerinde kısıtlayıcı politikalar üretmekten çok açıklık, güven ve bütünlüğe yönelik bir kültür yerleştirmektir. Kurum, bilerek veya bilmeyerek yapılan, yasadışı veya zararlı eylemlere karşı, çalışanların ve kurumun haklarını korumayı amaçlar. Bilişim ile alakalı sistemler, kurumun sahip olduğu değerlerdir. Güçlü bir güvenlik, bütün çalışanların içerisine dahil olduğu bir takım çalışmasıyla oluşturulabilir. Bütün bilgisayar kullanıcıları, günlük aktivitelerini yerine getirebilmek için bu kuralları iyi bilmeli ve uygulamalarının sorumluluğunu taşımalıdır.

Müşteri bilgilerinin güvenliğindeki önem KTSO'nun devamlılığını sağlayan öğelerden biridir. Bu nedenle müşteri memnuniyeti ve daha sağlıklı bir hizmet verebilmek amacıyla bilgilerin paylaşımı ve güvenliği önem taşımaktadır.

2.0 Amaç

Bu politikanın amacı kurum bünyesindeki bilişim cihazlarının uygun kullanımı hakkında taslak oluşturmaktır, güvenli oturum açılması şartlarını sağlamaktır. Uygunsuz kullanım, sisteme Bilgi Güvenliği Ekip Liderinin onayı olmadan erişim sağlayabilecek cihazların yarattığı risk, virüs saldırılarına, ağ sistemlerinin çökmesine veya hizmetlerin aksamasına sebep olabilir ve bunlar yasal yaptırımlara dönüşebilir. Bunun yanında bilgi sistemleri için ayrıcalıklı destek programlarının kullanımına ilişkin kuralları belirlemektir.

3.0 Kapsam

Bu politika kurumun bütün çalışanları ve kurum adı altında çalışan bütün kişiler için geçerlidir. Aynı zamanda kurumun sahip olduğu bütün cihazlar için geçerlidir.

4.0 Politika

4.1 Genel Kullanım Ve Sahip Olma

- ✓ Kurumun güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da kurumun bünyesinde oluşturulan tüm veriler kurumun mülkiyetindedir.

- ✓ Çalışanlar, kişisel kullanımları için bilgi sistemlerinden makul seviyede yararlanabilirler. Kişisel bilgi sistemi kullanım kuralları Bilgi Güvenliği Ekibi tarafından politika ve prosedürler ile düzenlenir.
- ✓ Kullanıcı, kritik olduğunu düşündüğü şifresiz bilgi varlıklarını Bilgi Güvenliği Ekip liderine bildirir.
- ✓ Ağ bakımı ve güvenliği için yetkilendirilmiş kişiler, cihazları, sistemleri ve ağ trafiğini üzerinde düzenli olarak test ve denetimler yaparlar.
- ✓ Kurum, bu politika çerçevesinde terminalleri, ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.
- ✓ Bilgisayarlarda oyun, eğlence, sohbet ve paylaşım amaçlı programlar çalıştırılamaz veya kopyalanamaz.
- ✓ Bilgisayarlar üzerinden, iç yazışma, program ve eğitim belgeleri haricinde dosya alışverişinde bulunulmaz.
- ✓ Birimlerde, bilgi işlem yetkilisi ve ilgili teknik personel dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vb. ayarların mevcut düzenlemeleri hiçbir surette değiştirilemez.
- ✓ Bilgisayarlara hiçbir surette lisanssız program yüklenemez.
- ✓ Gerekmedikçe bilgisayar kaynakları paylaşıma açılmaz, kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilir ve güvenli oturum açılması sağlanır. Bilgisayarların paylaşıma açılması Bilgi Güvenliği Ekip Liderinin izni ile yapılır.
- ✓ Bilgi sistemleri destek programlarının kullanımı yetkisi Sistem Yetkilisine (Sözleşmeli Tedarikçi) aittir. Sistem yetkilisi Her ay yapılan Bilgi Güvenliği Toplantılarından önce destek programlarına ilişkin kontrol raporunu Bilgi Güvenliği Ekip Liderine yazılı olarak iletir.
- ✓ KTSO prensip olarak lisanslı paket programlar kullanır. Ancak, ihtiyaç olunması halinde yazılacak yama yazılım programların kaynak kodlarına erişim sadece Sistem Yetkilisine aittir. Sistem Yetkilisi kurumun talebi doğrultusunda oluşturduğu programın kaynak kodlarının kuruma ait olduğunu kabul eder ve programda yapılan her değişikliği Her ay yapılan Bilgi Güvenliği Toplantılarından önce Bilgi Güvenliği Ekip Liderine yazılı olarak raporlamak.
- ✓ Teçhizatın güvenli yok edilmesi aşamasında; bilgi üretilen, depolanan ya da taşınan teçhizatın içinde bulunan tüm bilgiler güvenli ortama yedeklenir, teçhizatın içi boşaltılır ve formatlanır. İşlemler Bil İşlem Sorumlusu ve/veya Sistem Yetkilisi tarafından yapılır. Yapılan işlem kayıt altına alınır ve Bilgi Güvenliği Ekip Liderine raporlanır.

4.2 Güvenlik Ve Kişiye Ait Bilgiler

- ✓ Bilgi sistemlerinde bulunan kritik bilgilere yetkisiz kişilerin erişimini engellemek için gerekli erişim hakları ***Bilgiye Ulaşım ve Bilgi Kullanımı Yetki Tablosu*** ile tanımlanmıştır.
- ✓ Şifreler güvenli bir şekilde tutulur ve hesaplar 3. kişilerle paylaşılmaz. Sistem seviyeli şifreler 3 ayda bir kullanıcı seviyeli şifreler ise en az 6 ayda bir yeniden şifrelenir.

- ✓ Bütün masaüstü ve dizüstü bilgisayarlar otomatik olarak 10 dakika içerisinde şifreli ekran korumasına geçecek şekilde ayarlanır.
- ✓ Dizüstü bilgisayarlar, güvenlik açıklarına karşı daha dikkatle korunmalıdır. Bios ve işletim sistemi şifreleri aktif hale getirilir. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanır.
- ✓ Dizüstü bilgisayarın çalınması / kaybolması durumunda, durum fark edildiğinde en kısa zamanda Bilgi İşlem Sorumlusu ve BG Ekip Lideri'ne haber verilir.
- ✓ Çalışanlar tarafından haber gruplarına gönderilen maillerde şöyle bir açıklama KTSO tarafından eklenmiştir:
  "Bu elektronik posta ve onunla iletilen bütün dosyalar sadece göndericisi tarafından alması amaçlanan yetkili gerçek ya da tüzel kişinin kullanımı içindir. Eğer söz konusu yetkili alıcı değilseniz bu elektronik postanın içeriğini açıklamanız, kopyalamanız, yönlendirmeniz ve kullanmanız kesinlikle yasaktır ve bu elektronik postayı derhal silmeniz gerekmektedir. KTSO bu mesajın içerdiği bilgilerin doğruluğu veya eksiksiz olduğu konusunda herhangi bir garanti vermemektedir. Bu nedenle bu bilgilerin ne şekilde olursa olsun içeriğinden, iletilmesinden, alınmasından ve saklanmasından sorumlu değildir. Bu mesajdaki görüşler yalnızca gönderen kişiye aittir ve KTSO'nun görüşlerini yansıtmayabilir Bu e-posta bilinen bütün bilgisayar virüslerine karşı taranmıştır".
- ✓ Bütün kullanıcılar, ağın kaynaklarının verimli kullanımı konusunda dikkatli olmalıdır. E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olup ve gerekirse dosyaları sıkıştırmalıdır.
- ✓ Bütün kullanıcılar, kendi bilgisayar sisteminin güvenliğinden sorumludur. Herhangi bir sistemden kaynaklanabilecek kuruma veya kişiye yönelik saldırılardan sistemin sahibi sorumludur.
- ✓ Müşteriye ait hiçbir bağlantı bilgisi (şifre, kullanıcı adı, uzaktan bağlantı adresi vs) mail yolu ile bildirilmemelidir.
- ✓ Müşteri bağlantılarının tutulmakta olduğu program şifreleri bilgi işlem yetkilisinin bulunduğu ekipler dâhillinde yetkilendirilmiş şifrelerle saklanmaktadır. Bu şifreler ilgili ekip liderlerince güncellenip program paylaşıma açılmaktadır.

4.2 Uygunsuz Kullanım

Aşağıdaki eylemler yasaklanmıştır. Kimse, bu uygulamanın dışında değildir. Kurum kaynakları, hiçbir koşulda yasadışı aktiviteler için kullanılamaz.

Sistem Ve Ağ Aktiviteleri

Aşağıdaki aktiviteler, istisnasız olarak yasaklanmıştır. İlgili yetkilendirme BG Ekip Lideri/Genel Sekreter tarafından yapılır.

- ✓ Her türlü yetkisiz kopyalama,
- ✓ Herhangi bir kişi veya kuruma ait, ticari sır, patent, KTSO bilgileri ve yazılım lisansları gibi hakların çiğnenmesi,
- ✓ Zararlı veya kaynağı şüpheli programların ağa veya sunuculara bulaştırılması,

- ✓ Kullanıcı şifrelerinin ve hesaplarının, kullanıcı dışında bir şahısla paylaşılması veya ortak kullanımı,
- ✓ Ağ güvenliğini etkilemek, ağ haberleşmesini bozmak, sistemleri gereksiz meşgul edilmesi,
- ✓ Kurum içerisindeki işlemlerde, kimlik doğrulamalarını aşmaya çalışılması, Kurum bilgilerinin, kurum dışından üçüncü şahıslara iletilmesi,
- ✓ Her hangi bir nedenle ilişiği kesilen personelin KTSO'dan edindiği ve KTSO veya müşterilerine ait bilgileri 10 (On) yıl süre ile kullanımı yasaktır.

E-posta ve Haberleşme Aktiviteleri

- ✓ Kurum E-postalarına güvenliğinden emin olunmayan yerlerden girilmesi,
- ✓ İstenilmeyen e-posta mesajlarının iletilmesi,
- ✓ E-posta başlık bilgilerinin yetkisiz kullanılması veya değiştirilmesi,
- ✓ Zincir e-postaların oluşturulması veya iletilmesi

P02 PERSONEL GÜVENLİĞİ POLİTİKASI

1.0 Genel Bakış

Kurumun bilgi varlıklarının güvenliğinin sağlanması, çalışanlarının bu konuya duyarlı olması, bilinç seviyeleri, kendilerine verilen yetki ve sorumlulukları iyi anlamaları ve yerine getirmeleriyle çok yakından bağlantılıdır.

2.0 Amaç

İlgili personelin seçimi, sorumluluk ve yetkilerinin atanması, eğitilmesi ve iş akdinin feshi gibi konuların bilgi güvenliği ile ilgili boyutunun ne şekilde ele alınacağını bu politika belirler.

3.0 Kapsam

Personel Güvenlik Politikası, tüm çalışanları kapsamaktadır.

4.0 Politika

Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılmalıdır.

- ✓ Kullanıcılara erişim haklarını açıklayan yazılı bildiriler verilmeli ve teyit alınmalıdır.
- ✓ Yetkisi olmayan personelin, kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.
- ✓ Bilgi sistemlerinde sorumluluk verilecek kişinin özgeçmişi araştırılmalı, beyan edilen akademik ve profesyonel bilgiler teyit edilmeli, karakter özellikleriyle ilgili tatmin edici düzeyde bilgi sahibi olmak için iş çevresinden ve dışından referans sorulması sağlanmalıdır.
- ✓ Bilgi sistemleri ihlallerinde, sorumluluk alacak kurum ve tedarikçi, KTSO personeli için güvenlik gereksinim ve incelemeleriyle ilgili koşullar eklenmelidir.
- ✓ Çalışanların gizlilik taahhütleri bulunmalıdır.
- ✓ Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenmelidir.

- ✓ Çalışanlara, telefon görüşmeleri yaparken civardakiler tarafından işitilebileceği veya dinlenebileceği için hassas bilgilerin konuşulmaması hatırlatılmalıdır.
- ✓ Çalışanlara, kamuya açık alanlarda, açık ofis ortamlarında ve ince duvarları olan odalarda gizliliği olan konuşmaların yapılmaması hatırlatılmalıdır.
- ✓ İş tanımı değişen veya kurumdan ayrılan kullanıcılar, bilgi işlem departmanına ilgili bölüm sorumlusu tarafından hemen bildirilmeli ve erişim hakları revize edilmeli veya silinmelidir.
- ✓ Kurum bilgi sistemlerinin işletilmesinden sorumlu personelin, konularıyla ilgili teknik bilgi düzeyini güncel tutması çalışma sürekliliği açısından önemli olduğundan, eğitim planlamaları periyodik olarak yapılmalı, bütçe ayrılmalı, eğitimlere katılım sağlanmalı ve eğitim etkinliği değerlendirilmelidir.
- ✓ Yetkiler, "görevler ayrımı" ve "en az ayrıcalık" esaslı olmalıdır. Görevler ayrımı; rollerin, sorumlulukların paylaştırılması ile ilgilidir ve bu paylaşım sayesinde kritik bir sürecin tek kişi tarafından kırılma olasılığı azaltılır. En az ayrıcalık; kullanıcıların gereğinden fazla yetkiyle donatılmamaları ve sorumlu oldukları işleri yapabilmeleri için yeterli olan asgari erişim yetkisine sahip olmaları demektir.
- ✓ Kritik süreçler tek bir çalışana bağlı bırakılmamalı ve silsile yolu üzerinde, her kritik süreç için o sürece hakim bir çalışan daha bulundurulmalıdır.
- ✓ Çalışanlar kendi işleri ile ilgili olarak bilgi güvenliği sorumlulukları, riskler, görev ve yetkileri hakkında periyodik olarak eğitilmelidir. Yeni işe alınan elemanlar için de bu eğitim, oryantasyon sırasında verilmelidir.

P03 İNTERNET ERİŞİM VE KULLANIM POLİTİKASI

1.0 Amaç

KTSO'nun güvenli internet erişimi için sahip olması gereken standartları belirlemektir.

2.0 Kapsam

İnternetin uygun olmayan kullanımı, kurumun yasal yükümlülükleri, kapasite kullanımı ve kurumsal imajı açısından istenmeyen sonuçlara neden olabilir. Bilerek ya da bilmeyerek bu türden olumsuzluklara neden olunmaması ve internetin kurallarına, etiğe ve yasalara uygun kullanımının sağlanmasını amaçlanmaktadır.

Bu politika KTSO'nun bütün kullanıcılarını kapsamaktadır.

3.0 Politika

Bütün kullanıcılar ve Sistem yöneticileri aşağıdaki internet erişim ve kullanım yönteminden dışarıya çıkmamalıdır.

- ✓ Kurumun bilgisayar ağı erişim ve içerik denetimi yapan bir ağ güvenlik duvarı üzerinden internete çıkacaktır. Ağ güvenlik duvarları kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır.
- ✓ Ağın dışından ağın içine erişimin denetimi buradan yapılır. Güvenlik duvarı aşağıda belirtilen hizmetlerle birlikte çalışarak ağ güvenliğini sağlayabilmelidir.

- ✓ Kurumun ihtiyacı doğrultusunda içerik filtreleme sistemleri kullanılır. İstenilmeyen siteler (kumar, şiddet, oyun, sohbet, facebook, youtube gibi paylaşım siteleri vs.) yasaklanır.
  Not: Kurumun facebook sayfasının yönetimi ve bu sayfalara giriş yetkisi Basın Ve Halkla İlişkiler Sorumlusunun sorumluluğundadır.
- ✓ Kurumun ihtiyacı doğrultusunda saldırı tespit ve önleme sistemi kullanılır. Saldırı tespit ve önleme sistemi (IPS); şüpheli olayları, nüfuz ve saldırıları tespit etmeyi hedefleyen bir sistemdir. IPS, şüpheli durumlarda e-posta veya sms gibi yöntemlerle sistem yöneticisini uyarabilmektedir.
  Not: Server kurulumu ile birlikte Saldırı Tespit ve Önleme Sistemi (IPS) devreye alınacaktır.
- ✓ Anti-virüs gateway sistemleri kullanılır. İnternete giden veya internetten gelen bütün trafik virüslere karşı taranır.
- ✓ Ancak yetkilendirilmiş sistem yöneticileri, internette bütün servisleri kullanma hakkına sahiptir.
- ✓ Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilemez ve dosya indirimi yapılamaz.
- ✓ Üçüncü şahısların kurum internetini kullanmaları Bilgi Güvenliği Ekip Liderinin izni ve bu konudaki kurallar dahilinde gerçekleştirilir.

P04 E-POSTA POLİTİKASI

1.0 Genel Bakış

Kurumda oluşturulan e-postalar resmi bir kimlik taşımaktadırlar. E-posta KTSO'nun en önemli iletişim kanallarından biridir ve bu kanalın kullanılması kaçınılmazdır. Bunun yanı sıra e-posta basitliği ve hızı nedeni ile yanlış kullanıma veya gereğinden fazla kullanıma açık bir kanaldır.

2.0 Amaç

Bu politikanın amacı, KTSO e-posta altyapısına yönelik kuralları ortaya koymaktır.

3.0 Kapsam

Bu politika kurumda oluşturulan e-postaların doğru kullanımını içermektedir ve bütün çalışanları kapsamaktadır.

4.0 Politika

4.1 Yasaklanmış Kullanım

- ✓ 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 bu mesajın derhal silinmesi gerekmektedir.
- ✓ Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.
- ✓ Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemeli. Ayrıca sistem üzerinden otomatik engellenmelidir.

- ✓ Kişisel kullanım için internet'teki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.
- ✓ Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır. Ayrıca otomatik olarak sitem tarafından engellenmelidir.
- ✓ Kullanıcı kodu veya şifre girilmesi istenen e-postalar, sahte e-posta olabileceği dikkate alınarak, bilgi işlem sorumlusuna bildirilmeli ve bilgi işlem sorumlusu gözetiminde silinmelidir.
- ✓ Çalışanlar, uygun olmayan içerikli e-posta (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet hakları içeren malzeme vb.) gönderemezler.

3.2 Kişisel Kullanım

- ✓ KTSO'da kişisel amaçlar için e-posta kullanımı mümkün olduğunca makul seviyede olmalıdır.
- ✓ Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu yüzden şifre kullanılmalı ve e-posta erişimi için donanım /yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.
- ✓ Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplandırmalıdır.
- ✓ Kurum çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesi ve okunmasını engellemekten sorumludurlar.
- ✓ Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir.
- ✓ Elektronik postalar sık sık gözden geçirilmeli, gelen mesajlar uzun süreli olarak genel elektronik posta sunucusunda bırakılmamalı ve bilgisayardaki kişisel klasörlere kaydedilmelidir.
- ✓ E-posta kullanıcılarına ait her türlü değişiklik (emeklilik, işten ayrılma, pozisyon değişikliği vb.), yetki ve şifrelerin yeniden yapılandırılması için bilgi işlem yetkilisine bildirilmelidir.

3.3 Gözlemleme

KTSO çalışanlarının gönderdikleri, aldıkları veya sakladıkları e-postaların mülkiyet hakları KTSO'ya ait olduğundan, yetkili kişiler tarafından haber verilmeksizin denetlenebilirler.

3.4 E-Posta Yönetimi

KTSO E-postaların kurum bünyesinde güvenli ve başarılı bir şekilde iletilmesi için gerekli yönetim ve altyapıyı sağlamakla sorumludur.

3.5 E- Posta Virüs Koruma

Virüs, solucan, Truva atı veya diğer zararlı kodlar bulaşmış olan bir e-posta kullanıcıya zarar verebilir. Bu tür virüslerle bulaşmış e-postalar anti-virüs sistemleri tarafından analiz edilip temizlenmelidir. Bilgi işlem yetkilisi bu sistemin planlı kontrolünden ve çalıştırılmasından sorumludur.

P05 ANTİ-VİRÜS POLİTİKASI

1.0 Amaç

Kurumdaki bütün bilgisayarların efektif virüs algılama ve engelleme standardına sahip olması için gereklilikleri belirlemektir.

2.0 Kapsam

Bu politika KTSOdaki bütün kişisel bilgisayarları kapsamaktadır. Bunlar desktop bilgisayarlar, file/ftp/tftp/proxy vs. sunucularıdır.

3.0 Politika

Kurumun bütün kişisel bilgisayarları anti-virüs yazılımına sahip olmalıdır ve belli aralıklarda düzenli olarak güncellenmelidir. Buna ek olarak anti-virüs yazılımı ve virüs patternleri otomatik olarak güncellenmelidir. Virüs bulaşan makineler tam olarak temizleninceye kadar ağdan çıkarılmalıdır. Sistem yöneticileri anti-virüs yazılımının sürekli ve düzenli çalışması ve bilgisayarların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur. Zararlı programları (solucan, truva atı vs) kurum bünyesinde oluşturmak ve dağıtmak yasaktır. Hiç bir kullanıcı herhangi bir sebepten dolayı anti-virüs programını sistemden kaldıramaz.

Anti-Virüs Prosesi

Virüs problemlerine karşı tavsiye edilen adımlar:

- ✓ Anti-virüs güncellemeleri; her makinenin lokalinde otomatik update şeklinde gerçekleşmektedir. b)
- ✓ Bilinmeyen kişilerden e-posta ile birlikte gelen dosya ve makrolar kesinlikle açılmamalı, hemen daha sonra silinmiş öğelerden tekrar silinmelidir.silinmeli,
- ✓ Spam, zincir ve junk e-postalar silinmelidir
- ✓ Bilinmeyen ve şüpheli kaynaklardan asla dosya indirilmemelidir.
- ✓ Bilinmeyen kaynaklardan gelen taşınabilir bellek ve cd'lere virüs taraması yapılmalıdır.
- ✓ Kritik data ve sistem konfigürasyonları düzenli aralıklar ile yedeklenmeli ve güvenli bir yerde saklanmalıdır.

P06 ŞİFRE POLİTİKASI

1.0 Genel Bakış

Şifreleme bilgisayar güvenliği için önemli bir özelliktir. Kullanıcı hesapları için ilk güvelik katmanıdır.

Zayıf seçilmiş şifreler, ağ güvenliğini tümüyle riske atabilir. KTSO çalışanları ve uzak noktalardan erişenler aşağıda belirtilen kurallar dahilinde şifreleme yapmakla sorumludurlar.

2.0 Amaç

Bu politikanın amacı güçlü bir şifreleme sistemi oluşturulması, oluşturulan şifrelerin korunması ve bu şifrelerin değiştirilme sıklığı hakkında standart oluşturmaktır.

3.0 Kapsam

Bu politika kullanıcı hesabı olan (Bilgisayar ağına erişen ve şifre gerektiren kişiler) bütün kullanıcıları kapsamaktadır.

4.0 Politika

4.1 Genel

- ✓ Bütün sistem seviyeli şifreler (örnek; root, administrator) en az 3 ayda bir değiştirilmelidir.
- ✓ Bütün kullanıcı seviyeli şifreler (örnek; e-posta, web vs.) en az 6 ayda bir değiştirilmelidir. Tavsiye edilen değiştirme süresi her 4 ayda birdir. Bütün şifrelerin oluşturulması, tutanak ile kullanıcılara teslim edilmesi ve güvenli bir ortamda kilit altında tutulması bilgi işlem sorumlusunun yükümlülüğündedir.
- ✓ Bilgi işlem yetkilisi her sistem için farklı şifreler kullanır.
- ✓ Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenemez.
- ✓ Kullanıcı, şifresini 3. Kişiler ile paylaşmaması, kağıtlara ya da elektronik ortamlara yazmaması konusunda eğitilmelidir.
- ✓ Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de kolayca kırılamayacak güçlü bir yapıya sahip olmalıdır.
- ✓ Bir kullanıcı adı ve şifresi aynı anda birden çok bilgisayarda kullanılmamalıdır.
- ✓ Kablosuz bağlantı için misafir modemi şifresi ayda bir değiştirilmelidir.

4.2 Ana Noktalar

A Genel Şifre oluşturma Kuralları

Şifreler değişik amaçlar için kullanılmaktadırlar. Bunlardan bazıları: Kullanıcı şifreleri, Web erişim şifreleri, e-posta erişim şifreleri, ekran koruma şifreleri, yönlendirici erişim şifreleridir. Her türlü şifre seçiminde özen gösterilmelidir.

Zayıf şifreler aşağıdaki karakteristiklere sahiptir.

- ✓ Şifreler sekiz veya daha fazla karakterden oluşmuyordur.
- ✓ Şifrelerde sözlükte bulunan bir kelime vardır.
- ✓ Şifreler ortak değerlere sahiptir.
  - ➢ Ailesinin, arkadaşının, sahip olduğu bir hayvanın veya bir sanatçının ismi,
  - ➢ Bilgisayar terminolojisi ve isimleri, komutlar, donanım veya yazılımlar,
  - ➢ “bilişim” , “Ankara” , “İstanbul” gibi kelimeler,
  - ➢ AaaBb, asdfgh, qwerty, qazwsx, 12332 gibi sıralı harf veya rakamlar,
  - ➢ Herhangi bir dildeki argo, lehçe veya teknik bir kelime,

Güçlü Şifreler aşağıdaki karakteristiklere sahiptir.

- ✓ Küçük ve büyük karakterlere sahiptir. (A-Z, a-z)
- ✓ Hem dijit hem de noktalama karakterleri ve ayrıca harflere sahiptir.(0-9,!,@,&=(,}?,\)
- ✓ En az sekiz adet alfa-nümerik karaktere sahiptir.

B Şifre Koruma Standartları

KTSO bünyesinde kullanılan şifreleri kurum dışında herhangi bir şekilde kullanmayınız. Üçüncü şahıslar ile paylaşmayınız. İlgili şifreler KTSO'ya ait gizli bilgiler olarak düşünülmeli ve değişik sistemler için farklı şifreleme kullanılmalıdır.

Dikkat edilmesi gereken hususlar şunlardır;

- ✓ Herhangi bir kişiye telefonda şifre vermemek!
- ✓ E-posta mesajlarında şifre belirtmemek!
- ✓ Üst yöneticinize şifreleri söylememek!
- ✓ Başkaları önünde şifreler hakkında konuşmamak!
- ✓ Aile isimlerini şifre olarak kullanmamak!
- ✓ Şifreleri işten uzakta olduğunuzda iş arkadaşlarınıza bildirmemek!
- ✓ Uygulamalardaki "şifre hatırlatma " özelliklerini seçmemek!
- ✓ Şifreleri en az 6 ayda bir değiştirmek!
- ✓ Şifrelerin değiştirilip değiştirilmediği yapılan testler ile takip etmek!

C Uygulama Geliştirme Standartları

Uygulama geliştiricileri, programlarındaki güvenlik özelliklerinin sağlandığından emin olmalıdırlar.

- ✓ Bireylerin kimlik doğrulaması işlemi desteklenebilmeli,
- ✓ Şifreleri text olarak veya kolay anlaşılabilir formda saklanmalıdır.

D Uzaktan Erişen Kullanıcılar İçin Şifre Kullanımı

Kurumun bilgisayar ağına uzaktan erişim tek yönlü şifreleme algoritması veya güçlü bir algoritma ile yapılacaktır.

P07 KABLOSUZ İLETİŞİM POLİTİKASI

1.0 Amaç

Bu politika, kablosuz cihazların, onaysız olarak kurumun bilgisayar ağına erişimini engellemeyi amaçlamaktadır. Bu politikanın güvenlik kriterlerine uyan cihazlar, kurumun bünyesinde kullanılabilir.

2.0 Kapsam

Bu politika kurum bünyesinde kullanılabilecek bütün kablosuz haberleşme cihazlarını kapsamaktadır.

Kablosuz veri transferi sağlayabilen herhangi bir cihaz (Bilgisayar, Telefon vb.) bunun kapsamındadır. Kuruma bağlantısı olmayan herhangi bir cihaz veya bilgisayar ağı bu politikanın kapsamı içerisinde değildir.

Kurum bünyesinde kullanılmayan cihazlar KTSO'ya ait Guess (Misafir) modeminden Bilgi Güvenliği Ekip Liderinin yazılı onayı ile kablosuz bağlantı kurabilir.

3.0 Politika

3.1 Onaylanmış Teknoloji

Bütün kablosuz erişim cihazları Bilgi Güvenliği Ekibi tarafından onaylanmış olmalıdır ve belirlenen güvenlik ayarlarını kullanmalıdır.

3.2 Güvenlik Ayarları

- ✓ Güçlü bir şifreleme ve erişim kontrol sistemi kullanılır.
- ✓ Erişim cihazları kolayca erişilebilir bir yerde bulundurulamaz.
- ✓ Erişim cihazları üzerinden gelen kullanıcılar Firewall üzerinden ağa dahildirler.
- ✓ Kullanıcı bilgisayarlarında kişisel firewall yazılımları yüklü olmalıdır.
- ✓ Hem kullanıcılar, hem de erişim cihazları statik IP adresleri kullanmalıdır. Aynı zamanda donanım adresleme kullanılmalıdır
- ✓ Erişim cihazları, bir yönetim yazılımı ile aylık olarak gözlemlenmelidir. Sistemde hackerlar tarafından konulmuş casus bir erişim cihazı olabilir veya mevcut erişim cihazı resetlenmiş olup, kurumun güvenlik politikalarına aykırı bir şekilde ayar yapılmış olabilir.
- ✓ Misafir modeminden kablosuz bağlantının usulsüz ve kontrolsüz kullanımının önlenmesi için her ay Bilgi Güvenliği Ekibi toplantısı sonrası şifresi değiştirilir.

P08 UZAKTAN ERİŞİM POLİTİKASI

1.0 Amaç

Bu politikanın amacı herhangi bir yerden kurumun bilgisayar ağına erişilmesine ilişkin standartları saptamaktır. Bu standartlar, kaynakların yetkisiz kullanımı sebebiyle, kurumun gizli ve hassas bilgilerinin kaybı, kritik süreçlerin kesintiye uğraması veya kurumsal prestijin zarar görmesi gibi olumsuz etkileri minimize etmek için tasarlanmıştır.

2.0 kapsam

Kurumun herhangi bir birimindeki bilgisayar ağına erişebilen tüm çalışanları kapsamaktadır.

3.0 Politika

3.1 Genel

Uzaktan erişim metotları ile kuruma bağlantılarda bilgi sistemlerinin güvenliğinin sağlanması için şifreleme politikasına uyulması önemlidir.

KTSO Çalışanları ofis dışından bağlı bulundukları departman veya müşteri sorumluluklarına göre VPN yaparak kurum networkünde bulunan verilere erişmesi mümkündür.

VPN bağlantısı ile KTSO ile bağlantı kurabilecekleri Bilgi Güvenliği Ekip Lideri/Genel Sekreter belirler.

3.2 Gereklilikler

- ✓ Mümkünse uzaktan erişim güvenliği sıkı bir şekilde denetlenmelidir. Kontrol tek yönlü şifreleme veya güçlü bir passpharase destekli PGP sistemi kullanılmalıdır.
- ✓ Kurum çalışanları hiçbir şekilde kendilerinin login ve e-posta şifrelerini, aile bireyleri ve çalışma arkadaşları da dahil olmak üzere 3. şahıslarla paylaşamazlar.

- ✓ Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri (tedarikçiler) bağlantı esnasında aynı anda başka bir ağa bağlı olmadıklarından emin olmalıdırlar. Kullanıcının tamamıyla kontrolünde olan ağlarda bu kural geçerli değildir.
- ✓ Çalışanlar kurum ile ilgili çalışmalarında kurumun dışındaki e-posta hesaplarını kullanamazlar.
- ✓ Kurum ağına standart dışı erişim isteğinde bulunan organizasyon veya kişiler, Genel Müdür'ün özel izni ile geçici olarak izin verilebilirler.
- ✓ Periyodik olarak yapılan kontrollerle, kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcı kimlikleri ve hesapları kaldırılmalıdır.

P09 KRİZ / ACİL DURUM YÖNETİMİ POLİTİKASI

1.0 Genel Bakış

Kritik süreçlerin izlenmesi, raporlanması, belirlenen önlem ve acil durum faaliyetlerinin uygulanması önemlidir. Kurum çalışanlarının, bilgi güvenliği veya iş sürekliliği ile ilgili acil müdahale gerektiren durumlarda, sorumlulukları dahilinde gerekli müdahaleyi yapabilmelerine yönelik normlar belirlenmelidir.

2.0 Amaç

Bu politika, kurum çalışanlarının bilgi güvenliği ve iş sürekliliği ile ilgili acil müdahale gerektiren durumlarda, sorumlulukları dahilinde gerekli müdahaleyi yapabilmelerine yönelik standartları belirler.

3.0 Kapsam

Acil durumlar yaşanmadan, uygun acil durum hareket planlarının yapılması esastır. Bilgi güvenliğine yönelik tehlike senaryolarından bazıları; sisteme yapılacak direkt saldırılar, zararlı kod içeren programların veya kişilerin sisteme sızması, bilgi hırsızlığı, dışarıdan veya içeriden gerçekleştirilebilecek saldırı öncesi taramalar olarak tanımlanabilir.

4.0 Politika

- ✓ Acil durum sorumluları atanmalı ve yetki ve sorumlulukları belirlenmeli ve dokümante edilmelidir.
- ✓ Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınmalıdır. Örneğin, uygulama veya veritabanı sunucularında, donanım ya da yazılıma ait problemler oluştuğunda, yerel veya uzak sistemden yeniden kesintisiz çalışma sağlanabilmelidir.
- ✓ Kurum bilişim sistemlerinin kesintisiz çalışmasını sağlamak için, pasif sistem çözümleri hayata geçirmelidir. Kurumlar sistemlerini tasarlarken, ne kadar süre iş kaybını tolere edebileceklerini göz önüne almalıdırlar.
- ✓ Acil durumlarda, kurum içi işbirliği gereksinimleri tanımlanmalıdır.
- ✓ Acil durumlarda incelenmek üzere, sistem logları saklanmalıdır.
- ✓ Güvenlik açıkları ve ihlallerinin rapor edilmesi için, kurumsal bir mekanizma oluşturulmalıdır.
- ✓ Yaşanan acil durumlar sonrası politikalar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilmelidir.

- ✓ Güvenlik ihlali yaşandığında, ilgili sorumlulara bildirilmeli ve bildirim süreçleri tanımlanmış olmalıdır.
- ✓ 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 kesintisine yol açabilecek durumlar
  - ➢ Seviye C: Şüpheli durumlar. Yukarıda tanımlı ilk iki seviyedeki durumlara sebebiyet verebileceğinden şüphe duyulan, ancak gerçekliği ispatlanmamış durumlar
- ✓ Acil durumlarda ilgili sorumluya erişilebilmeli, ulaşılamadığında koordinasyonu sağlamak üzere Bilgi Güvenliği Ekip Lideri'ne bilgi verilmelidir. Zarar tespit edilerek süratle daha önceden tanımlanmış acil durum faaliyetleri yürütülmelidir.
- ✓ Bilgi Güvenliği Ekibinin gerekli gördüğü durumlarda, konu hukuksal zeminde incelenmek üzere ilgili makamlara iletilir.

P10 FİZİKSEL GÜVENLİK POLİTİKASI

1.0 Amaç

Bu politika, bilgi varlıkları ve sistemlerinin güvenliği için yeterli koşulların sağlanması amacını gütmektedir.

2.0 Kapsam

Kurumun tesislerinde yer alan bilgi varlıklarına istenmeyen erişimi engellemek için oluşturulan fiziksel güvenlik konularını kapsamaktadır.

3.0 Politika

- ✓ Bilgi varlıkları ve sistemlerinin korunması için fiziksel koşulların oluşturulması önemlidir.
- ✓ Bölümlere ait çalışma alanları üçüncü şahısların girişlerine kapalı olmalıdır, bu sayede kontrolsüz girişler engellenmektedir.
- ✓ Kurumsal bilgi varlıklarının dağılımı ve mevcut bilgilerin gizlilik seviyeleri göz önünde bulundurularak, KTSO'da ayrılan bölümlere (Arşiv, Server) girişler/kullanım yetkilendirilmiştir.
- ✓ Üye haricinde kurum dışı ziyaretçilerin ziyareti çalışma ofisinde yapılır ve ziyaret süreleri en fazla 10 dakika ile sınırlıdır. Üyeler ise çalışma alanlarında karşılanır.
- ✓ Tüm elektronik bilgi varlıkları Server odasında yer almaktadır. Server odası kapısı kilitli olup sadece Bilgi Güvenliği Ekip Lideri, Bilgi İşlem Sorumlusu erişebilir. Sistem Yetkilisi Bilgi Güvenliği Ekip Lideri'nin yazılı izni ile Server Odasına giriş yapılabilmektedir.
- ✓ Server odası, elektrik kesintilerine ve voltaj değişikliklerine karşı korunur, yangın ve benzer felaketlere karşı koruma altına alınmıştır.

P11 SUNUCU (SERVER) GÜVENLİK POLİTİKASI

1.0 Amaç

Bu politikanın amacı, kurumun sahip olduğu sunucunun (server) temel güvenlik standartlarını belirlemektir.

2.0 Kapsam

Bu politika, kurumun sahip olduğu bütün dahili sunucular için geçerlidir.

3.0 Politika

3.1 Sahip Olma ve sorumluluklar

Kurum bünyesindeki bütün dahili sunucuların yönetiminden yetkilendirilmiş sistem yöneticileri (Bilgi Güvenliği Yönetim Temsilcisi ve Bilgi Güvenliği Ekip Lideri'nin izni ile tedarikçiler) sorumludur. Sunucu konfigürasyonları, sadece bu gruptaki kişiler tarafından yönetilecektir.

- ✓ Bütün sunucular, kurumun yönetim sistemine kayıtlı olmalıdır
  En az aşağıdaki bilgileri içermelidir.
  - ➢ Sunucuların yerleri ve sorumluları
  - ➢ Donanım ve işletim sistemleri
  - ➢ Ana görevleri ve üzerlerinde çalışan uygulamalar
  - ➢ İşletim sistemi versiyonları ve yamaları

3.2 Genel Konfigürasyon Kuralları

- ✓ İşletim sistemi konfigürasyonları, kurumun bilgi yetkilisi yapar.
- ✓ Kullanılmayan servisler ve uygulamalar kapatılır.
- ✓ Ayrıcalıklı bağlantılar, teknik olarak güvenli kanallar (IPSEC, SSL, PGP) üzerinden gerçekleştirilir.
- ✓ Sunucular, fiziksel olarak korunmuş sistem odalarında saklanır.

Sunucular üzerine yapılacak erişim mümkün olduğunca farklı portlar üzerinden gerçekleştirilir. Bu sayede her hangi bir atak riskine karşı standart dışı davranıldığı için daha güvenli bir erişim sağlanmış olmakla beraber bu spesifik portların takibi de kolaylaşmıştır.

3.3 Gözlemleme

15 gün öncesine kadar makine imajı dönülebilir. Sunucular üzerindeki loglar ise her sunucunun kendi üzerinde olmak üzere sunucunun kurulduğu günden itibaren saklanır.

Loglar, bilgi işlem sorumlusu tarafından değerlendirilir ve gerekli tedbirler alınır.

3.4 Uygunluk

- ✓ Denetimler, kurum bünyesinde Bilgi Güvenliği Ekibi tarafından belirlenen aralıklarda yapılır.

3.5 İşletim

- ✓ Sunucular, elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda muhafaza edilir.

- ✓ Sunucuların yazılım ve donanım bakımları, 4 aylık sürelerde, bilgi işlem yetkilisi gözetiminde onaylı tedarikçiler tarafından yapılır.
- ✓ Sistem odalarına yetkisiz girişler engellenmiştir.

P12 AĞ CİHAZLARI GÜVENLİK POLİTİKASI

1.0 Amaç

Bu doküman, kurumun ağındaki yönlendirici (router) ve anahtarların (switch) sahip olması gereken minimum güvenlik konfigürasyonlarını tanımlar.

2.0 Kapsam

Kurumun ağına bağlı olan veya bağlanabilen ağ cihazları için geçerlidir.

1.0 Politika

Bütün yönlendirici ve anahtarlar, aşağıdaki konfigurasyon standartlarına sahip olmalıdır.

- ✓ Bilgisayar ağında bulunan tüm cihazların, IP ve MAC adres bilgileri bilgi işlem sorumlusu tarafından muhafaza edilir.
- ✓ Kurumun standart SNMP community stringleri kullanılır.
- ✓ Yönlendirici ve anahtarlar, kurumun yönetim sisteminde kayıt altındadır.
- ✓ Yazılım ve firmware güncellemeleri, test ortamlarında denenir ve mesai saatleri dışında uygulamaya sokulur.
- ✓ Bilgisayar ağının bulunduğu kabinler, aktif cihazlar, CAT-6 aktarma kabloları, cihaz portları etiketlenir.

P13 AĞ YÖNETİMİ POLİTİKASI

1.0 Genel Bakış

Kurumun bilgisayar ağında yer alan bilgilerin ve ağ alt yapısının güvenliği, gizlilik, bütünlük ve erişilebilirlik kavramları göz önüne alınarak sağlanmalı, uzaktan erişim hususunda özel önem gösterilmeli, yetkisiz erişimle ilgili tedbirler alınmalıdır. Ağın güvenliği ve sürekliliğini sağlamak amacıyla, kontroller gerçekleştirilmelidir.

2.0 Amaç

Ağ Yönetimi politikası, güvenlik gereksinimlerini karşılayan kuralları belirlemek ve bilgiye erişimin onayı ve kısıtlanması amacıyla geliştirilmiştir.

3.0 Kapsam

Ağ yöneticileri ve teknik sorumlular, faaliyetlerini Ağ Yönetimi Politikasına uygun şekilde yürütmekle yükümlüdür.

4.0 Politika

- ✓ Ağın kontrol ettiği alan, yönetim ve KTSO Bilgi İşlem çalışma alanları ile sınırlıdır.
- ✓ Ağların ve bağlı sistemlerin, iş sürekliliğini sağlamak için, düzenli testler yapılır.

- ✓ Uzak erişim ağlarının bağlanması, gerekli alt yapı sağlanmadan ve Bilgi Güvenliği Ekip Liderinin yazılı onayı alınmadan yapılamaz.
- ✓ Ağ üzerinde kullanıcının erişeceği servisler / bilgiye erişim kısıtlanmalıdır.
- ✓ Uzaktan teşhis ve müdahale için kullanılacak portlarda, güvenlik önceliklidir.
- ✓ E-posta, tek yönlü dosya transferi, çift yönlü dosya transferi ve etkileşimli erişim gibi uygulamalar, kişilere verilen yetkiler çerçevesinde gerçekleştirilir.
- ✓ Ağ üzerindeki yönlendirmeler, bilgi işlem tarafından kontrol edilir.
- ✓ Bilgisayar ağına bağlı bütün makinelerde, kurulum ve konfigürasyon parametreleri, kurumun güvenlik politika ve standartlarıyla uyumlu olmalıdır.
- ✓ Sistemde tasarım veya geliştirme yapılırken, kurum tarafından onaylanmış ağ ara yüzü ve protokolleri kullanılır.
- ✓ Bilgisayar ağındaki adresler, ağa ait konfigürasyon ve diğer tasarım bilgileri, bilgi işlem tarafından, 3. şahıs ve sistemlerin ulaşamayacağı bir şekilde saklanır.

P14 RİSK DEĞERLENDİRME POLİTİKASI

1.0 Amaç

Ağda, sistem açıklarını tespit etmek ve gerekli tedbirlerin alınmasını sağlamak amacıyla yapılan risk analizleri ile ilgili kuralları belirlemektir.

2.0 Kapsam

Risk analizi, kurum içinde herhangi bir varlık için yapılabilir.

3.0 Politika

Sistemi mükemmelleştirmeyi amaçlayan risk değerlendirme yöntemlerinin geliştirilmesi, uygulanması ve denetlenmesi bilgi güvenliği ekibinin ve bilgi işlemin sorumluluğundadır. Risk analizi raporları Bilgi Güvenliği Ekip Lideri'ne onaylatılır. Risk ve uygunsuzluklar giderilene kadar raporlar Bilgi İşlem Sorumlusu tarafından gerekli fiziksel güvenlik önlemleri alınmış alanlarda muhafaza edilir.

P15 DONANIM VE YAZILIM ENVANTERİ OLUŞTURMA POLİTİKASI

1.0 Amaç

Bu politika, kurumun sahip olduğu donanım ve yazılım envanterinin oluşturulması ile ilgili kuralları belirlemektedir.

2.0 Kapsam

Bu politika, kurum bünyesinde kullanılan bütün donanım ve yazılımları kapsar ve uygulanmasından yetkili ve birim yöneticileri sorumludur.

3.0 Politika

Donanım ve yazılım envanteri oluşturulur ve düzenli olarak güncellenir.

- ✓ Oluşturulan envanter tablosunda şu bilgiler olmalıdır; Sıra No, Varlık İsmi, Varlık Sınıfı, Gizlilik sınıfı, Özellikleri, Sahibi, Bulunduğu Yer, Yedek Durumu, Elde Ediliş Tarihi…

- ✓ Envanter listesi, Bilgi Güvenliği Ekibi tarafından tutulur ve belirli periyotlarla güncellenir.
- ✓ Envanter taramaları, Bilgi İşlem Yetkilisi tarafından düzenli olarak yapılır.
- ✓ Envanter bilgileri, uygun parametrelerle kontrol edilir. Bilgi Güvenliği Ekibi önderliğinde tüm personel, envanter bilgilerindeki eksiklik veya yanlışlıkların ciddi kayıplara yol açabileceğinin bilincinde olmalıdır.

P16 VERİ TABANI GÜVENLİK POLİTİKASI

1.0 Amaç

Kurumun veritabanı sistemlerinin, kesintisiz ve güvenli şekilde işletilmesine yönelik standartları tanımlar.

2.0 Kapsam

Tüm veritabanı sistemleri, bu politikaların kapsamı altında yer alır.

3.0 Politika

- ✓ Veritabanı envanteri, tanımlanır ve dokümante edilir.
- ✓ Veritabanı kullanım şekli belirlenir ve dokümante edilir.
- ✓ Kritik verilere erişim işlemleri (okuma, değiştirme, silme, ekleme) loglanır. Log kayıtlarına, Bilgi Güvenliği ekip liderinin izni olmadan kesinlikle hiçbir şekilde erişim yapılamaz.
- ✓ Veritabanı sistemlerinde tutulan bilgiler sınıflandırılır ve uygun yedekleme politikaları oluşturulur. Yedeklemeden sorumlu sistem yöneticileri belirlenir ve yedeklerin düzenli alınması sağlanır.
- ✓ Yedekleme talimatına uyulur.
- ✓ Veritabanı erişimi, Sistem Güvenliği Prosedürü çerçevesinde oluşturulur.
- ✓ Hatadan arındırma ve geri yedekleme kuralları, "Acil Durum Yönetimi" politikasına uygun olarak oluşturulur ve dokümante edilir.
- ✓ Bilgilerin saklandığı sistemler (Arşiv ve Server), fiziksel güvenliği sağlanmış sistem odalarında tutulur.
- ✓ Veritabanı sistemlerinde yapılacak bakım onarım, yama ve güncelleme çalışmalarından önce, ilgili yetkililer bilgilendirilir.
- ✓ Bilgi saklama medyaları, Bilgi Güvenliği Ekip Lideri'nin yazılı onayı olmadan, kurum dışına çıkarılamaz.
- ✓ Ortaya çıkan beklenmedik durumlarda, destek için önceden belirlenmiş personel ile iletişime geçilir.
- ✓ Veritabanı sunucularına erişim şifreleri, kapalı ve imzalı bir zarfla, çelik kasada saklanır. Zarfın açılması gerektiğinde, Genel Sekretere bildirilir.
- ✓ Veritabanı sunucusuna, sadece admin hakkına sahip olanlar bağlanır
- ✓ Bağlanacak kişilerin kendi adına kullanıcı adı verilir ve yetkilendirme yapılır.
- ✓ Bütün kullanıcıların yaptıkları işlemler, loglanır.

P17 DEĞİŞİM YÖNETİMİ POLİTİKASI

1.0 Amaç

Kurumun bilgi sistemlerinde yapılması gereken konfigürasyon değişikliklerinin, güvenlik ve sistem sürekliliğini aksatmayacak şekilde yürütülmesine yönelik politikaları belirler.

2.0 Kapsam

Tüm bilgi sistemleri ve bu sistemlerin işletilmesinden sorumlu personel, bu politikanın kapsamında yer almaktadır.

3.0 Politika

- ✓ Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümante edilmiştir.
- ✓ Değişiklikler gerçekleştirilmeden önce, Bilgi Güvenliği Ekibi'nin onayı alınır.
- ✓ Sistemde yapılan her değişiklik dokümantasyon üzerinde izlenir.
- ✓ Planlanan değişiklikler yapılmadan önce, yaşanabilecek sorunlar ve geri dönüş planlarına yönelik, kapsamlı bir çalışma hazırlanır ve ilgili yöneticilere bildirilir.
- ✓ Yapılan değişiklikler sonrasında oluşabilecek güvenlik zafiyetleri, Ölçüm Yöntemleri ve Kontrolleri Prosedürü çerçevesinde kontrol edilir.
- ✓ Teknolojik değişikliklerin etkileri, belirli aralıklarla gözden geçirilir.

P.18 AĞ ERİŞİM POLİTİKASI

1.0 Genel Bakış

Kurumun bilgi varlıklarının güvenliğinin sağlanması, çalışanlarının bu konuya duyarlı olması, bilinç seviyeleri, kendilerine verilen yetki ve sorumlulukları iyi anlamaları ve yerine getirmeleriyle çok yakından bağlantılıdır.

Ağ erişiminin kontrolü ile ilgili adımların değerlendirilmesi ve belirlenmesi bu süreçte çok önemlidir.

2.0 Amaç

Ağ erişiminin düzenlenmesi

3.0 Kapsam

Ağ erişim yetkisi olan tüm çalışanları kapsamaktadır.

4.0 Politika

4.1 Erişim Seviyeleri

KTSO ağına ve internet sitesine 5 seviyede erişim mümkündür.

1. Public-Herkese açık. /private (özel) dizini hariç tüm URL`lere salt-okunur erişim.
2. Danışmanlık çalışanları
3. Yazılımcılar
4. Yöneticiler
5. Sistem Yöneticileri

Yetkilendirme Prosedürü
3, 4 ve 5 erişim seviyeleri için personelin Direktörlerin yazılı izin alması gerekmektedir. Yazılı izin, gerekli kullanıcı hesaplarını ve haklarını tanımlayacak olan bir sistem yöneticisine sunulmalıdır.

2. erişim seviyesi tüm yeni çalışanlara, e-posta hesaplarını ve LAN şifrelerini aldıklarında otomatik olarak verilmektedir.

Yetkilerin İptali
2`den 5`e kadar olan erişim seviyeleri için yetkiler, Bilgi Güvenliği Ekip Lideri uygun gördüğünde herhangi bir uyarı yapılmadan kaldırılabilir. Ayrıca acil bir durum söz konusu olduğunda sistem yöneticisi de kaldırabilir. Bu işlem 24 saat içerisinde Bilgi İşlem Yetkilisi tarafından gözden geçirilmeli ve onaylanmalıdır.

ERİŞİM HAKLARI
Yerel Login olma (sisteme giriş)
Sunucuya yerel (konsoldan) login sadece sistem yöneticileri için sağlanmalıdır. Login`lerin amacı sadece site bakımı için olmalıdır.

Ağdan Login olma
Dosya paylaşımı dahil olmak üzere ağ login'lerinin her şekli yasaktır.

Yazar Erişimi
Yazılımcıları ve yöneticilerin doküman ağacında değişiklikler yapmaya hakları vardır. Tüm yetkili erişimler kayıt altındadır. Acil durumlar hariç, yerel login ile doküman ağacında değişiklikler yapmak yasaktır.

Uzaktan Sunucu Yönetimi
İzin yok. Tüm sunucu yönetimi yerel olarak yapılmalıdır.

BAKIM

24x7 çalışma

Ağ, bakım süresi dışında, günde 24 saat, haftada 7 gün erişilebilir olmalıdır. Sistem yöneticileri ana sunucuda problem olduğunda yedek bir sunucuya geçebilecek şekilde hazırlıklı olmalıdırlar.

Yedekler
Yedekleme planına uygun alınmalıdır

İzleme
Bir sistem yöneticisi sunucu sistem log dosyalarını hatalar ve diğer beklenmeyen aktiviteler için izlemekle yükümlüdür. Bir sistem yöneticisi, sistemin gizli bilgilerinin bütünlüğünün tehdit altında olduğuna emin olduğunda server kapatabilme hakkına sahiptir.

P.19 MOBİL CİHAZ POLİTİKASI

1.0 Amaç
Kurumun bilgi sistemlerine erişim sağlayacak mobil cihazların güvenlik ve sistem sürekliliğini aksatmayacak şekilde yürütülmesine yönelik politikaları belirler.

2.0 Kapsam
Tüm bilgi sistemleri ve bu sistemlerin işletilmesinden sorumlu personel, bu politikanın kapsamında yer almaktadır.

3.0 Politika
- ✓ Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümante edilmiştir.
- ✓ Kurum kullanıcılarına ait olmayan mobil cihazlar "Misafir Modeminden" bağlantı kurar.
- ✓ Bilgi sistemlerine mobil bağlantı tanımlamaları yapılmadan önce Bilgi Güvenliği ekip Liderinin yazılı onayı alınır.
- ✓ Sisteme kaydı yapılan Mobil cihazların servera erişim ilk üç ay Bilgi Güvenliği Ekibi tarafından gözden geçirilir.
- ✓ Kurumda taşınabilir bilgisayarlar kullanıcılarına zimmetlenir ve ikinci şahısların kullanımına kapalıdır. İkinci şahısların kullanımı Bilgi Güvenliği Ekip Liderinin yazılı iznine bağlıdır.
- ✓ Taşınabilir bellek sadece yedek almak amacı ile kullanılır. Yedek almaktan sadece Bilgi İşlem Sorumlusu yetkilidir.

P.20 TEMİZ MASA TEMİZ EKRAN POLİTİKASI

1.0 Amaç
Kurumun bilgi varlıklarının üçüncü şahısların ya da bilgiye ulaşma ve kullanma yetkisi olmayanların eline geçmemesi için çalışma alanlarının ve bilgisayar ekranlarının bilgiden arındırılması için güvenlik ve sistem sürekliliğini sağlanmasına yönelik politikaları belirler.

2.0 Kapsam
Tüm çalışma alanları, bilgi sistemleri ve bu sistemlerin işletilmesinden sorumlu personel, bu politikanın kapsamında yer almaktadır.

3.0 Politika
- ✓ Tüm çalışma alanları bilgi varlıklarının sınıflarına bağlı olarak tanımlanmış (MM, KM, YK) muhafaza ortamlarında tutulur.
- ✓ Kağıt ortamda bulunan kamuya açık bilgiler dahi kapaklı dolaplarda tutulur ve kapakları kapalı tutulur.
- ✓ Çalışma masalarında sadece o anda verilen hizmete ilişkin doküman bulundurulur.
- ✓ Kaybedilen bilgi varlıklarından, bilgi varlığını kullanan birey sorumludur ve Bilgi Güvenliği Disiplin Talimatındaki yaptırımları itiraz etmeksizin kabul eder.

- ✓ Bilgisayar ekranları üçüncü şahısların göremeyeceği açı ile çalışma masalarına yerleştirilir.
- ✓ Bilgisayarlar açık bırakıldığında Beş dakika sonra ekran koruyucu moduna geçer. Ekran koruyucu moduna geçen bilgisayar server tarafından sistem ile bağlantısı otomatik olarak kesilir.
- ✓ Bilgisayarlar internette sürekli bağlı kullanılmaz.

21. BİLGİ GÜVENLİĞİ POLİTİKASI ONAYI

1.0 Amaç

Bu form, KTSO Bilgi Güvenliği Politikalarının okunduğu, anlaşıldığı ve onaylandığı dokümandır. Bu formu, Bilgi Güvenliği Ekibi, Yönetim Temsilcisi, Bilgi İşlem Sorumlusu ve ilgili yöneticiler onaylayacaklardır. Genel Müdür ve Yönetim Temsilcisi bu politikaların uygulanabilirliğinden sorumludur.

İzlenecek Prosedür

Aşağıdaki adımlar takip edilmelidir.

- ✓ Bilgi Güvenliği politikasını okuyunuz.
- ✓ Aşağıda belirtilen bölümlere tarih atınız ve imzalayınız.
- ✓ Bu sayfayı ilgili birim amirine iletiniz.