BİLGİ GÜVENLİĞİ POLİTİKASI

İÇİNDEKİLER

1. Giriş

Bu politika; **……** bilgi varlıklarının yönetimini, korunmasını, gizliliğini, bütünlüğünü, dağıtımını ve sadece yetki verilen kişilerce erişilebilirliğini sağlayarak önemli işlevlerinin korunmasını düzenleyen kurallar ve uygulamalar bütününü içermektedir. Bu çerçevede, bilgi güvenliği politikası, tanımlanan politikalar doğrultusunda uygulanacak prosedürlerin amaçlarını tanımlayan en üst düzey doküman niteliğindedir.

2. Amaç

Bilgi güvenliği politika dokümanının amacı grup standartları ve en iyi uygulamalara uygun olarak doğru güvenlik gereksinimlerinin tanımlanması ve şirket bünyesindeki Bilgi Teknolojileri hizmetlerinin güvenli ve yürürlükteki Kanun ve düzenlemelere uygun kullanımının sağlanmasıdır. Dokümanın hedefi şirket ve kullanıcılar için kabul edilebilir seviyede güvenlik tehditlerine karşı korunmasıdır.

3. Kapsam

Söz konusu politika kurumdaki tüm kullanıcıları, geçici personeli, ziyaretçileri, bilgi teknolojileri cihazları ve yazılımlarını kapsamaktadır.

4. Bilgi Güvenliği Hedefleri

Şirketimizin bu politika ile hedefledikleri:

- Şirketimizin sahip olduğu veya tutmakla yükümlü olduğu bilgilerin mevzuata uygun olarak tutarak, şirketin veya çalışanların olası mevzuat ihlalleri nedeniyle idari/adli yaptırımlar ile cezalandırılmasını önlemek.
- şirketin güvenilirliğini ve temsil ettiği makamın imajını korumak,
- Üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak,
- Şirketin temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak

amacıyla Şirket bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi varlıklarının bilgi güvenliğini sağlamayı hedeflemektedir.

5. Rol ve Sorumluluklar

Roller	Sorumluluklar
Bilgi İşlem sorumlusu	• BT altyapı güvenliğinin sağlanmasıyla yükümlüdür. • Güvenlik tehditleri, zafiyet ve risklere karşı plan yapmakla yükümlüdür. • Felaket kurtarma planları yardımcı olmakla yükümlüdür. • Yetki ve erişim haklarının belirlenmesini sağlamakla yükümlüdür. • BT altyapısının Güvenlik Politikalarını desteklemesinin sağlamasıyla yükümlüdür.
Eğitim ve Kalite Sorumlusu	• BT güvenliğini uyarlama ve işletmekle yükümlüdür. • Güvenlik politikalarının desteklenmesiyle yükümlüdür. • Güvenlik politika dokümanlarının uyarlanması ve güncel tutulması konularında yükümlüdür. • Bilgi güvenliği eğitim programlarının gerçekleşmesiyle yükümlüdür. • Bilgi güvenliği olaylarını incelemekle yükümlüdür.
Kullanıcılar	• Güvenlik politikalarına uymakla yükümlüdür. • Olası güvenlik ihlallerini bildirmekle yükümlüdür. • İlgili alanlarda güvenlik gereksinimlerinin belirlenmesinde yardımcı olmakla yükümlüdür. • İlgili alanlarda yetki ve erişim haklarının belirlenmesiyle yükümlüdür. • Kendileri ile ilgili politikaları uygulamakla yükümlüdür.

6. Kısaltmalar

Kısaltma	Tanım
Şirket	
Spam e-posta	Yetkisiz ve/veya istenmeyen mesajların toplu olarak e-posta ile gönderilmesi
Uzaktan Erişim	İnternet veya kiralık hatlar vasıtası ile kurumun ağına erişilmesi.
Risk	Kurumun bilgi sistemlerin gizliliğini, mevcudiyetini ve bütünlüğünü etkileyen faktörlerdir.
Kullanıcı Denetimi	Sisteme erişmek isteyen kullanıcının yetkili olup olmadığını denetleme metodu
Güvenli Kanal	Güçlü bir şifrelemeden oluşan iletişim kanalı.
Uygulama Sunucusu	Dağıtık yapıdaki bir ağda bulunan bir bilgisayarda çalıştırılan sunucu yazılımı. Üç katmanlı uygulamaların bir parçasıdır. Bu üç katman: Kullanıcı arayüzü (GUI), uygulama sunucusu ve veritabanı sunucusudur.
Yetkilendirme	Sisteme giriş izni vermek. Çok kullanıcılı sistemlerde sistem yöneticisi, sisteme girebilecek kişilere giriş izni ve kişilere bağlı olarak da sistemde yapabileceği

Kısaltma	Tanım
	işlemler için belirli izinler verir.
Yedekleme	Ekipmanın bozulması durumu düşünülerek dosyaların veya veritabanının başka bir yere kopyalanması işlemi.
Veritabanı	Kolayca erişilebilecek, yönetilebilecek ve güncellenebilecek şekilde düzenlenmiş olan bir veri topluluğu. Bir veritabanı, satış işlemleri, ürün bilgileri, stoklar ve müşteri bilgileri ile ilgili kayıtları barındırır.
Varsayılan (default)	Kullanıcı bir ayar parametresini veya herhangi bir değeri belirlemediği zaman, uygulamanın kullandığı daha önceden belirlenmiş sabit bir değer veya ayar parametresi.
Şifreleme (encryption)	Veriyi, istenmeyen kişilerin anlayamayacakları bir biçime sokan özel bir algoritmanın uygulanması.
Hacker	Aslen akıllı programcı anlamına gelen bir terim, ancak günümüzde Internet üzerinden bilgisayar sistemlerini çökertmeye çalışan kötü niyetli programcılar için kullanılıyor.
SSL (Secure Sockets Layer)	Ağ üzerindeki güvenli mesaj iletişiminin sağlanması için oluşturulmuş bir program katmanı.
Virtual Private Network (VPN)	Sanal özel ağ. Herkese açık olan iletişim altyapısını kullanan özel bir veri ağıdır. Tünel protokolü ve çeşitli güvenlik prosedürleri ile izinsiz girişlere karşı korunur.
VLAN (Virtual LAN)	Sanal yerel ağ. Birçok farklı ağ bölümüne dağılmış olan, ancak aynı kabloya bağlıymışlar gibi birbiri ile iletişim kurmaları sağlanan, bir veya birkaç yerel ağ üzerindeki cihazlar grubu.

7. Bilgi Güvenliğinin Yönetilmesi

Risk Yönetimi

Şirketin risk yönetimi, bilgi güvenliği risklerinin tanımlanmasını, değerlendirilmesini, işlenmesini kapsamaktadır. Risk değerlendirmesi ve risk yönetim planı, bilgi güvenliği risklerinin nasıl kontrol edildiğini tanımlar ve bu planın yönetiminden ve gerçekleştirilmesinden Eğitim ve Kalite Sorumlusu sorumludur.

Yönetimin Gözden Geçirmesi

Yönetimin gözden geçirme toplantısında bilgi güvenliği ile ilgili aşağıdaki maddelerin görüşmesi yapılır.

- Bilgi güvenliği programı hedeflerinin belirlenmesi,
- Bilgi güvenliği yönetim politika, standart ve prosedürlerinin geliştirilmesi ve gözden geçirilmesinin koordine edilmesi,
- Bilgi güvenliği proje ve aksiyonlarını önerme, gözden geçirme ve önceliklendirme,
- Bilgi güvenliği ihtiyaçlarının iletimi ve aksiyon planı,
- Bilgi güvenliği program farkındalığı oluşturma eğitimlerinin raporları,

- Güvenlik politikalarının yayın ve değişiklikleri yılda bir kez YGG toplantılarında görüşülür.

Bilgi Güvenliği İlkeleri

Şirket bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişen tüm personel:

- Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde Şİrkete ait bilginin gizliliğini sağlamalı,
- Kritiklik düzeylerine göre işlediği bilgiyi yedeklemeli,
- Bilgi güvenliği ihlal olaylarını ve Eğitim ve Kalite Sorunmlusu'na bildirmeli ve DÖF Formu oluşturmalıdır.
- Şirket içi bilgi kaynakları (duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletmemelidir.
- Şirket bilişim kaynakları mevzuata aykırı faaliyetler amacıyla kullanılmamalıdır.

Politikanın İhlali ve Yaptırımları

Bilgi güvenliği politikası, prosedür ve talimatlarına uyulmaması halinde, Şirket personelin imzaladığı Gizlilik Sözleşmesi cezai şart maddesi uygulanacaktır.

8. BT Varlıkları Yönetim Politikası

Amaç

BT varlık yönetimi şirkete değer yaratan fikri mülkiyet (fikir, kavram, know-how, teknik, materyal ve dokümantasyon), insan, teknoloji, bina ve donanım varlıkları ile kurumsal belleği oluşturan süreçler, varlık olarak açık ve net bir şekilde belirlenmesi, sahiplendirilmesi, sınıflandırılması, etiketlenmesi ve güncellenmesi süreçlerini düzenlemektedir.

Kapsam

Söz konusu süreç kurumdaki masaüstü, dizüstü, yazıcı, mobil cihazları ve diğer donanımları, uygulama ve yazılım envanterini kapsamakta olup etkin zimmet sürecinin işletilmesi değerlendirilecektir.

Politika

1. Bilgi teknolojileri envanteri sadece ilgili iş aktivitelerinde atama ve/veya yetkilendirme şeklinde kullanılmalıdır.
2. Kritiklik değeri ve gizlilik seviyesi yüksek olan bilgilerin ilgili personellerin dışında ulaşılamayak olan kilitli dolap veya kasalarda saklanmalıdır.
3. Yazıcı çıktısı alma, fotokopi ile çoğaltma, tarayıcı kullanımı, şirkete içi/dışı sözel (sunum, toplantı, vb.), fiziksel (basılı kopya, vb.) ya da elektronik (e-posta, vb.) yöntemlerle paylaşma, saklama ve imha etme (basılı kopyaların imhası, taşınabilir medyadaki bilgilerin imhası, vb.) kuralları, gizlilik seviyesi esas alınarak belirlenmelidir.
4. Zimmet sahibi kullanıcılar (zimmet formu imzaladığı cihazlar için) BT envanterinin korunmasından ve doğru şekilde kullanılmasından sorumludur.
5. Masaüstü ve dizüstü bilgisayarlar kullanılmadıkları durumda fiziksel güvenlik altına

alınmalıdır. Söz konusu cihazların üstünde gizli bilgiler saklandığı durumda otomatik araçlar kullanılarak bilgiler geri döndürülemeyecek şekilde silinmelidir.

6. Kullanıcılar kendilerine zimmetlenen varlıkları temiz kullanmak ve kazalardan korumak veya uygunsuz şekilde kullanmamakla yükümlüdür.
7. Şirket içindeki varlıklara fiziksel ve uzaktan erişim kısıtlanmalı, doğru şekilde yetkilendirilmelidir. şirketin dizüstü, tablet ve diğer taşınabilir cihazları düzenli olarak envanter takibi yapılmlahıdır.
8. BT envanterinde sadece yetkilendirilen BT teknik personeli yapılandırma değişikliği yapmakla yetkilidir. İfade edilen haricindeki kullanıcıların yazılım ve donanım değişikliği gerçekleştirmesi yasaktır.
9. Dizüstü, akıllı telefon ve tablet benzeri cihazlar çalınmaya karşı korunması sorumluluğu zimmeti yapılan personelin yükümlülüğündedir.
10. Dizüstü, akıllı telefon ve tablet benzeri taşınabilir cihazlardaki veriler çalınmaya karşı şifreleme ve veri imha yöntemleriyle korunmalıdır.
11. Kayıp, çalıntı, zarar, yetkisiz müdahale veya envantere ilişkin benzer güvenlik olayları en kısa zaman Eğitim ve Kalite Sorumlusuna bildirilmelidir.
12. Veri imha süreci Saklama ve İmha Politikasında belirlendiği şekilde gerçekleştirilmelidir. Gizli bilgi taşıyan cihazlar Şirket yöneticisinin gözetiminde fiziksel olarak imha edilmelidir.

9. Kullanıcı ve Erişim Kontrol Yönetim Politikası

Amaç

Kullanıcı ve Erişim kontrol yönetim süreci, BT hizmet ve altyapısına doğru ve güvenli şekilde erişilebilmesi için genel politikaları düzenlemektedir. Bu çerçevede erişim kontrolü kimlik doğrulama, yetkilendirme ve hesap verilebilirlik hususları sistem kritikliğine istinaden değerlendirilmelidir.

Kapsam

Söz konusu süreç kurumdaki iç kullanıcı, geçici personel, ziyaretçi ve dış kaynak erişimlerini ve ilgili hizmetleri kapsamaktadır.

Politika

1. Değerli bilgi taşıyan sistemler şifre koruması sağlayan erişim kontrol sistemiyle korunur.
2. Gizli bilgi taşıyan sistemler iki faktörlü (şifre+SMS) erişim kontrolü ile korunmalıdır.
3. Kaynaklara erişim kişi bazlı yetkilendirme, grup bazlı yetkilendirme gerçekleştirilir.
4. Erişim hakları yetkili kişi tarafından merkezi olarak tanımlanır ve yönetilir.
5. Kullanıcı bilgisayarlarında tutulan Şirket bilgileri ortak dizin altında saklanır.
6. Kullanıcı erişimleri en az yılda 2 kez gözden geçirilmeli ve uygunsuzluklar değerlendirilmelidir.
7. Görevleri veya işleri değişen veya kurumdan ayrılan kullanıcıların erişim hakları aynı iş günü içerisinde kullanıma kapatılır.
8. Geçmişte kullanılmış olan kullanıcı erişim bilgileri başka kullanıcılara verilmez.
9. Yetkisiz erişimlerin takip edildiği kullanıcılara bildirilmelidir. Yetkisiz

erişim teşebbüslerinde Gizlilik Sözleşmesi uygulanır.

10. Tüm kullanıcı adı ve şifreler Şirketin isimlendirme ve şifreleme standardına uygun şekilde yapılmalıdır.
11. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

10. Şifre Kontrol Yönetim Politikası

Amaç

Şifre kontrol yönetim süreci kurumda kullanılan şifrelerin doğru ve güvenli şekilde yönetilmesi için gereksinimleri düzenlemektedir.

Kapsam

Söz konusu süreç kurumdaki iç kullanıcı, geçici personel, ziyaretçi ve dış kaynak erişimlerini ve ilgili hizmetleri kapsamaktadır.

Politika

1. Değerli bilgi taşıyan sistemler şifre bazlı erişim kontrol sistemiyle korunmalıdır.
2. Kullanıcı bilgisayar ve sistem giriş şifreleri, aşağıda bulunan şifre yönetimi standartlarına uygun olarak oluşturulmalıdır.
3. Her kullanıcı sistemlere erişmek için ayrı ve benzersiz kullanıcı adı kullanmalıdır.
4. Tüm kullanıcıların nitelikli (güçlü) şifre kullanmasını zorunlu kılan bir şifre yönetim sistem ve yöntemleri kullanılmalıdır.
5. Parolalarda, başka kişilerin kolayca tahmin edebileceği veya kişiyle bağlantılı bilgileri kullanarak elde edebileceği herhangi bir bilginin (örnek; Adı, soyadı, çocuğunun adı ve doğum tarihleri vb.) kullanılmaması sağlayacak kontrol mekanizmaları tesis edilmelidir.
6. Kullanıcı şifreleri en fazla 90 gün içinde geçerliliğini yitirir ve kullanıcılar en az 10 gün önceden uyarılır.
7. Ayrıcalıklı kullanıcı şifreleri en fazla 30 gün için geçerliliğini yitirir ve kullanıcılar en az 10 gün önceden uyarılır.
8. Kullanıcılar, son kullanılan 3 şifreyi tekrar kullanılamaz.
9. Şifreler rakamlar, özel karakterler ve hem büyük hem küçük harflerden seçilir ve en az 8 karakter uzunluğunda olmalıdır.
10. Başarısız şifre denemeleri dijital olarak kayıt altına alınır ve 3 kere denemenin sonunda hesap kitlenir.
11. Sıfırlanan / yeni verilen şifre ve kullanıcı isimleri kullanıcılara güvenli bir şekilde iletilmelidir. Sıfırlanan şifreler ilk kullanımdan sonra değiştirilmek zorundadır.
12. İfşa olan kullanıcı şifresi derhal değiştirilmelidir.
13. Yeni sistem kurulumlarında kullanılan tedarikçi şifreleri ve kullanıcı adları canlıya geçiş sonrasında değiştirilmelidir.
14. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

11. E-Posta Yönetim Politikası

Amaç

E-posta yönetim süreci Şirketin e-posta sistemlerinin doğru ve güvenli şekilde yönetilmesi için gereksinimleri düzenlemektedir.

Kapsam

Söz konusu süreç kurumdaki mesajlaşma sistemlerini ve ilgili dış kaynak sistemleri kapsamaktadır.

Politika

1. Şirket tarafından kullanıcılara atanan e-posta adresleri ve mesaj alanları sadece iş amaçlı kullanılmalıdır. Kişisel e-posta adreslerinin kullanımı yasaktır.
2. Şirket kaynakları kullanılarak yetkisiz reklam, iş harici mesajlaşma, spam, politik kampanya ve iş süreçlerine aykırı her türlü kullanım yasaklanmıştır.
3. E-posta sistemi gizli bilgi niteliğindeki bilginin iletilmesinde kullanılmayacaktır. Gizli bilginin e-posta kanalında iletilmesi kontrollü ve şifreli şekilde yapılmalıdır.
4. Şirket e-posta sistemleri, saldırgan, ırkçı, müstehcen veya kanun ve yönetmeliklere aykırı amaçlarda kullanılmamalıdır.
5. Şirket e-posta sisteminin kullanımı personel kurumda çalışırken aktif olmalıdır. İlişiğin kesilmesi ve işten ayrılma durumlarında kullanıcı hesapları pasifleştirilmelidir.
6. Kullanıcılar e-posta sistemlerini kendilerine atanmış benzersiz kullanıcılar aracılığıyla giriş yapmalıdır.
7. Özel inceleme ve soruşturma durumlarında Bölge şirkete e-postaların içeriğine erişim yetkisine sahiptir.
8. Kurumsal e-posta adreslerine erişimler güçlü şifrelerle korunmalıdır. Şifre yönetimi şirketin şifre yönetim standardına uygun şekilde gerçekleştirilmelidir.
9. Eklenti boyutları kurumda tanımlanan standartlara uygun şekilde ilgili profillere atanmalıdır. Söz konusu kontrollerin otomatize yöntemler aracılığıyla gerçekleştirilmesi sağlanmalıdır.
10. Virüs ve zararlı yazılımları tespit eden sistemler kullanıcı PC ve sunucuların en yüksek e-posta güvenliğini sağlayacak şekilde konumlandırılmalıdır.
11. Kurumsal e-posta kutuları yedeklemesi merkezi olarak Sistem Yöneticisi tarafından yapılmalıdır.
12. Dış kaynak firma ve üçüncü şahıslarla yapılan yazışmalarda Şirket bilgisi paylaşılmamalıdır. Paylaşıldığı hallerde Gizlilik Sözleşmesi uygulanır.
13. E-postaların Şirket dışındaki e-posta adreslerine yönlendirilmesi yasaktır.
14. Kullanıcıları Şirket dışında e-posta kullanma durumunda şirketin belirlemiş olduğu web erişim adresinden bağlantı kurabilir.
15. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

12. İnternet Erişim Yönetim Politikası

Amaç

İnternet erişim yönetim süreci şirketin kaynakları kullanılarak gerçekleştirilen internet erişimlerinin doğru ve güvenli yapılması için gereksinimleri düzenlemektedir.

Kapsam

Söz konusu süreç Şirket ağı kullanılarak gerçekleştirilen internet bağlantılarına ilişkin düzenlemeleri kapsamaktadır.

Politika

1. Tüm kullanıcılar kısıtlı şekilde internete erişebilir. şirket tarafından aşağıdaki yasaya göre kıstlanan web siteleri Ağ Gecidi uygulamasıyla kontrol edilmektedir.
2. 5651 numaralı "İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul Ve Esaslar Hakkında" konulu yönetmelik kapsamında yasaklanan kategorilerdeki web sitelerine giriş engellenmelidir. Bu çerçevede 26.9.2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan aşağıdaki kanun maddelerine aykırı siteler yasaklanacaktır:
    a. İntihara yönlendirme (madde 84),
    b. Çocukların cinsel istismarı (madde 103, birinci fıkra),
    c. Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),
    d. Sağlık için tehlikeli madde temini (madde 194),
    e. Müstehcenlik (madde 226),
    f. Fuhuş (madde 227),
    g. Kumar oynanması için yer ve imkân sağlama (madde 228),
    h. 25.7.1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun
3. Kullanıcılar, Şirket tarafından sunulmuş olan internet erişim, elektronik ve anlık mesajlaşma hizmetini şirketin belirlediği politikalar uyarınca iş amaçlı olarak kullanmalıdır.
4. Kullanıcılar internet erişimlerinde Şirket kültür ve saygınlığına uygun hareket etmekle yükümlüdür.
5. İnternet trafiği güvenlik duvarlarında gözlemlenmelidir. Oluşacak saldırı veya tacizler Sistem Yöneticisi'ne bildirilmelidir.
6. İnternet erişimi yoluyla elde edilen verilerin kullanımında, fikri mülkiyet hakkı kısıtlamalarına, kişisel verilerin korunması ilkelerine, gizlilik esaslarına, kullanım şartlarına ve Mevzuat hükümlerine uygun davranılmalıdır.
7. Sosyal paylaşım sitelerine erişim izni verilmemektedir.
8. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

13. Zararlı Yazılımlara Karşı Korunma Yönetim Politikası

Amaç

Zararlı yazılımlara karşı korunma yönetim süreci Şirket ağ ve sisteminin virüs ve benzeri zararlı yazılımlardan korunması için yapılan güvenlik kural ve uygulamalarını düzenlemektedir.

Kapsam

Zararlı yazılımlara karşı korunma yönetim süreci kurumda kullanılan sunucu, masaüstü bilgisayar, dizüstü bilgisayar, akıllı telefonlar, tablet ve diğer mobil cihazları kapsamaktadır.

Politika

1. Şirkette olan tüm bilgisayar, notebook ve tabletlerde lisanslı antivirus sistemi kullanılmalı ve en son sürümüyle güncellenmelidir.
2. Şirketin ağına bağlanan tüm bilgisayar ve cihazlarda gerçek zamanlı koruma sağlayan antivirüs kurulu olması zorunlu olmakla beraber virus koruma devre dışı bırakılamaz.
3. Şirketin ait sunucu ve bilgisayarlar merkezi olarak yönetilen ve onaylı antivirüs sistemini kullanmalıdır. Şirket dışında bulunan gezici cihazlar Şirket ağına bağlandığında antivirüs taramaları yapılmalıdır.
4. Antivirüs uygulaması düzenli ve otomatik olarak virüs güncellemelerini gerçekleştirmelidir.
5. Şirket ağına bağlanma mecburiyeti olan ziyaretçi bilgisayarlarında antivirüs, vb. güvenlik önlemlerinin alındığı teyit edilmelidir.
6. Taşınabilir bilgi depolama ortamlarında (CD/DVD, flaş bellek, harici disk, vb.) bağlantı kısıtlanmıştır.
7. Tüm bilgisayarlar ve ortamlar, belirlenmiş zaman aralıklarında otomatik olarak taranmalıdır.
8. Kötü niyetli yazılım ve zararlı/mobil kod içerebilecek dosya türleri ve dosya türlerini barındıran kaynaklar çalıştırılmadan önce mutlaka antivürüs sisteminde taranarak güvenli olduğuna emin olundukran sonra dosya açılmalıdır.
9. Taşınabilir cihazların dış ağdan erişimlerinde maruz kalabileceği saldırıları önlemek amacıyla kişisel güvenlik duvarları aktif olarak çalışmalıdır.
10. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

14. KVKK Uyumunun Sağlanması Politikası

Amaç

7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu özel hayatın gizliliğini, kişilerin temel hak ve özgürlüklerini korumayı ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemeyi hedeflemiştir. Bu Politika ile kanuna uyum hedeflenmiştir.

Kapsam

Söz konusu süreç Şirket tarafından üretilen, işlediği, sahibi olduğu veya yönettiği tüm bilgileri kapsamaktadır.

Politika

1. Kişisel verilerin Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenmesi sağlanmalıdır.
2. İlgili kişinin haklarını korunmalıdır; Kişisel Verileri hukuka aykırı olarak işlenmesi ve erişilmesin önlemelidir, kişisel verilerin muhafazası sağlanmalıdır.

3. Kişisel Veri Envanteri oluşturulmalıdır.
4. Kişisel verilerin yurtdışına aktarılması, silinmesi, yok edilmesi veya anonim hale getirilmesi kanuna uygun olarak yönetilmelidir.
5. Mevcut sözleşmeler (Çalışan, Katılımcı, Müşteri, Taşeron vb.) kanunla uyumlu hale getirilmelidir.
6. Veri Sahibini aydınlatma ve açık rıza alma yükümlülükleri yerine getirilmelidir.
7. Veri sahiplerinin başvurularını değerlendirmek ve sonuçlandırma melkanızması olmalıdır.
8. Organizasyon yapısını oluşturulmalıdır.
9. Veri Sorumluları Sicili'ne (VERBİS) kayıt işlemi yapılmalı ve gerektiğinde güncellenmelidir.
10. Kişisel Veri Güvenliğine sağlanmasına yönelik olarak idari ve teknik tedbirlerin alınması sağlanmalıdır.
11. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

15. Uzaktan Erişim Yönetim Politikası

Amaç

Uzaktan erişim yönetim süreci, şirketin iç kaynaklarına dışardan gerçekleştirilen bağlantıların güvenli şekilde gerçekleşmesi için gerekli hususların düzenlemektedir.

Kapsam

Şirket iç kaynaklarına erişme ihtiyacı bulunan kullanıcı ve cihazları kapsamaktadır.

Politika

1. Şirketin iç kaynaklarına dışarıdan erişimlerin gerçekleşmesi için kullanıcının gerekli yetkiye sahip olması gerekmektedir. Dışarıdan erişim talebi şirket yetkilisinin onayıyla verilir.
2. Şirket iç kaynaklarına güvensiz ağdan erişimler iki faktörlü kimlik doğrulaması sağlayan SSL-VPN aracılığıyla gerçekleştirilir.
3. Uzaktan erişim sağlayan kullanıcılara, güvenli bir ağa erişinceye kadar geçtikleri her bir ağ bileşeninde (düğümde) kimlik doğrulaması yapılmalıdır.
4. Ağa gelen tüm dış erişimler belirlenerek kontrol edilmeli, onaylanmalı, izlenmeli ve Şirketin belirleyeceği süre boyunca saklanmalıdır.
5. Uzaktan erişim için kullanıcı kayıt ve silme süreci Şirket kullanıcı yönetim sürecine uygun olarak gerçekleştirilmelidir.
6. Ağ tasarımı, dışarıdan gelen trafiği, sadece ağın belirli kısımlarıyla sınırlandıracak ve tanımlı giriş noktalarına yönlendirecek şekilde yapılandırılmalıdır.
7. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

16. Dış Kaynak Kullanım Yönetim Politikası

Amaç

Dış kaynak kullanım yönetim süreci tedarikçiden güvenli hizmet alınabilmesi için tanımlanacak

minimum güvenlik gereksinimlerini düzenlemektedir.

Kapsam

Politika, şirketin BT hizmetlerini, fonksiyonlarını ve süreçlerini dış kaynağa devrettiği yapı ve tedarikçiyi kapsamaktadır.

Politika

1. Riskler ve finansal etki değerlendirildikten sonra dış kaynak kullanımı gerçekleştirilmelidir.
2. Dış firmayla çalışılmadan önce paylaşılacak bilgilerini gizliliğini korumak amacı ile Gizlilik Taahhütnamesi imzalatılır.
3. Hizmet sağlayıcı seçilirken itibar, benzer hizmetlerde deneyim, teklif ve güvenceleri dikkate alınır.
4. Tedarikçiler her yıl düzenli olarak değerlendirilmeli ve performansı ölçülmelidir.
5. Şirket ile servis sağlayıcı arasında alınacak hizmeti ve hizmet seviyelerini tanımlayan bir sözleşme imzalanır.
6. Şirkete hizmet sağlayacak servis sağlayıcılar şirketin bilgi güvenliği standartlarına uyumlu olacağını taahhüt etmelidir. Şirket bilgilerine erişim ve bu bilgileri kullanımında servis sağlayıcı standart ve talimatları ile tüm güvenlik kuralları ve gereklilikleri ayrıntılı olarak Gizlilik Sözleşmesinde belirtilir.
7. Servis sağlayıcılar kendi çalışanlarına, hizmet verdikleri şirketin bilgi güvenliği kurallarına uygun davranmaları konusundaki kişisel sorumluluklarını resmi olarak bildirmekle ve bu sorumluluklara uyumu garanti altına almakla yükümlüdür.
8. Servis sağlayıcı tarafından gerçekleştirilen elektronik veri akışı, elektronik ticaret ve elektronik haberleşme için ticari ve yasal yükümlülükler Gizlilik Sözleşmesinde belirtilir.
9. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

17. Kabul Edilebilir Kullanım Politikası

Amaç

Kabul Edilebilir Kullanım Politikası, şirketin bilgi ve iletişim varlıklarının iş amaçlarına uygun kullanılması için gerekli kuralları düzenlemektedir.

Kapsam

Tüm Şirket çalışanları, geçici görevliler ve şirketin bilgi varlıklarına erişimine izin verilmiş olan diğer Şirket/kuruluş/şirket çalışanları bu politikada belirtilen kurallara uymak zorundadır. Personel Kaynakları birimi personelin işe girişinde bu politika ve kuralları imza karşılığı tebliğ eder.

Politika

1. Kullanıcı, şirketin ait BT Güvenlik Politika ve prosedürlerine uymakla yükümlüdür.
2. Şirketin bilgi ve haberleşme sistemleri ve donanımları (İnternet, e-posta, telefon, faks,

bilgisayarlar, mobil cihazlar ve cep telefonları da dâhil olmak üzere) Şirket işlerinin yürütülmesi için kullanılmalıdır. Bu sistemlerin yasa dışı, rahatsız edici, Şirketin diğer politika, standart ve rehberlerine aykırı veya şirkete zarar verecek herhangi bir şekilde kullanımı bu politikanın ihlal edilmesi olarak değerlendirilecektir.

3. Şirket, bu sistemleri ve bu sistemlerle gerçekleştirilen aktiviteleri izleme, kaydetme ve periyodik olarak denetleme hakkını saklı tutar.
4. Şirket, internet kaynakları öncelikli olarak resmi ve onaylı Şirket işlerinin gerçekleştirilmesi için kullanılır.
5. Kullanıcılar kendi kullanıcı hesaplarıyla internet üzerinde gerçekleştirilen tüm işlemlerden sorumludur. Bunun için kullanıcılar kimlik bilgilerini uygun şekilde saklamalı ve başkaları ile paylaşılmaz.
6. Şirket kaynakları uygunsuz içeriği saklamak, bağlantı olarak vermek, yer imi olarak eklemek, erişmek ve göndermek için kullanılmaz.
7. Şirketin resmi işlerinin yürütülmesi dışında sohbet gruplarına, forumlara, elektronik haber gruplarına katılmak yasaktır.
8. Kullanıcıların sistemi kullanmak için gerekli kimlik bilgilerini başkalarına vermeleri yasaktır.
9. Şirketin kritik bilgisinin ortaya çıkmasını veya Şirket servislerinin ulaşılamaz hale gelmesini sağlayacak tüm aktiviteler yasaktır.
10. İndirilen tüm yazılımlar kullanılmadan önce zararlı kodlara ve virüslere karşı taramadan geçirilir.
11. Şirket, kullanıcının internet sisteminde gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü partilerle, emniyet kuvvetleriyle veya yargıyla kullanıcının izni olmadan paylaşma hakkını saklı tutar.
12. Telefon konuşmaları sırasında karşı tarafın bilgilendirilmeden telefon hoparlörü, ses ve video kayıt cihazları kullanılamaz. Kullanılması gereken durumlarda görüşme yapılan kişiden izin alınır.
13. şirkete ait yazılımların izinsiz çoğaltılması yasaktır.
12. Kabul Edilebilir Kullanım Politikasına ve burada belirtilen diğer politika ve prosedürlere uymayanlar hakkında disiplin süreci başlatılır ve ilgili Gizlilik Sözleşmesi maddeleri uygulanır.
14. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

18. BT Risk Yönetim Politikası

Amaç

BT Risk Yönetim süreci, BT risklerinin etkin takip edilebilmesi için gerekli kuralları düzenlemektedir.

Kapsam

BT Risk Yönetim Süreci Şirkette kullanılan sunucu, masaüstü bilgisayar, dizüstü bilgisayar ve diğer cihazları kapsamaktadır.

Politika

1. Risk değerlendirme yöntemi varlık esaslı olarak uygulanır. Kritiklik değeri açısından "Kritik" ve "Yüksek" değere sahip varlıklar risk değerlendirme kapsamında bulunur.
2. Risk değerlendirme yöntemiyle, varlıklar için geçerli olan tehditler saptanmalı, tehditlerin gerçekleşmesine sebep olabilecek zayıflıklar belirlenerek ve ilgili varlıklar için mevcut kontroller değerlendirilir.
3. Risk Yönetim Prosedüründe riskin gerçekleşme olasılığı, riskin boyutu ve riskin Şirkete üzerinde etkileri birlikte değerlendirilerek risk düzeyinin belirlenir.
4. Kabul edilebilir risk düzeylerine ilişkin kriterler, risk değerlendirme yönteminde tanımlanır ve yönetim tarafınca imzalanır.
5. Kabul edilemez risk düzeyine sahip varlıklar için ilave kontroller ve sorumluların belirlendiği aksiyon planları hazırlanır üst yönetimin onayına sunulur.
6. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

19. BT Güvenlik Olay Yönetim Politikası

Amaç

BT Olay Yönetim süreci, şirketin teknoloji, bina ve donanım varlıkları ile kurumsal belleği oluşturan süreçler ile ilgili oluşmuş veya oluşabilecek olaylarının yönetilmesi için gerekli güvenlik kuralları düzenlemektedir.

Kapsam

BT Olay Yönetim Süreci, Şirkette kullanılan sunucu, masaüstü bilgisayar, dizüstü bilgisayar ve diğer cihazları kapsamaktadır.

Politika

1. Bilgi güvenliği olaylarının iç ve dış iletişim kuralları, düzeltici / önleyici aksiyonlar ve takip çalışmaları yer almaktadır.
2. Süreç takibi atanan sorumlu personeller tarafından yapılmaktadır.
3. Düzeltici ve Önleyici (DOF) Kayıt Formu tutukur.
4. Bilgi güvenliği ihlali gerçekleştiğinde, bu ihlali gerçekleştirerek kurumu doğrudan ve/veya dolaylı olarak zarara uğratan kişi ve/veya kuruluş aleyhine hukuki yollara başvurulmasının söz konusu olduğu durumlarda kanıtlar, hukuka uygun ve gerektiği şekliyle toplanır, saklanır vesunulur.
5. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

20. Ağ Güvenlik Yönetim Politikası

Amaç

Ağ Güvenlik Yönetim Politikası, Şirketin iç/dış ve kablolu/kablosuz ağ hizmetlerinin, güvenlik

özellikleri, hizmet düzeyleri ve yönetim gereklilikleri saptanması, uygun kontrollerle yönetilmesi için gerekli güvenlik kuralları düzenlemektedir.

Kapsam

Ağ Güvenlik Yönetim Süreci, Şirketin, iç/dış ve kablolu/kablosuz ağ hizmetlerini ve ilgili BT süreçlerini kapsamaktadır.

Politika

1. Ağ cihazlarının ayarlarındaki değişiklikler ve hizmet seviyeleri ile bu seviyelerle ilgili izleme faaliyetleri tanımlanmalıdır.
2. Ziyaretçiler ağ hizmetlerinden belirlenmiş güvenlik kontrolleri ve onay sonrasında faydalanabilir.
3. Ağ cihazları (router, hub, bridge, switch ve güvenlik duvarı, vb.) ile ilgili tanımlama ve yapılandırma portlarına sadece yetkili personel şifre kontrolüyle erişim sağlamalıdır.
4. İlk kurulum sonrasında ağ cihazlarındaki, üretici tarafından sağlanan varsayılan parolalar ve parametrelerdeğiştirilmelidir.
5. Kablosuz misafir ağlarında giriş şifreli yapılmalı ve hergün şifreler otomatik olarak değişmelidir.
6. İç ağda internete açık sunucular bulunmamalıdır. İş ihtiyaçları konumlandırılması durumunda ise genel ağdan izole edilmelidir.
7. Güvenlik duvarı kuralları, suiistimale açık iletişim protokollerini yasaklayacak şekilde düzenlenmelidir.
8. Ağ cihazları ARP Poisining ve benzeri ağ saldırılarını engelleyecek şekilde düzenlenmelidir.
9. Güvenlik duvarı kurallarında ANY kaynak veya ANY hedef tanımlamalarının yapılmaması sağlanmalıdır. Yetkilendirmeler IP bazlı yapılmalıdır.
10. Güvenlik duvarı kuralları her 6 ayda gözden geçirilmeli ve sonuçlar raporlanmalıdır.
11. Şirket ağına kablolu ve kablosuz protokoller kullanılarak yetkisiz erişimlerin gerçekleştirilmesini engelleyecek güvenlik kontrolleri uygulmalıdır.
12. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

21. Veritabanı Güvenlik Yönetim Politikası

Amaç

Veritabanı Güvenlik Yönetim süreci, Şirket veritabanlarına erişim ve yönetim süreçlerinin bütünlük, güvenlik, hesap verilebilirlik ve erişilebilirlik ilkelerine uyumlu şekilde yürütülmesi için gerekli güvenlik kuralları düzenlenir.

Kapsam

Veritabanı Güvenlik Yönetim Süreci Şirkete ait tüm veritabanlarını kapsamaktadır.

Politika

1. Veritabanları kullanıcı ve diğer sunuculardan izole alt ağda konumlandırılmalıdır. Ağ güvenliği standartlarına uygun şekilde alt ağ konfigüre edilmelidir.

2. İlk kurulum sonrasında veritabanında, üretici tarafından sağlanan varsayılan parolalar ve parametreler değiştirilmelidir.
3. Profil bazlı yetkilendirme standardı benimsenmelidir. Profiller iş süreci ihtiyaçlarına uygun olarak belirlenmelidir.
4. Yönetici hesapları ve ayrıcalıklı hesaplar hesap verilebilirlik prensibi esas alınarak kişiye atanarak tanımlanmalı, yönetici kullanıcıların şifreleri kasada saklanmalıdır.
5. Veritabanı logları sürekli aktif olarak çalışmalı ve düzenli olarak gözden geçirilmelidir.
6. Şifre yönetim standardına uygun şekilde karmaşık şifre uygulanmalıdır.
7. Veritabanlarına uzaktan erişim yapılmamalıdır. Sadece özel izinli kullanıcıların uzaktan bağlantı yapmaya yetkisi olmalıdır.
8. "Gizli Bilgi" olarak sınıflandırılan verilere sadece özel yetkili kişiler erişebilmelidir.
9. Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.
10. Bilgi saklama medyaları Şirket dışına çıkartılmamalıdır.
11. Test veritabanlarında "Gizli Bilgi" içerikli bilgi barındırılmamalıdır. Barındırılması gerektiği hallerde canlı sistemlerle aynı yetkilendirme kural ve profiller kullanılmalıdır.
12. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

22. Fiziksel Güvenlik Yönetim Politikası

Amaç

Fiziksel Güvenlik Yönetim süreci, Şirket çalışma ortamı ve tesislerin sadece yetkili kişilerin kullanımına izin verecek şekilde yapılandırılması ve güvenlik sistemleri ile korunması için gerekli kuralları düzenlemektedir.

Kapsam

Fiziksel Güvenlik Yönetim süreci, Şirket verilerinin bulunduğu lokasyonlarını kapsamaktadır.

Politika

1. Çalışma ortamı ve bina güvenliğine yönelik fiziksel ve çevresel güvenlik kuralları aşağıda maddeler halinde sıralanmıştır.
2. Çalışma ortamı veya bina girişinde, görevli kişinin bulunduğu bir resepsiyon alanı veya girişin kontrol edilmesini sağlayan bir uygulama olmalıdır.
3. Çalışma ortamı veya bina genelinde haftanın 7 günü, günün 24 saati aktif olan alt güvenlik sistemi bulunmalıdır.
4. Ziyaretçilerin kişisel bilgileri, geliş ve ayrılış bilgileri kaydedilmelidir.
5. Çalışma ortamlarında güvenlik kameraları kurulu olmalı, gözetim altında tutulmalı ve kayıtlar geriye dönük "Saklama ve İmha Politikasında " belirtilen süre boyunca saklanmalıdır.
6. Kapı erişim ve kamera sistemleri yetkisiz erişimlere karşı parmak izi / kart okuyucu ile korunmalıdır.
7. Bilgi işlem alanları ile belirlenmiş diğer kritik noktalar toz, ısı, duman, nem ve su sızıntısına karşı detektör koruması altında olup, bu noktalar 7 gün 24 saat kesintisiz izlenerek kontrol

altında tutulmalıdır.

8. Çalışma ortamı ve bina yürürlükteki deprem yönetmeliklerine göre inşa edilmiş olmalı veya bina güçlendirmeleri yapılmış olmalıdır.
9. Bilgi sistemi cihazlarının bulunduğu alanlara erişim refakatle ve onaylı şekilde gerçekleştirilşmelidir.
10. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

23. Sunucu Güvenlik Yönetim Politikası

Amaç

Sunucu Güvenlik Yönetim süreci, Şirket sunucularına erişim ve güvenli işletim için gerekli güvenlik kurallarını düzenlemektedir.

Kapsam

Sunucu Güvenlik Yönetim süreci, Şirket verilerinin bulunduğu lokasyonlarını kapsamaktadır.

Politika

1. Sunucu güvenlik yönetimine yönelik fiziksel ve çevresel güvenlik kuralları aşağıda maddeler halinde sıralanmıştır.
2. Sunucularda tanımlanan iş ihtiyacına sunucu görevine uygun şekilde yazılımlar kurulmalıdır.
3. Sunucularda kullanılmayan servis ve portlar kapatılmalıdır.
4. Sunucu erişim logları aktif olmalı ve sunucu kapasitesine göre düzenli olarak yedeklenmelidir.
5. Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.
6. Sunucular fiziksel ve mantıksal olarak ayrıştırılmış ağlarda kullanım amaçlarına uygun şekilde konumlandırılmalıdır.
7. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

24. İş Sürekliliği Yönetim Politikası

Amaç

İş Sürekliliği Yönetim süreci, şirketin maruz kalacağı felaket sonrasında iş sürekliliğinin sağlanabilmesi için gerekli güvenlik kurallarını düzenlemektedir.

Kapsam

İş Sürekliliği Yönetim süreci, şirketin veri kasyonlarında bulunan BT envanterini ve ilgili süreçleri kapsamaktadır.

Politika

1. İş sürekliliği yönetimi, ürünlerin, servislerin ve iş süreçlerinin devamlılığını sağlamak üzere gerekli planları, olası iş kesintileri göz önünde bulundurularak yönetim tarafından

onaylanmış kurtarma stratejilerini, rol ve sorumlulukları içermelidir.

2. Kesintilerin olasılıklarının ve zaman, hasar ölçeği ve normale dönme süresi açısından etkilerinin değerlendirilmesi için risk analizi yapılmalıdır.
3. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

25. Veri Yedekleme Yönetim Politikası

Amaç

Veri Yedekleme Yönetim süreci, şirketin veri yedeklemesinin bilgi sınıflandırması ve iş birimi ihtiyaçlarına uygun şekilde yapılması için gerekli güvenlik kurallarını düzenlemektedir.

Kapsam

Veri Yedekleme Yönetim süreci, şirketin lokasyonlarında bulunan verileri, veri depolama cihazlarını ve ilgili süreçleri kapsamaktadır.

Politika

1. Şirketin önemli verilerinin bulunduğu ortak veri klasörü ve veritabanlarının tamamının yedeği uygun ve düzenli olarak alınmalıdır.
2. Yedekleme işlemlerinin sağlanması için bir yedekleme planı oluşturulmalı ve bu plana göre yedekleme işlemi kesintisiz yapılmalıdır.
3. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

26. İnsan Kaynakları Yönetim Politikası

Amaç

İnsan Kaynakları Yönetim süreci, şirketin, çalışan ve stajyerlerin bilgi güvenliği ile ilgili görev ve sorumlulukları, şirketin bilgi güvenliği yaklaşımına uygun olarak tanımlanması için gerekli güvenlik kurallarını düzenlemektedir.

Kapsam

İnsan Kaynakları Yönetim süreci, şirketin çalışanlarını ve stajyerlerini kapsamaktadır.

Politika

1. Bilgi güvenliğiyle ilgili görev ve sorumluluklar tanımlanan ve yönetim tarafından onaylanan Gizlilik Sözleşmesi çalışanlara tebliğ edilmelidir.
2. Bilgi güvenliğiyle ilgili görev ve sorumluluklar, şirketin bilgi güvenliği politikalarına uygun davranılmasını, varlıkların korunmasını ve diğer dokümante edilmiş (politika, prosedür, taahhütname, vb.) sorumlulukları kapsamalıdır.
3. Çalışanlara ve stajyerlere işe başlangıçta imzalatılan Gizlilik Sözleşmesi şirketin bilgi güvenliği yaklaşımını içerecek şekilde hazırlanmalı ve tüm çalışanlar imzalamalıdır.
4. Şirket tarafından çalışanlara sağlanan cep telefonu, araç, bilgisayar ve benzeri Şirket kaynakları sadece iş amaçlı olarak kullanılmalıdır.

5. İş akdi/hizmet sözleşmesi, sözleşme içeriğinde yer alan kayıt ve koşullara aykırı davranılması halinde Gizlilik Sözleşmesinin ilgili maddeleri uygulanmalıdır.
6. Bilgi güvenliği farkındalığını artırmak amacıyla düzenlenen eğitim, oryantasyon programları sürekli tekrarlanmalıdır. İşe yeni başlayan her personele oryantasyon ve bilgi güvenliği eğitimi verilmelidir.
7. İstifa eden çalışan ve/veya Şirket tarafından ihbar önelini kullandırmak suretiyle iş akdi/hizmet sözleşmesi sona erdirilen çalışanın sahip olduğu tüm erişim yetkileri kaldırılmalıdır. PDKS cihazından erişim yetkileri silinmelidir.
8. Uzun süreli sağlık raporu, doğum ve ücretsiz izin kullanan çalışanların uzaktan erişim yetkileri var ise kapatılmalıdır. Ancak sisteme giriş yetkileri kapatılmamalıdır.
9. İşten ayrılan çalışanın, iş amacıyla kullandığı elektronik ve fiziksel varlıklar (cep telefonu/tablet, dizüstü bilgisayar, vb.) zimmet formu ile kayıttan düşürülür.
10. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

27. Log Kayıtları Gözden Geçirme Yönetim Politikası

Amaç

Log Kayıtları Gözden Geçirme Yönetim süreci, şirketin sistemlerinden alınan log kayıtlarının izlenmesi ve gözden geçirilmesi için gerekli güvenlik kurallarını düzenlemektedir.

Kapsam

Log kaydı üreten sistem kaynaklarını kapsamaktadır.

Politika

1. Kullanıcı işlemlerine ait kayıtlarda değişikliğe sebep olan işlemler için asgari olarak aşağıdaki şekilde bilgileri içeren log kayıtları (denetim izleri) tutulmalıdır:
    - Bu kapsamdaki işlemlere ilişkin yetkisiz erişim teşebbüsleri,
    - İşlemi gerçekleştirenuygulama,
    - İşlemi gerçekleştiren kişinin kimliği,
    - Yapılan işlemlerinzamanı,
2. Log kayıtları en az 5 yıl süre ile saklanmalıdır.
3. Şirket, personelini, aktivitelerinin kaydının tutulduğu hususunda bilgilendirmelidir.
4. Log kayıtlarında karşılaşılan, olağanüstü durumlar üst yönetime raporlanmalıdır.
5. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

28. Bilgi Sistemleri Tedarik, Geliştirme ve Bakım Yönetim Politikası

Amaç

Bilgi Sistemleri Tedarik, Geliştirme ve Bakım Yönetim süreci, şirkete bilgi sistemlerine yönelik

her türlü alım, geliştirme, değişiklik vb. çalışmaların iş ihtiyaçları doğrultusunda gerçekleştirilmesi için gerekli güvenlik ve süreç kurallarını düzenlemektedir.

Kapsam

Bilgi Sistemleri Tedarik, Geliştirme ve Bakım Yönetim süreci, şirketin bilgi sistemleri tedarik, geliştirme ve bakım süreçleri ile ilintili BT varlıklarını kapsamaktadır.

Politika

1. İş ihtiyaçları doğrultusunda temin edilecek mal ve hizmetler Şirket tarafından hazırlanacak şartnamede yer almalı ve ilgili firmalarla paylaşılmalıdır.
2. Belirlenen kuruluş ve firmalardan alınan teklifler, hizmet başarı kriterleri göz önünde bulundurularak değerlendirilmelidir. Analiz sürecinde minimum aşağıdaki kriterler değerlendirilmelidir:
    - Fiyat avantajı,
    - Şartnameye uygunluk,
    - İstenilen tarihte teslim,
    - Satıcının referansları, güvenirliliği ve piyasadaki yeri,
    - Geçmiş dönem performansı (Varsa),
    - Nakliye vb. ek masrafların yansıtılma şekilleri,
    - Garanti süresi ve yedek parça fiyatlaması,
    - Satıcının veya ürünün, şirketimiz tarafından kabul edilmiş satıcı davranış kurallarına uyumluluğu,
    - Bilgi güvenliği standart ve uygulamalarına uyum,
3. Tedarik, geliştirme veya bakım çalışmalarına konu olan bilgi sistemleri için güvenlik ihtiyaçları belirlenerek ve Gizlilik Sözleşmesi imzalanmalıdır.
4. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir.

29. Bilgi Güvenliği İhlali Yönetim Politikası

Amaç

Bilgi Güvenliği İhlali Yönetim süreci, Şirkette iç ve dış faktörlerden dolayı oluşabilecek güvenlik zaafiyetlerinin engellenmesi, oluşması dahilinde kayıtlara geçirilerek zaafiyetle ilgili tedbir alınması gibi gerekli güvenlik ve süreç kurallarını düzenlemektedir.

Kapsam

Bilgi Güvenliği ihlali Yönetim Süreci, şirket süreçlerine ilişkin mevzuat düzenleme ve sözleşmeleri ve 6698 sayılı kanunu kapsamaktadır.

Politika

1. Bilgi güvenliği ihlal olayları şirkete bildirilmeli, Şirket kapsamını ilgilendiren olaylarda DÖF Formu oluşturmalı, 6698 sayılı kanun kapsamında yer alan veri ihlali bildirimlerinde ise “Kişisel Veri İhlal Bildirim Form” u doldurulmalı ve ilgili KVKK süreci başlatılmalıdır.

2. Kullanıcıların kasti olarak gerçekleştirdiği Bilgi güvenliği ihlal olaylarında şirketin ve kullanıcı arasında imzalanan Gizlilik Sözleşmesine bağlı olarak sözleşmesinin ilgili maddesi uygulanmalıdır. Ayrıca bu ihlali gerçekleştirerek kurumu doğrudan ve/veya dolaylı olarak zarara uğratan kişi ve/veya kuruluş aleyhine hukuki yollara başvurma hakkını Şirket saklı tutmaktadır.
3. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

30. Güvenlik açıkları Tespit Etme Politikası

Amaç

Bu politikanın amacı şirkete bilgisayar ağının (PC, sunucu, firewall, ağ anahtarı vs) güvenlik açıklarına karşı taranması hususunda politika belirlemektir.

Denetim sebepleri :

- Bilgi kaynaklarının bütünlüğünü ve gizliliğini sağlamak
- Kurumun güvenlik politikalarına uyumunun kontrolü için güvenlik açıklarını tespit etmek
- Gerektiği zaman kullanıcıların veya sistemin aktivitelerini kontrol etmek.

2.0 Kapsam

Bu politika şirketin bünyesinde sahip olunan bütün bilgisayar ve haberleşme cihazlarını kapsamaktadır. Bu politika şirketin bünyesinde bulunan fakat sahip olmadığı herhangi bir sistemi de kapsamaktadır. Denetim yapan kişi veya kurum Hizmetlerin durdurulması (Denial of Service) aktivitesi yapmamalıdır.

Politika

1. Şirket denetim yapan firmaya bilgisayar ağına erişim izni vermelidir. Şirket, denetim yapan firmaya ağ taraması yapması için protokol, adres bilgileri, ağ bağlantıları vs. hakkında bilgi verebilecektir. Bunlar aşağıdaki bilgileri kapsamaktadır:

- Bilgisayar veya haberleşme cihazlarına kullanıcı ve/veya sistem seviyeli erişim bilgileri.
- Kurumun bünyesindeki üretilen, iletilen veya saklanan bilgilere (elektronik, hardcopy vs) erişim.
- Çalışma alanlarına erişim (laboratuvar, ofisler, sistem odaları, bilgi depolama alanları vs).
- Şirket ağının trafiğini etkileşimli olarak gözlemleme ve trafiğin loglanması isteği.

2. Güvenlik taraması yapacak firma, denetleme zaman periyodunu şirkete yazılı olarak bildireceklerdir.
3. Şirket ile güvenlik taraması yapacak firma, tarama sonucunda elde edilecek bilgilerin hiçbir şekilde üçüncü şahıslara aktarmayacağına dair gizlilik anlaşması yapacaktır.

31. Doküman Kontrol

Hazırlayan

Aksiyon	İsim	Görev
Dokümanın oluşturulması		Bilgi Güvenliği Yönetim Temsilcisi

Onay Listesi

Aksiyon	İsim	Görev
İçerik Onayı		Şirket Yetkilisi
Yayınlama Onayı		Yönetim Kurulu Temsilcisi

BİLGİ GÜVENLİĞİ POLİTİKASI
AÇIK RIZA BEYANI

…… Bilgi Güvenliği Politikası'nda yer alan tüm yükümlülüklere uygun davranacağımı, bu yükümlülüklerden bir veya birkaçına herhangi bir şekilde uygun davranmamam halinde, idari, mali, hukuki ve cezai yaptırımların uygulanabileceğini kabul ve beyan ederim.

.

İLGİLİ PERSONEL	
TC Kimlik No	
Adı, Soyadı	
Cep Telefonu	
Adresi	
E-Posta Adresi	
Tarih	
İmza	