

FORM NO	PL.04
YAYIN TARİHİ	20.05.2020
REV.NO	
REV.TARİHİ	

İÇİNDEKİLER

1. Giriş.....	3
2. Amaç	3
3. Kapsam.....	3
4. Bilgi Güvenliği Hedefleri	3
5. Rol ve Sorumluluklar	4
6. Kısaltmalar	4
7. Bilgi Güvenliğinin Yönetilmesi	5
8. BT Varlıkları Yönetim Politikası	6
9. Kullanıcı ve Erişim Kontrol Yönetim Politikası	7
10. Şifre Kontrol Yönetim Politikası.....	8
11. E-Posta Yönetim Politikası.....	9
12. İnternet Erişim Yönetim Politikası	10
13. Zararlı Yazılımlara Karşı Korunma Yönetim Politikası	11
14. Veri Envanteri Oluşturma Yönetim Politikası	12
15. Uzaktan Erişim Yönetim Politikası	12
16. Dış Kaynak Kullanım Yönetim Politikası	13
17. Kabul Edilebilir Kullanım Politikası	14
18. BT Risk Yönetim Politikası	15
19. BT Güvenlik Olay Yönetim Politikası	15
20. Ağ Güvenlik Yönetim Politikası.....	16
21. Veritabanı Güvenlik Yönetim Politikası.....	17
22. Fiziksel Güvenlik Yönetim Politikası.....	18
23. Sunucu Güvenlik Yönetim Politikası	18
24. İş Sürekliliği Yönetim Politikası.....	19

FORM NO	PL.04
YAYIN TARİHİ	20.05.2020
REV.NO	
REV.TARİHİ	

25.	Veri Yedekleme Yönetim Politikası	19
26.	İnsan Kaynakları Yönetim Politikası	20
27.	Log Kayıtları Gözden Geçirme Yönetim Politikası	21
28.	Bilgi Sistemleri Tedarik, Geliştirme ve Bakım Yönetim Politikası	21
29.	Bilgi Güvenliği İhlali Yönetim Politikası	22
30.	Güvenlik açıkları Tespit Etme Politikası	23
31.	Doküman Kontrol	24

FORM NO	PL.04
YAYIN TARİHİ	20.05.2020
REV.NO	
REV.TARİHİ	

1. Giriş

Bu politika; **Sekamsan Kağıtçılık San.Tic.Ltd.Şti.’nin** bilgi varlıklarının yönetimini, korunmasını, gizliliğini, bütünlüğünü, dağıtımını ve sadece yetki verilen kişilerce erişilebilirliğini sağlayarak ve önemli işlevlerinin korunmasını düzenleyen kurallar ve uygulamalar bütününe 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

İdaremizin bu polikata 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.

	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

5. Rol ve Sorumluluklar

Roller	Sorumluluklar
Genel Müdür	<ul style="list-style-type: none"> Şirketin tüm bilgi güvenliği hususlarından sorumludur.
Muhasebe Müdürü	<ul style="list-style-type: none"> BT altyapı güvenliğinin sağlanmasıyla yükümlüdür. Güvenlik tehditleri, zafiyet ve risklere karşı plan yapmakla yükümlüdür. Yetki ve erişim haklarının belirlenmesini sağlamakla yükümlüdür.
Kullanıcılar	<ul style="list-style-type: none"> 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	Sekamsan Kağıtçılık San.Tic.Ltd.Şti.
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.
Yetkilendirme	Sisteme giriş izni vermek. Çok kullanıcıli sistemlerde sistem yöneticisi, sisteme girebilecek kişilere giriş izni ve kişilere bağlı olarak da sistemde yapabileceği işlemler için belirli izinler verir.
Yedekleme	Ekipmanın bozulması durumu düşünülerek dosyaların veya veritabanının başka bir yere kopyalanması işlemi.

	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

Kısaltma	Tanım
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 çöktürmeye 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,

 lađıt & karton	BİLGİ GÜVENLİĐİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

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

Bilgi Güvenliđi İlkeleri

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

- Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde Şirkete ait bilginin gizliliđini sağlamalı,
- Kritiklik düzeylerine göre işlediđi bilgiyi yedeklemeli,
- Bilgi güvenliđi ihlal olaylarını ve Eğitim ve Kalite Sorumlusu'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 güvenliđi politikası, prosedür ve talimatlarına uyulmaması halinde, Şirket personelin imzaladıđı Gizlilik Sözleşmesi cezai şart maddesi uygulanacaktır.

8. BT Varlıkları Yönetim Politikası

Amaç

BT varlık yönetimi Şirkete deđer yaratan fikri mülkiyet (fikir, kavram, know-how, teknik, materyal ve dokümantasyon), insan, teknoloji, bina ve donanım varlıkları ile kurumsal belleđi 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 diđer donanımları, uygulama ve yazılım envanterini kapsamakta olup, etkin zimmet sürecinin işletilmesi deđerlendirilecektir.

Tanımlar

1. Bilgi teknolojileri envanteri sadece ilgili iş aktivitelerinde atama ve/veya yetkilendirme şeklinde kullanılmalıdır.
2. Kritiklik deđeri ve gizlilik seviyesi yüksek olan bilgilerin ilgili personellerin dışında ulaşılamayak olan kilitli dolap veya kasalarda saklanmalıdır.
3. Yazıcı çıktısı alma, fotokopi ile çođaltma, 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 imzaladıđı cihazlar için) BT envanterinin

 lağıt & karton	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

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, PDA ve diğer taşınabilir cihazları düzenli olarak envanter takibi yapılmalıdır.
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, tablet pc ve PDA benzeri cihazlar çalınmaya karşı korunması sorumluluğu zimmeti yapılan personelin yükümlülüğündedir.
10. Dizüstü, akıllı telefon, tablet pc ve PDA 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.

Tanımlar

1. Değerli bilgi taşıyan sistemler şifre koruması sağlayan erişim kontrol sistemiyle korunur.
2. Gizli bilgi taşıyan sistemler iki faktörlü (şifre+kripto) 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.

 lağıt & karton	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

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 kimliklerinin, başka kullanıcılara verilmez.
9. Yetkisiz erişimlerin takip edildiği kullanıcılara bildirilmeli ve 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.

Tanımlar

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 için 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 kilitlenir.

	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

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.

Tanımlar

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 sistemleri gizli bilgi niteliğinde bilginin iletilmesinde kullanılmayacaktır. Gizli bilginin e-posta kanalında iletilmesi kontrollü ve şifreli şekilde yapılmalıdır.
4. Şirket e-posta kaynakları kullanılarak saldırgan, ırkçı, müstehcen veya yerel kanun ve yönetmeliklere aykırı amaçlarda mesajlaşma sistemi kullanılmamalıdır.
5. Şirket e-posta kaynaklarının kullanımı personel kurumda çalışırken aktif olmalıdır. İlişğın 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 Şirket yöneticisi e-posta erişim yetkisine sahiptir.
8. Kurumsal e-posta adreslerine erişimler güçlü şifrelerle korunmalıdır. Şifre yönetimi Şirketin şifre yönetim standardına uygun şekilde gerçekleştirilmelidir.
9. Dış kaynaklara iletilen e-postalarda sadece onaylı imzalar kullanılmalıdır.
10. Eklenti boyutları kurumda tanımlanan standartlara uygun şekilde ilgili profillere atanmalıdır. Söz konusu kontrollerin otomatize yöntemler aracılığıyla gerçekleştirilmesi sağlanmalıdır.

 lağıt & karton	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

11. Virüs ve zararlı yazılımları tespit eden sistemler kullanıcı PC ve sunucular en yüksek e-posta güvenliğini sağlayacak şekilde konumlandırılmalıdır.
12. Kurumsal e-posta kutuları yedeklemesi merkezi olarak Sistem Yöneticisi tarafından yapılmalıdır.
13. Dış kaynak firma ve üçüncü şahıslarla yapılan yazışmalarda Şirket bilgisi paylaşılmamalıdır. Paylaşıldığı hallerde Gizlilik Sözleşmesi uygulanır.
14. E-postaların Şirkete dışına e-posta adreslerine yönlendirilmesi yasaktır.
15. Kullanıcıları Şirket dışında e-posta kullanma durumunda şirketin belirlemiş olduğu web erişim adresinden bağlantı kurabilir.
16. 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.

Tanımlar

1. Tüm kullanıcılar kısıtlı şekilde internete erişebilir. Şirkete tarafından aşağıdaki yasaya göre kısıtlanan 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 kullanılmalıdır.

 lağıt & karton	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

4. Kullanıcılar internete 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 pc, PDA ve diğer mobil cihazları kapsamaktadır.

Tanımlar

1. Kurumda tüm Bilgisayar, notebook, tablet ve pdalarda lisanslı antivirus sitemi kullanılmaktadır. Her yeni çıkan sürümüyle güncellenmektedir.
2. Şirketin ağına bağlanan tüm bilgisayar ve cihazlarda gerçek zamanlı koruma sağlayan anti virüs kurulu olması zorunlu olmakla beraber virus koruma devre dışı bırakılamaz.
3. Şirkete ait sunucu ve bilgisayarlar merkezi olarak yönetilen ve onaylı anti virüs sistemini kullanılır. Şirket dışında bulunan gezici cihazlar Şirket ağına bağlanmasıyla ve anti virüs taramaları yapılmaktadır.
4. Antivirus uygulaması düzenli ve otomatik olarak virüs güncellemelerini gerçekleştirir.
5. Şirket ağına bağlanma mecburiyeti olan ziyaretçi bilgisayarlarında anti virüs, 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 taranır.
8. Kötü niyetli yazılım ve zararlı/mobil kod içerebilecek dosya türleri ve dosya türlerini barındıran kaynaklar çalıştırılmadan önce mutlaka antivirüs sisteminde taranarak güvenli olduğuna emin olunduktan sonra dosya açılır.
9. Taşınabilir cihazların dış ağdan erişimlerinde maruz kalabileceği saldırıları önlemek amacıyla kişisel güvenlik duvarları aktif olarak çalışır.

 sekamson lağıt & karton	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

10. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

14. Veri Envanteri Oluşturma Yönetim Politikası

Amaç

Veri envanteri oluşturma yönetim süreci, Şirket verilerinin kişisel veri, özel nitelikli kişisel veri, kritiklik ve gizlilik unsurları göz önünde bulundurularak sınıflandırılmasını sağlayacak çerçeve düzenle niteliğindedir. Sürecin amacı Şirket verilerinde bütünlük, gizlilik ve erişilebilirlik ilkelerinin uygulanmasını sağlamaktır.

Kapsam

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

Tanımlar

1. Veri sahipleri sorumluluklarında olan verinin ve sistemlerin güvenliğinden sorumludur.
2. Bilgi güvenliği ihlalleri derhal Eğitim ve Kalite Sorumlusuna bildirilmelidir. Gerektiği durumlarda karşı önlemler aktif hale getirilmeli, zarar ve kontrol değerlendirilir.
3. "Gizli Bilgi" olarak tanımlanan bilgi en yüksek güvenlik seviyesinde korunmalıdır. Sadece kısıtlı teknik personelin ve iş ihtiyaçları gereği veriyi kullanması gereken personelin erişimine açık olmalıdır.
4. İlgili kişiler için aydınlatma ve açık rıza beyanı metinleri oluşturulmalıdır.
5. "Şirkete Özel" olarak tanımlanan bilgi iş ihtiyaçları ve yapılan Tedarikçi Firma Gizlilik Sözleşmesi imzalanan üçüncü şahıslarla uygun olarak güvenli şekilde paylaşılır.
6. "Halka Açık" olarak tanımlanan bilgi umuma açıktır ve Şirketin internet sitesinde yayınlanır.
7. Veri envanteri oluşturulması, ilgili birimlerin, Veri koruma komitesinin ve irtibat kişinin aktif katılımıyla yapılır.
8. Kullanıcılar, veri yedekleme ve imha standardında belirtilen veri sınıflandırmasına uygun olarak yedekleme ve saklama yapmak zorundadır.
9. 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 düzenlemektir.

Kapsam

Şirket iç kaynaklarına erişme ihtiyacı bulunan kullanıcı ve cihazları kapsamaktadır.

Tanımlar

 lađıt & karton	BİLGİ GÜVENLİĐİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

1. Şirketin iç kaynaklarına dışarıdan erişimlerin gerçekleşmesi için kullanıcının gerekli yetkiye sahip olması gerekmektedir. Dışarıdan erişim talebi Şirket müdürünün 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 sınırlandırarak ve tanımlı giriş noktalarına yönlendirecek şekilde yapılandırılmalıdır.
11. 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.

Tanımlar

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

 lađıt & karton	BİLGİ GÜVENLİĐİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

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.

Tanımlar

1. Kullanıcı, Şirkete 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 paylaşmaz.
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.

 lağıt & karton	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

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 hopperlörü, 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, PDA ve diğer cihazları kapsamaktadır.

Tanımlar

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

 lađıt & karton	BİLGİ GÜVENLİĐİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

güvenlik kuralları düzenlemektedir.

Kapsam

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

Tanımlar

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 ve sunulur.
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.

Tanımlar

1. Ağ cihazlarının ayarlarındaki değişiklikler ve hizmet seviyeleri ile bu seviyelerle ilgili izleme faaliyetleri tanımlanmalıdır.
2. Şirket dışı personel ve/veya 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 şifre kontrolüyle sadece yetkili personel erişimi sağlanabilir.
4. Bilgisayar veya ağ sistemi üzerinde kurulu olan ve işin yapılabilmesi için gerekli olan portlar, hizmetler ve ağ yapısına erişimler kısıtlanmış olup yetkilendirmeler yapılmıştır.
5. İlk kurulum sonrasında ağ cihazlarındaki, üretici tarafından sağlanan varsayılan parolalar ve parametreler değiştirilir.
6. Kablosuz misafir ağlarında giriş şifreli yapılı ve hergün şifreler otomatik olarak değişir.
7. İç ağda internete açık sunucular bulunmamalıdır. İş ihtiyaçları konumlandırılması

	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

- durumunda genel ağdan izole edilmelidir.
- Güvenlik duvarları kuralları, suiistimale açık iletişim protokollerini yasaklayacak şekilde düzenlenmelidir.
 - Ağ cihazları ARP Poisoning ve benzeri ağ saldırılarını engelleyecek şekilde düzenlenmelidir.
 - Güvenlik duvarı kurallarında ANY kaynak veya ANY hedef tanımlamalarının yapılmaması sağlanmalıdır. Yetkilendirmeler IP bazlı yapılmalıdır.
 - Güvenlik duvarı kuralları her 6 ayda gözden geçirilir ve sonuçlar raporlanır.
 - Şirket ağına kablolu ve kablosuz protokoller kullanılarak yetkisiz erişimlerin gerçekleştirilmesini engelleyecek güvenlik kontrolleri uygulanır.
 - Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

21. Veritabanı Güvenlik Yönetim Politikası

Amaç

Veritabanı Güvenlik Yönetim süreci Şirketin 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.

Tanımlar

- Veritabanları kullanıcı ve diğer sunuculardan izole alt ağda konumlandırılmalıdır. Ağ güvenliği standartlarına uygun şekilde alt ağ konfigüre edilmelidir.
- İlk kurulum sonrasında veritabanında, üretici tarafından sağlanan varsayılan parolalar ve parametreler değiştirilmelidir.
- Profil bazlı yetkilendirme standardı benimsenmelidir. Profiller iş süreci ihtiyaçlarına uygun olarak belirlenmelidir.
- Yönetici hesapları ve ayrıcalıklı hesaplar hesap verilebilirlik prensibi esas alınarak kişiye atanarak tanımlanır, yönetici kullanıcıların şifreleri kasada saklanır.
- Veritabanı loglar sürekli aktif olarak çalışır ve düzenli olarak gözden geçirilir.
- Şifre yönetim standardına uygun şekilde karmaşık şifre uygulanır.
- Veritabanlarına uzaktan erişim yapılamaz. Sadece özel izinli kullanıcıların uzaktan bağlantı yapmaya yetkisi vardır.
- “Gizli Bilgi” olarak sınıflandırılan verilere sadece özel yetkili kişiler erişebilir.
- Standart kurulumda tanımlanan listener portu kurulumdan sonra değiştirilir.
- Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulur.
- Bilgi saklama medyaları Şirket dışına çıkartılamaz.
- Test veritabanlarında “Gizli Bilgi” içerikli bilgi barındırılmaz. Barındırılması gerektiği

	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

hallerde canlı sistemlerle aynı yetkilendirme kural ve profilleri kullanılır.

13. 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 tesisler sadece yetkili kişilerin kullanımına izin verecek şekilde yapılandırılmış güvenlik sistemleri ile korunması için gerekli güvenlik kuralları düzenlemektedir.

Kapsam

Fiziksel Güvenlik Yönetim süreci, Şirket verilerinin bulunduğu lokasyonlarını kapsamaktadır.

Tanımlar

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 ile kontrol edilir.
3. Çalışma ortamı veya bina genelinde haftanın 7 günü, günün 24 saati aktif olan alt güvenlik sistemi bulunur.
4. Ziyaretçilerin kişisel bilgileri, geliş ve ayrılış bilgileri kaydedilir.
5. Çalışma ortamlarında güvenlik kameraları kurulu olup gözetim altında tutulur ve kayıtları geriye dönük "Saklama ve İmha Politikasında " belirtilen üsre boyunca saklanır.
6. Kapı erişim ve kamera sistemleri yetkisiz erişimlere karşı parmak izi / kart okuyucu ile korumalıdır.
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 tutulur.
8. Çalışma ortamı ve bina yürürlükteki deprem yönetmeliklerine göre inşa edilmiş olup bina güçlendirmeleri yapılmıştır.
9. Bilgi sistemi cihazlarının bulunduğu alanlara erişim refakatle ve onaylı şekilde gerçekleştirilir.
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.

 lağıt & karton	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

Kapsam

Sunucu Güvenlik Yönetim süreci, Şirket verilerinin bulunduğu lokasyonlarını kapsamaktadır.

Tanımlar

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 kapatılır.
4. Sunucu erişim logları aktif olmalı ve sunucu kapasitesine göre düzenli olarak yedeklenir.
5. Sunucular fiziksel olarak korunmuş sistem odalarında bulunur.
6. Sunucular fiziksel ve mantıksal olarak ayrıştırılmış ağlarda kullanım amaçlarına uygun şekilde konumlandırılmıştır.
7. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

24. İş Sürekliliği Yönetim Politikası

Amaç

İş Sürekliliği Yönetim süreci, Şirketi 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.

Tanımlar

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 içerir.
2. Kesintilerin olasılıklarının ve zaman, hasar ölçeği ve normale dönme süresi açısından etkilerinin değerlendirilmesi için risk analizi yapılır.
3. İş sürekliliği planının her bir unsuruna ait test adımları, yöntemi, zamanlaması ve katılacak personel tanımlanarak İş Sürekliliği talimatında yer alır. Organizasyonda, süreçlerde ve teknolojilerde değişiklik olduğunda, iş sürekliliği planları güncellenir.
4. Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

25. Veri Yedekleme Yönetim Politikası

 lağıt & karton	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

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.

Tanımlar

1. Şirketin önemli verilerinin bulunduğu ortak veri klasörü ve veritabanlarının tamamının yedeği uygun ve düzenli olarak alınır.
2. Yedekleme işlemlerinin sağlanması için bir yedekleme planı oluşturulur ve bu plana yedekleme işlemi kesintisiz yapılır.leri sürekli ait kayıtlar tutulur.
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.

Tanımlar

1. Bilgi güvenliğiyle ilgili görev ve sorumluluklar tanımlanan ve yönetim tarafından onaylanan Gizlilik Sözleşmesi çalışanlara tebliğ edilir.
2. Bilgi güvenliğiyle ilgili görev ve sorumluluklar, Şirketin bilgi güvenliği politikalarına uygun davranılmasını, varlıkların korunmasını ve diğer dokümanite edilmiş (politika, prosedür, taahhütname, vb.) sorumlulukları kapsar.
3. Çalışanlara ve stajyerlere işe başlangıçta imzalatılan Gizlilik Sözleşmesi Şirketin bilgi güvenliği yaklaşımını içerecek şekilde hazırlanmış olup tüm çalışanları imzalaması zorunludur.
4. Şirket tarafından çalışanlara sağlanan cep telefonu, araç, bilgisayar ve benzeri Şirket kaynakları sadece iş amaçlı olarak kullanılabilir.
5. İş akdi/hizmet sözleşmesi, sözleşme içeriğinde yer alan kayıt ve koşullara aykırı davranılması halinde Gizlilik Sözleşmesinin ilgili maddeleri uygulanır.
6. Bilgi güvenliği farkındalığını artırmak amacıyla düzenlenen eğitim, oryantasyon programları sürekli tekrarlanır. İşe yeni başlayan her personele oryantasyon ve bilgi

 lađıt & karton	BİLGİ GÜVENLİĐİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

güvenliđi eğitimi verilir.

- İstifa eden çalıřan ve/veya řirket tarafından ihbar önelini kullandırmak suretiyle iş akdi/hizmet sözleşmesi sona erdirilen çalıřanın sahip olduđu tüm erişim yetkilil kaldırılır. PDSK cihazından erişim yetkileri silinir.
- Uzun süreli sađlık raporu, doğum ve ücretsiz izin kullanan çalıřanlar uzaktan erişim yetkileri var ise kapatılır. Ancak sisteme giriş yetkileri kapatılmaz.
- İřten ayrılan çalıřanın, iş amacıyla kullandıđı elektronik ve fiziksel varlıkları (cep telefonu/tablet, dizüstü bilgisayar, vb.) ZİMMET FORMU'nda kişiye kayıtlı olan cihazların iadesi alınır ve Zimmet Formu'nun bir örneđi personele iade edilir.
- 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, řirketin sistemlerinden alınan log kayıtlarının izlenmesi ve gözden geçirilmesi için gerekli güvenlik kurallarını düzenlemektedir.

Kapsam

Log kaydı üreten sistem kaynaklarını kapsamaktadır.

Tanımlar

- Kullanıcı işlemlerine ait kayıtlarda deđişikliğe sebep olan işlemler için asgari olarak ařađıdaki şekilde bilgileri içeren log kayıtları (denetim izleri) tutulmalıdır:
 - Bu kapsamdaki işlemlere ilişkin yetkisiz erişim teşebbüsleri,
 - İşlemi gerçekleřtiren uygulama,
 - İşlemi gerçekleřtiren kişinin kimliđi,
 - Yapılan işlemlerin zamanı,
- Log kayıtları en az 5 yıl süre ile saklanır.
- řirket, personelini, aktivitelerinin kaydının tutulduđu hususunda bilgilendirilir.
- Log kayıtlarında karşılaşılan, olađanüstü durumlar üst yönetime raporlanır.
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

28. Bilgi Sistemleri Tedarik, Geliřtirme ve Bakım Yönetim Politikası

Amaç

Bilgi Sistemleri Tedarik, Geliřtirme ve Bakım Yönetim süreci, řirketi bilgi sistemlerine yönelik her türlü alım, geliřtirme, deđişiklik vb. çalıřmaların iş ihtiyaçları dođrultusunda gerçekleştirilmesi için gerekli güvenlik ve süreç kurallarını düzenlemektedir.

	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

Kapsam

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

Tanımlar

- İş ihtiyaçlar Şirket tarafından hazırlanacak şartnamede yer almalı ve ilgili firmalarla paylaşılır.
- İş ihtiyaçları doğrultusunda belirlenen kuruluş ve firmalarda teklif alınarak alınan teklifler, hizmet başarı kriterleri göz önünde bulundurularak değerlendirilir. Analiz sürecinde minimum aşağıdaki kriterler değerlendirilmelidir:
 - Fiyat avantajı,
 - Şartnameye uygunluk,
 - İstenilen tarihte teslim,
 - Satıcının referansları, güvenilirliği 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,
- Tedarik, geliştirme veya bakım çalışmalarına konu olan bilgi sistemleri için güvenlik ihtiyaçları belirlenerek ve Gizlilik Sözleşmesi imzalanır.
- 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 olabilecek güvenlik zaafiyetlerinin engellenmesi, oluşması dahilinde kayıtlara geçirilerek zaafiyetle ilgili tedbir alınması gibi gerekli güvenlik ve süreç kurallarını düzenlemektedir.

Kapsam

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

Tanımlar

- Bilgi güvenliği ihlal olayları, Bölge Şirketine bildirilmeli, Şirket kapsamını ilgilendiren olaylarda DÖF Formu oluşturmalı, 6698 sayılı kanun kapsamında yer alan veri ihlali bildirimlerinde ise KVKK sitesinde yer alan "Kişisel Veri İhlal Bildirim Form" u

 lağıt & karton	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

doldurulmalıdır.

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

30. Güvenlik açıkları Tespit Etme Politikası

Amaç

Bu politikanın amacı Kurumun 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.
- Gerekli zaman kullanıcıların veya sistemin aktivitelerini kontrol etmek.

2.0 Kapsam

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

Tanımlar

İstenildiğinde denetim yapan firmanın bireylerine erişim izni verilecektir. Bu anlaşmada Şirket denetim yapan firmaya kendi izni ile bilgisayar ağına erişim hakkı vermektedir. Kurumun birimleri denetim yapan firmaya ağ taraması yapması için protokol, adres bilgileri, ağ bağlantıları vs. hakkında bilgi verecektir.

Bu istekler aşağıdaki bilgileri kapsamaktadır:

1. Bilgisayar veya haberleşme cihazlarına kullanıcı ve/veya sistem seviyeli erişim bilgileri.
2. Kurumun bünyesindeki üretilen, iletilen veya saklanan bilgilere (elektronik, hardcopy vs) erişim.
3. Çalışma alanlarına erişim (laboratuvar, ofisler, sistem odaları, bilgi depolama alanları vs).

	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

- Bakanlık ağının trafiğini etkileşimli olarak gözlemleme ve trafiğin loglanması isteği.
- Tarama esnasında muhatap olan kişi, denetimi yapan firmaya oluşabilecek muhtemel sorunlar hakkında danışabileceği bir kişiyi yazılı olarak verecektir.
- Denetimi yapan firma, denetleme zaman periyodunu Şirkete yazılı olarak bildireceklerdir.
- 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
Şablon dokümanın oluşturulması Bilgi toplama Dokümanın tamamlanması Yıllık Gözden Geçirme		Bilgi Güvenliği Yönetim Temsilcisi

Onay Listesi

Aksiyon	İsim	Görev
İçerik Onayı		Bilgi İşlem Müdürü
Yayınlama Onayı		Genel Müdür

Sekamsan Kağıtçılık San.Tic.Ltd.Şti. **BİLGİ GÜVENLİĞİ POLİTİKASI AÇIK RIZA BEYANI**

Sekamsan Kağıtçılık San.Tic.Ltd.Şti. 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.

Sekamsan Kağıtçılık San.Tic.Ltd.Şti. Bilgi Güvenliği Politikası'nda bir kopyasını teslim aldım, okudum ve anladım.

sekamsan lağıt & karton	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKASI	FORM NO	PL.04
		YAYIN TARİHİ	20.05.2020
		REV.NO	
		REV.TARİHİ	

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