Kolay İK, hizmet kalitesini yükseltmek amacı ile, bilgi güvenliği yönetim sistemi standartları olarak kabul edilen TS ISO IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemleri ile Kalite Yönetim Standardı olan TS EN ISO 9001:2008 yaklaşımlarını uygulama kararı almıştır. Bu belge bu anlamda müşterilerimize bilgi verme amacı ile hazırlanmıştır. Kolay İK, dünya çapında kabul görmüş olan bu standartları uygulayarak müşterilerine daha güvenli ve kaliteli hizmet vermeyi amaçlamaktadır.

Bilgi Güvenliği Nedir

Bilgi, kurumdaki diğer varlıklar gibi, kurum için önem taşıyan ve bu nedenle de en iyi şekilde korunması gereken bir varlıktır. Bilgi güvenliği; kurumdaki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve yatırımlardan gelecek faydanın artırılması için bilginin geniş çaplı tehditlerden korunmasını sağlar.

Bilgi birçok biçimde bulunabilir. Bilgi, kâğıt üzerinde yazılı olabilir, elektronik olarak saklanıyor olabilir, posta ya da elektronik posta yoluyla bir yerden bir yere iletilebilir ya da kişiler arasında sözlü olarak ifade edilebilir.

Bilgi hangi formda olursa olsun, mutlaka uygun bir şekilde korunmalıdır. Bilgi güvenliğinin sağlanabilmesi bilginin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin yeterli düzeylerde sağlanabilmesi ile mümkündür. Bilgi güvenliği temelde aşağıdaki üç unsuru hedefler

- Gizlilik (Confidentiality)
- Bütünlük (Integrity)
- Kullanılabilirlik (Availability)

Bu kavramları biraz daha açacak olursak gizlilik, bilginin yetkisiz kişilerin erişimine kapalı olması şeklinde tanımlanabilir. Bir diğer tarif ile gizlilik bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir. Bütünlük, bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır. Bütünlük için kısaca kazara veya kasıtlı olarak bilginin bozulmaması diyebiliriz. Kullanılabilirlik, bilginin her ihtiyaç duyulduğunda kullanıma hazır durumda olması demektir. Herhangi bir sorun ya da problem çıkması durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Bu erişim kullanıcının hakları çerçevesinde olmalıdır.

Kullanılabilirlik ilkesince her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir.

Politika Detayları

Amaç

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

Bilgi güvenliği yönetim sisteminin amacı tüm bilgi varlıklarımızın gizliliği, bütünlüğü ve gerektiğinde yetkili kişilerce erişilebilirliğini sağlamaktır. Bilgi diğer kıymetli varlıklarımızın içinde en çok ihmal edilen fakat kurum açısından en önemli varlıklardan biridir.

Bilgi güvenliği yönetim sistemimiz TS ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi Standardına uygun olarak kurulmuş ve bu standardın gerekliliklerini karşılayacak şekilde PUKÖ (Planla, Uygula, Kontrol Et, Önlem Al) sürekli iyileştirme döngüsü çerçevesinde bir süreç olarak uygulanmaktadır.

Bilgi güvenliği sadece bilgi teknolojileri çalışanlarının sorumluluğunda değil eksiksiz tüm çalışanların katılımı ile başarılabilecek bir iştir. Ayrıca bilgi güvenliği sadece bilgi teknolojileri ile ilgili teknik önlemlerden oluşmaz. Fiziksel ve çevresel güvenlikten, insan kaynakları güvenliğine, iletişim ve haberleşme güvenliğinden, bilgi teknolojileri güvenliğine birçok konuda çeşitli kontrollerin risk yönetimi metoduyla seçilmesi uygulanması ve sürekli ölçülmesi demek olan bilgi güvenliği yönetim sistemi çalışmalarımızın genel özeti bu politikada verilmektedir. Uygulama detay bilgileri için sistem dokümantasyonuna, ilgili prosedürlere, rehberlere, planlara ve raporlara bakılmalıdır. Bu politika bilgi güvenliği politikası ve detaylı kullanım politikalarını da kapsayan bir üst dokümandır.

BGYS Tanımları

Bilgi Güvenliği Politikasının hazırlanması, gözden geçirilmesi ve güncellenmesinden Bilgi Güvenliği Yönetim Sistemi Yöneticisi ve Bilgi Güvenliği Yönetim Sistemi Sorumlusu sorumludur. Kolay İK Bilgi Güvenliği Politikasını onaylar ve duyurulmasını sağlar.

Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır.

Bilgi Güvenliği Yöneticisi; Bilgi Güvenliği Yönetim Sistemi'nin operasyonundan ve sürekli iyileştirilmesinden sorumludur.

Bilgi Güvenliği Sorumlusu ; Bilgi Güvenliği Yöneticisi 'ne destek olmak ve tüm bilgi güvenliği süreçlerinde Bilgi Güvenliği Yönetici ile yer almaktan sorumludur.

Bilgi Varlığı

Kolay İK' nın sahip olduğu, işlerini aksatmadan yürütebilmesi için önemli olan varlıklardır. Bu politikaya konu olan bilgi varlıkları aşağıdadır:

- Kâğıt, elektronik, görsel veya işitsel ortamda sunulan her türlü bilgi ve veri,
- Bilgiye erişmek ve bilgiyi değiştirmek için kullanılan her türlü yazılım ve donanım,
- Bilginin transfer edilmesini sağlayan ağlar,
- Bölümler, birimler, ekipler ve çalışanlar,
- Ofis ve Özel alanlar,
- Çözüm ortakları,
- Üçüncü taraflardan sağlanan servis ve hizmetler,

Bilgi Varlığının İş Sahibi

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

Bilgi Varlığının Tek Sahibi

Bilgi varlıklarının kurum içinde kullanılması için gerekli olan teknik operasyonda sorumluluğu bulunan kişi veya ekipleri tanımlar.

Politika

Bilgi kaynakları, ofis ve cihazlar gibi Kolay İK açısından büyük önem taşıyan varlıklardır. Bilgi varlıklarını ve kaynaklarını kullanan veya bilgi sağlayan herhangi bir kişi, bilgi varlıklarını korumakla yükümlüdür.

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

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

Kolay İK için tüm bu bilgi varlıkları ve kaynakları içerisinde en kritik olanı, özenle korunması, gizliliğinin sağlanması, ihtiyaç duyulduğu anda erişilmesi gereken bilgi varlıkları, Servis sağlayıcılar olan Microsoft Azure, AWS, Online.net ve Radore firmalarında bulunan sunucular ve Kolay İK ofislerindedir.

Bilgi varlıkları ve kaynakları farklı konumlarda veya ortamlarda bulunabilir. Hangi konumda veya ortamda olursa olsun müşteri iletişim gereksinimleri ve kurumsal değerler bu varlıkların ve kaynakların kullanımını belirler.
Bilgi güvenliği, sadece bilginin gizliliğinin değil, bütünlüğünün ve kullanılabilirliğinin de sağlanması ile mümkündür. Bilginin gizlilik gerekliliği, sadece yetkilendirme dahilinde gereken bilgi varlıklarına erişim verilmesi anlamına gelir. Bilginin bütünlüğü, tüm bilgi varlıklarının tamlığını ve doğruluğunu sağlamayı gerektirir. Bilginin kullanılabilirliği, bilgi varlıklarının ihtiyaç duyulduğu anda ulaşılabilir ve kullanılabilir olması anlamına gelir.
Bilginin kullanımı, yerleşimi ve korunması ile ilgili ihtiyaçların karmaşıklığı ve çokluğu, kapsamlı ve geniş bilgi güvenliği süreçlerinin ve politikalarının tanımlanmasını zorunlu kılmaktadır. Bu nedenle belirlenen süreçler doğrultusunda bilgi güvenliği riskleri, bilgi varlığından sorumlu olan kişiler tarafından değerlendirilir, risklerin önceliği belirlenir ve gereken önlemler alınır.
Sistem odası ve sunucuların güvenliğinin sağlanması öncelikli olarak ele alınır. Varlık envanterinin ve bu envanterin olası risklerinin önceden belirlenerek müşterilerin güven içinde ve kesintisiz hizmet almaları için çalışılır.
Karar ve eylemlerde, güvenilir nesnel bilgiler ile teknolojinin tüm olanaklarının kullanılmasına önem ve öncelik verilir. Hareketler sezgilere, duygulara ya da doğru görünene göre değil; bilimsel ve teknolojik gerçeklerin ortaya koyduğu objektif esaslara göre düzenlenir. Bunu sağlamak için bilgi dünyadaki en ileri kaynaklardan transfer edilir, benimsenir ve mesleki uygulamalar bu doğrultuda yapılır. Kaynaklar verimli kullanılarak teknolojiye yatırım yapılır, gelişim bu doğrultuda sürdürülür.
Bu nedenle bilgi güvenliği yönetim sisteminin planlama, uygulama, izleme ve iyileştirme adımları ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardına ve bu standardı destekleyen standartlara uygun olarak yürütülür.

Bilgi Varlıklarının ve Kaynaklarının Kullanımı

Kolay İK' da yürütülen işlerin sürekliliğinin ve gelişiminin sağlanması nedeniyle, bilginin gizliliğinin korunması öte yandan bilginin ve fikirlerin paylaşılması ve yaygınlaştırılması gerekir. Bilginin

hassasiyeti ve güvenliği ile ilgili ihtiyaçlar gözetilirken, aynı zamanda bilgiye ihtiyaç anında hızla ulaşılması büyük önem taşımaktadır. O nedenle, bilgi kaynaklarının değerinin iyi tespit edilmesi, bilginin korunmasını sağlayacak çaba ve maliyetin bilginin hassasiyeti ile orantılı olması gerekir. Kolay İK bilgi kaynaklarını kullanarak etik dışı veya yasalara karşı faaliyetlerde bulunmak, hiç kimse için kabul edilemez bir durumdur. Politikanın asgari gereği olarak;

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

Bu ve benzeri faaliyetler ve teşebbüsler disiplin suçu olarak ele alınır, gereken disiplin süreçleri ve yasal süreçler disiplin prosedürüne göre disiplin kurulu tarafından uygulanır.

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

Sorumluluklar

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

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

Bütün bu faaliyetlerin kurumsal ISO/IEC 27001 standardı ile uyumlu bir çerçevede ele alınması için, tüm kuruluşun süreç ve hizmetlerini kapsayan bir Bilgi Güvenliği Yönetim Sistemi kurulmuş ve Genel Müdür, "Bilgi Güvenliği Sorumlusu", "Bilgi Güvenliği Yöneticisi", "Bilgi Güvenliği Komisyon" olarak atanmıştır.

Prosedür ve Politikaların Kullanıldığı Birimler : Kolay İK Çalışanları

Prosedür ve Politikaların Yürütülmesi için Sorumlular : Kolay İK BGYS Yöneticisi

Bilgi Güvenliği Kurulu

Bilgi Güvenliği Kurulu (BGK) aşağıdaki kişilerden oluşur;

- Bilgi Güvenliği Sorumlusu
- Bilgi Güvenliği Yöneticisi

BGK, altı ayda bir, Bilgi Güvenliği Yöneticisinin oluşturduğu gündem çerçevesinde toplanır. Bu toplantılar aynı zamanda yönetim gözden geçirme toplantılarıdır.

Toplantılarda görüşülen konular aşağıda belirtilen maddeleri içerir, ancak bunlarla sınırlı kalmayabilir;

- Bilgi Güvenliği Politikasının gözden geçirilmesi.
- Risk Yönetim Metodolojisinin onaylanması.
- Güncel risk raporunun değerlendirilmesi.
- Kabul edilebilir risk seviyesinin Genel Müdür tarafından onaylanması.
- Kabul edilebilir risklerin Genel Müdür tarafından onaylanması.
- Risk işleme planının Genel Müdür tarafından onaylanması.
- Güvenlik ihlal olaylarının değerlendirilmesi.
- İş süreklilik stratejisinin gözden geçirilmesi.
- İş sürekliliği tatbikat sonuçlarının değerlendirilmesi.
- Bilgi güvenliği bilinçlendirme çalışmalarının gözden geçirilmesi.
- İç denetim raporlarının değerlendirilmesi.
- Kurumu etkileyebilecek önemli değişiklikler.
- Bu politika Kolay İK Genel Müdürü tarafından gözden geçirilmiş ve onaylanmıştır.

Bilgi Sistemleri Genel Kullanım Politikası

Kolay İK'nın amacı herhangi kimse üzerinde kısıtlayıcı politikalar üretmek değil aksine açıklık, güven ve bütünlüğe yönelik kültürü yerleştirmektir. Kolay İK bilerek veya bilmeyerek yapılan yasa dışı veya zararlı eylemlerine karşı çalışanların ve kurumun haklarını korumaya adamıştır. Bilişim ile alakalı sistemler kurumun sahip olduğu değerlerdir.

Güçlü bir güvenlik bütün çalışanların içerisine dâhil olduğu takım çalışmasıyla oluşturulabilir. Bütün bilgisayar kullanıcıları günlük aktivitelerini yerine getirebilmesi için bu kuralları iyi bilmeli ve uygulamanın sorumluluğunu taşımalıdır.

Kurum bünyesindeki bilişim cihazlarının uygun kullanımı hakkında taslak oluşturmaktır. Uygunsuz kullanım kurumu virüs saldırılarına, ağ sistemlerinin çökmesine hizmetlerin aksamasına sebep olabilir ve bunlar yasal yaptırımlara dönüşebilir. Bu politika kurumun bütün çalışanları, sözleşmelileri ve kurum

adı altında çalışan bütün kişiler için geçerlidir. Aynı zamanda Kolay İK' nın sahip olduğu ve kiraladığı bütün cihazlar için geçerlidir.

Genel Kullanım ve Sahip Olma

- Kullanıcılar şunun farkında olmalıdırlar; kurumun güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da kurumun bünyesinde oluşturulan tüm veriler kurumun mülkiyetindedir.
- Çalışanlar bilgi sistemlerini kendi kişisel kullanımı için makul seviyede yararlanabilirler. Her bir departman kendi bilgi sistemlerinin kişisel kullanımı için gerekli kuralları koymalıdır. Birimler böyle bir kural koymamış ise kurumun koyduğu genel güvenlik politikaları geçerlidir.
- Kullanıcı herhangi bir bilginin çok kritik olduğunu düşünüyorsa o bilgi şifrelenmelidir.
- Güvenlik ve ağın bakımı amacı ile yetkili kişiler cihazları, sistemleri ve ağ trafiğini gözlemleyebilir.
- Kolay İK, bu politika çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.
- Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı, kopyalanmamalı ve kullanılmamalıdır.
- Bilgisayarlar üzerinden resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.
- Birimlerde sorumlu bilgi işlem personeli ve ilgili teknik personel dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vb. üzerinde mevcut yapılan düzenlemeler hiçbir surette değiştirilmemelidir.
- Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.

Güvenlik ve Kişiye Ait Bilgiler

Genel olarak aşağıdaki eylemler yasaklanmıştır. Kritik öneme sahip sistem yöneticileri bu kapsamın dışında olabilir. Herhangi bir kullanıcı kurumun kaynaklarını kullanarak hiçbir şart altında herhangi bir yasa dışı aktivitede bulunamaz.

- Bilgi sistemlerinde bulunan kritik bilgilere yetkisiz kişilerin erişimini engellemek için gerekli erişim hakları tanımlanmalıdır.
- Şifreleri güvenli bir şekilde tutun ve hesabınızı başka kimselerle paylaşmayın. Sistem seviyeli şifreler 4 ayda bir kullanıcı seviyeli şifreler ise en az 6 ayda bir şifrelenmelidir.

- Bütün PC ve Laptoplar otomatik olarak 10 dakika içerisinde olarak oturum kapatılarak şifreli ekran korumasına geçebilmelidir.
- Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. Bios ve işletim sistemi şifreleri aktif hale getirilmelidir. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmalıdır.
- Laptop bilgisayarın çalınması / kaybolması durumunda, durum fark edildiğinde en kısa zamanda yetkili kişiye haber verilmelidir.
- Bütün cep telefonu ve PDA cihazları kurumun ağı ile senkronize olsun veya olmasın şifreleri aktif halde olmalıdır. Kullanılmadığı durumlarda kablosuz erişim özellikleri aktif halde olmamalıdır ve mümkünse anti-virüs programları ile yeni nesil virüslere karşı korunmalıdır.
- Geçici personel kullanıcı hesapları açılırken sezon sonunda otomatik olarak süresi dolacak şekilde oluşturulur.
- Çalışanlar bilinmeyen kimselerden gelen dosyaları açarken çok dikkatli olmalıdırlar. Çünkü bu mailler virüs, e-mail bombaları ve Truva atı gibi zararlı kodları içerebilirler.
- Bütün kullanıcılar ağın kaynaklarının verimli kullanımı konusunda dikkatli olmalıdırlar. E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olunmalıdır.
- Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek kuruma veya kişiye yönelik saldırılardan sistemin sahibi sorumludur.

İlgili Prosedürler

- **Kayıtların Kontrolü Prosedürü :** Entegre Yönetim Sisteminin etkin olarak uygulandığını ve etkin olarak işlediğini göstermek amacıyla tutulan kayıtların; tanımlanması, dosyalanması, muhafazası, istenildiğinde tekrar ulaşılması, elden çıkarılması, saklanma sürelerinin belirlenmesi gerekli durumlarda ulaşılabilirliğinin sağlanması ve imhası esaslarını belirler.
- **Düzeltme ve Düzeltici Faaliyet Prosedürü :** Hizmetlerde, proseslerde ve entegre yönetim sisteminde ortaya çıkan uygunsuzlukların; sebeplerinin belirlenerek uygunsuzlukların tekrarını önlemek üzere gerekli düzeltici faaliyetlerin belirler.
- **Yönetim Gözden Geçirme Prosedürü :** Bilgi Güvenliği Yönetim Gözden Geçirme Prosedürü Kolay İK BGYS yönetim prensip ve esaslarının bulunduğu ana dokümandır.
- **Personel Yetkileri ve Yedeklilik Prosedürü :** Personel yetkilerini ve Yedeklilik esaslarını belirler.
- **Temiz Masa Temiz Ekran Prosedürü :** Normal çalışma saatleri süresince ve dışında bilgiye yetkisiz erişim, bilgi kaybı ve hasarı risklerini azaltmak amacıyla kâğıtlar ve kaldırılabilir depolama ortamları ve kişisel bilgisayarlar için gerekli şartları tanımlar.

- **Zararlı Yazılımlardan Korunma Prosedürü :** Kolay İK BGYS kapsamında kötü niyetli koda ve yazılımlara karşı korunmak için yazılımların kullanılmasını tanımlar.
- **Yasal Gereksinimlere Uyum ve Kontrol Prosedürü :** Kolay İK bilgi sistemleri kaynaklarının oluşum ve kullanımı ile kurumsal ve yasal kurallara uyum arasındaki yapılanma esasları ile güvenlik politikaları ve standartlarla uyum ile denetim esaslarını tanımlar.
- **Yedekleme Prosedürü :** Kolay İK sistemlerinin oluşabilecek hatalar karşısında sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için sistem ve kurumsal verilerin düzenli olarak yedeklenmesi hususunda kuralları tanımlamaktır.
- **Yeni Bilgi Sistemleri ve Yapılan Geliştirmeler Prosedürü :** Kolay İK yeni bilgi sistemleri ve yapılan geliştirmelerde dikkat edilmesi gereken hususları tanımlar.
- **Kapasite Planlama Prosedürü :** Kolay İK sistem takip ve ihtiyaç belirleme esaslarını tanımlamaktadır.
- **Kullanıcı Sorumlulukları Prosedürü :** Kolay İK personelinin kurum bünyesinde işe giriş, çıkış esaslarının belirtilmesi; sorumlulukların tanımlanması ve ilgili kişiye sorumluluklarının bildirilmesini tanımlar.
- **İzleme ve Ölçme Prosedürü :** Kolay İK Entegre Yönetim Sistemleri Faaliyetleri performansı için kilit performans parametrelerini belirtir.
- **Fiziksel ve Çevresel Güvenlik Prosedürü :** Bilgi güvenliği gereksinimlerine bağlı olarak ortaya çıkan fiziksel güvenlik gereksinimlerini ve bunlara dair kuralları belirler.
- **Erişim Kontrolü Prosedürü :** Kurumda Erişim Kontrol prosedürünü açıklamaktadır. Erişim kontrolü, en basit tanımıyla, belli bir varlığa sadece yetkili kişi veya grupların tanımlanan haklar dahilinde erişebilmesini sağlama amacıyla uygulanır.
- **Fikri Mülkiyet Haklarına Uyum Prosedürü :** Kolay İK çalışanları tarafından fikri mülkiyet hakkı içerisinde yer alan; şirkete ait teknolojiler kullanılması sonucunda ortaya çıkan know-how, patent, tasarım veya marka mahiyetindeki bilgi ve ürünler üzerindeki haklar ile Fikir ve Sanat Eserleri Kanunu'nda eser olarak tanımlanan her türlü çalışma üzerindeki şirkete ait fikri hakların korunması ve şirket dışındaki üçüncü kişilere ait ürün ve eserler üzerindeki hakların ihlalinin önlenmesi için uyulacak kuralları ve işlemleri tanımlamaktır.
- **İş Ortaklarına Hizmet Sağlama Prosedürü :** Kolay İK hizmetlerinin yürütülmesi, sürdürülmesi ve yapılacak yatırımlar için ihtiyaç duyulan her türlü hizmetin satın alınmasına ilişkin BGYS ile ilişkili maddelerin düzenlenmesini tanımlar.
- **Bilgi Güvenliği İhlal Olayı Yönetimi Prosedürü :** Kurumda bilgi güvenliği ihlal olayları tespitinde dikkat edilmesi gereken noktaları açıklar.
- **BGYS Uygulama Prosedürü :** ISO 27001:2013 bilgi güvenliği yönetim sistemi standardı gereklerinin kuruluşumuzda uygulanmasını sağlamak üzere esasları belirlemektir.

- **İnternet Erişim Kuralları Prosedürü :** Kolay İK personelinin internete girerken uyacağı kuralları belirlemektir.
- **Teçhizat Yok Etme Prosedürü :** Kurumda ki teçhizat yok etme için gereken kuralları tanımlar.
- **Proje Güvenliği Prosedürü :** Kolay İK personelinin projelerin güvenliğini ve proje gizliliğini tanımlar.
- **Kriptografi Prosedürü :** Kolay İK' da uygulanan şifreleme yönteminin güvenlik esaslarını tanımlar.
- **Yazılım Geliştirme Prosedürü** : Yazılımların geliştirilmesine ve değişikliğine ilişkin çerçeveyi belirler.

Politika ve Prosedürler ile Uyum

Çalışanların ve Firmaların BGYS'ne uygun davranıp davranmadığı, kontrol sistemleri ve bilgi işlem sistemlerinin güvenlik gereksinimlerine uyum, BGYS Uygulama Prosedürü'ne uygun şekilde kontrol edilir.