İçindekiler

1 Temel İlkeler

1.1 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.

1.2 Bilgi Güvenliği Politikası

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.

Bilgi kaynakları, ofis ve cihazlar gibi Prizma A.Ş. 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.

Prizma A.Ş. için tüm bu bilgi varlıkları ve kaynakları içerisinde en kritik olanı, özenle korunması, gizliliğinin sağlanması, ihtiyaç duyulduğu anda erişilmesi gereken bilgi varlıkları, sunucu sistem odası ve ofistedir.

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 dâhilinde 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.

1.3 Bilgi Varlığı

Prizma A.Ş.' in 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.

1.3.1Varlıklar Ve Teknoloji

Prizma A.Ş. internet hattının yönetimi barındırılması dışındaki hizmetlerini kendisi yerine getirmektedir.

İnternet hattının yönetimi dış kaynak kullanımı yolu ile gerçekleştirilmektedir.

BGYS, aşağıdakilerin hepsini kapsar;

- Şirketin tüm ticari bilgileri
- Şirket çalışanlarına ait kişisel bilgiler
- Müşterilerin tüm kişiye özel bilgileri
- Tedarikçiler ve müşteriler ile yapılan sözleşmeler
- Yukarıdaki bilgileri içeren BT(Bilgi Teknolojileri) Sistemleri
- Dış kaynak kullanım faaliyeti
- Sistem Dokümantasyonu

1.4 Bilgi Varlıklarının ve Kaynaklarının Kullanımı

Prizma A.Ş. 'de 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.

Prizma A.Ş.'nin 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 suiistimal edilmesi.
- Cihazların, yazılımların veya herhangi diğer bir bilgi kaynağının çalınması, tahrip edilmesi.
- Bilgi kaynaklarının bilişim sistemlerinin performans kaybına sebep olacak şekilde kullanılması.
- Tesislerin, fiziksel cihazların, ağların tahrip edilmesi kabul edilemez.

Bu ve benzeri faaliyetler ve teşebbüsler disiplin suçu olarak ele alınır, gereken disiplin süreçleri ve yasal süreçler 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.

1.5 Bilgi Güvenliği Organizasyonu

Prizma A.Ş. Firması 5 bölümden oluşmaktadır.

- Üst Yönetim
- Yazılım /Proje Geliştirme
- Sistem Destek
- Muhasebe / Finansman
- Destek Ve Uzaktan Yardım

1.6 Rol Ve Sorumluluklar

Bilgi Güvenliği Politikasının hazırlanması, gözden geçirilmesi ve güncellenmesinden Bilgi Güvenliği Yönetim Sistemi Yöneticisi ve Bilgi Güvenliği Yönetim Sistemi Sorumlusu sorumludur. **Prizma A.Ş. Bilgi Güvenliği Politikasını** onaylar ve duyurulmasını sağlar.

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

- Prizma A.Ş. Çalışanları

Prosedür ve Politikaların Yürütülmesi için Sorumlular

- Prizma A.Ş. BGYS Yöneticisi

1.6.1Bilgi Güvenliği Yönetim Sistemi (BGYS)

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

1.6.2Bilgi Güvenliği Yöneticisi

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

1.6.3Bilgi Güvenliği Yönetim Sistemi Sorumlusu

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

1.6.4Bilgi 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.

1.6.5Bilgi Varlığının Tek Sahibi

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

2 Politikalar

2.1 Bilgi Sistemleri Genel Kullanım Politikası

Prizma A.Ş. 'in amacı herhangi kimse üzerinde kısıtlayıcı politikalar üretmek değil aksine açıklık, güven ve bütünlüğe yönelik kültürü yerleştirmektir. Prizma A.Ş. bilerek veya bilmeyerek yapılan yasadışı 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 Prizma A.Ş. 'nin sahip olduğu ve kiraladığı bütün cihazlar için geçerlidir.

2.1.1 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.
- Prizma A.Ş., 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.

2.1.2 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 yasadışı aktivitede bulunamaz.

- Bilgi sistemlerinde bulunan kritik bilgilere yetkisiz kişilerin erişimini engellemek için gerekli erişim hakları tanımlanmalıdır.
- Bütün PC ve Laptoplar otomatik olarak 5 dakika içerisinde olarak oturum kapatılarak şifreli ekran korumasına geçebilmelidir.

- Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. İşletim 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.
- Çalışanlar bilinmeyen kimselerden gelen dosyaları açarken çok dikkatli olmalıdırlar.
- 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.

2.2 Sistem ve Ağ Aktiviteleri

Aşağıdaki aktiviteler; Prizma A.Ş. çalışanları için geçerlidir. Ayrıca bu aktiviteler hiçbir istisna olmadan kesinlikle yasaklanmıştır.

- Herhangi bir kişi veya kurumun izinsiz kopyalama, ticari sır, patent veya diğer şirket bilgileri, yazılım lisansları vs. haklarını çiğnemek.
- Zararlı programların ağa veya sunuculara bulaştırmak.
- Kendi hesabınızın şifresini başkalarına vermek veya kendi hesabınızı kullandırmak.
- Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışmak.
- Ağ güvenliğini etkilemek, ağ haberleşmesini bozmak.
- Kullanıcı kimlik tanıma yöntemlerinden kaçmak.
- Kurum bilgilerini kurum dışından üçüncü şahıslara iletmek.
- Kullanıcıların kişisel bilgisayarları üzerine sistem yöneticisinin onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapması.
- Yazılım ve verinin izinsiz olarak kurum dışına çıkarılması.
- Kurumun politikaları olarak belirlediği programlar dışında kaynağı belirsiz olan programları kurmak ve kullanmak yasaktır.
- Yetki verilmeyen sunucu ve ağ kaynaklarına erişimi denenmemeli, erişim ihtiyacı durumunda mutlaka sistem yöneticisinden gerekli izinler alınmalıdır.

2.3 Personel Güvenliği

Kurumun bilgi kaynaklarının güvenliğinin sağlanması, çalışanlarının bu konuya duyarlı olması, bilinç seviyesi kendisine verilen yetki ve sorumlulukları iyi anlaması ve yerine getirmesiyle çok yakından bağlantılıdır. Bu nedenle kurum, ilgili personelin seçimi sorumluluk ve yetkilerin atanması, işten atılması, eğitilmesi, vb. konularının güvenlik ile ilgili boyutunu ne şekilde ele alacağını bu politika ile belirler. Ayrıca bu politika kurum bilgi sistemlerini kullanan tüm yönetici ve çalışanlarını kapsamaktadır.

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

- Kullanıcılara erişim haklarını açıklayan yazılı bildiriler verilmeli ve teyit alınmalıdır.
- Yetkisi olmayan personelin, kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.
- Bilgi sistemlerinde sorumluluk verilecek kişinin özgeçmişi araştırılmalı, beyan edilen akademik ve profesyonel bilgiler teyit edilmeli, karakter özellikleriyle ilgili tatmin edici düzeyde bilgi sahibi olmak için iş çevresinden ve dışından referans sorulması sağlanmalıdır.
- Bilgi sistemleri ihalelerinde sorumluluk alacak firma personeli için güvenlik gereksinim ve incelemeleriyle ilgili koşullar eklenmelidir.
- Kritik bilgiye erişim hakkı olan çalışanlar ile gizlilik anlaşmaları imzalanmalıdır.
- Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenmelidir.
- Çalışanlara telefon görüşmeleri yaparken civardakiler tarafından işitilebileceği veya dinlenebileceği için hassas bilgilerin konuşulmaması hatırlatılmalıdır.
- İş tanımı değişen veya kurumdan ayrılan kullanıcıların erişim hakları hemen silinmelidir.
- Kurum bilgi sistemlerinin işletilmesinden sorumlu personelin konularıyla ilgili teknik bilgi düzeylerini güncel tutmaları çalışma sürekliliği açısından önemli olduğundan eğitim planlamaları periyodik olarak yapılmalı, bütçe ayrılmalı eğitimlere katılım sağlanmalı ve eğitim etkinliği değerlendirilmelidir.
- Yetkiler "görevler ayrımı" ve "en az ayrıcalık" esaslı olmalıdır. "Görevler ayrımı " rollerin sorumlulukların paylaştırılması ile ilgilidir ve bu paylaşım sayesinde kritik bir sürecin tek kişi tarafından kırılma olasılığı azaltılır." En az ayrıcalık" ise kullanıcıların gereğinden fazla yetkiyle donatılmamaları ve sorumlu oldukları işleri yapabilmeleri için yeterli olan asgari erişim yetkisine sahip olmaları demektir.
- Kritik bir görevin tek kişiye bağımlılığını azaltmak ve aynı işi daha fazla sayıda çalışanın yürütebilmesini sağlamak amacıyla, bir sıra dahilinde çalışanlara görev ve sorumluluk atanmalıdır. Böylece kritik bir iş birden fazla kişi tarafından öğrenilmiş olacaktır.
- Çalışanlar kendi işleri ile ilgili olarak bilgi güvenliği sorumlulukları, riskler görev ve yetkileri hakkında periyodik olarak eğitilmelidir. Yeni işe alınan elemanlar içinde bu eğitim, oryantasyon sırasında verilmelidir.
- Çalışanların başka görevlere atanması ya da işten ayrılması durumlarında işletilecek süreçler tanımlanmalıdır. Erişim yetkilerinin, kullanıcı hesaplarının, laptop, akıllı kart vs. gibi donanımların iptal edilmesi, geri alınması veya güncellenmesi sağlanmalı, varsa devam eden sorumluluklar kayıt altına alınmalıdır.

2.4 Fiziksel Güvenlik

Fiziksel güvenlik kurum personeli ve kritik kurumsal bilgilerin korunması amacıyla sistem odasına, kurumsal bilgilerin bulundurulduğu sistemlerin yer aldığı tüm çalışma alanlarına ve kurum binalarına yetkisiz girişlerin yapılmasını önlemek amacını taşımaktadır.

- Kurumun fiziksel olarak korunması, farklı koruma mekanizmaları (Kartlı giriş sistemi) ile donatılması temin edilmelidir.

- Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binada ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanmalı ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilmelidir.
- Kurum dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili görevliler gözetiminde gerçekleştirilmelidir.
- Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin güncelliği sağlanmalıdır.
- Kritik sistemler özel sistem odalarında tutulmalıdır.
- Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmalı, yangın ve benzer felaketlere karşı koruma altına alınmalıdır.
- Kuruma giriş yapacak ziyaretçi veya kurye teslimatları yetkili görevliler gözetiminde gerçekleştirilmelidir.
- Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve kontrol altında tutulması temin edilmelidir.
- Fotoğraf, video, ses vb. kayıt cihazlarının yetki verilmeyen kişiler tarafından güvenli alanlara sokulması yasaklanmalıdır.

2.5 İnternet Erişimi

Prizma A.Ş., çalışanlarına güvenli internet erişimi için sahip olması gereken standartları belirlemektedir. İnternetin uygun olmayan kullanımı, kurumun yasal yükümlülükleri, kapasite kullanımı ve kurumsal imajı açısından istenmeyen sonuçlara neden olabilir. Bilerek ya da bilmeyerek bu türden olumsuzluklara neden olunmaması ve internetin kurallarına, etiğe ve yasalara uygun kullanımının sağlanmasını amaçlamaktadır. Bütün kullanıcılar ve sistem yöneticileri aşağıdaki internet erişim ve kullanım yönteminden dışarıya çıkmamalıdır.

- Kurumun bilgisayar ağı erişim ve içerik denetimi yapan bir firewall üzerinden internete çıkacaktır. Ağ güvenlik duvarı kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır. Ağın dışından ağın içine erişimin denetimi burada yapılır. Güvenlik duvarı aşağıda belirtilen hizmetlerle birlikte çalışarak ağ güvenliğini sağlayabilmelidir.
- Kurumun ihtiyacı doğrultusunda saldırı tespit ve önleme sistemi güvenlik duvarıyla birlikte olup tüm kontroller güvenlik duvarı üzerinden yapılmaktadır.
- Ancak yetkilendirilmiş sistem yöneticileri internete çıkarken bütün servisleri kullanma hakkına sahiptir.(ftp, telnet)
- Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemeli ve dosya indirimi yapılmamalıdır.
- Üçüncü şahısların kurum internetini kullanmaları bilgi işlem sorumlularının izni ve bu konudaki kurallar dahilinde gerçekleştirilebilecektir.

2.6 Zararlı İçerik Yönetimi

2.6.1 Kurum Çalışanları

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

2.6.2 Anti-Virüs Prosesi

Virüs problemlerine karşı tavsiye edilen adımlar;

- Anti-virüs güncellemeleri, her makinanın lokalinde otomatik update şeklinde gerçekleşmektedir.
- Bilinmeyen kişilerden e-posta ile birlikte gelen dosya ve makroları kesinlikle açılmamalı, Bu ekli dosyalar hemen silinmeli, daha sonra silinmiş öğelerden tekrardan temizlenmelidir.
- Spam, ve junk e-mailleri mail uygulamalarında kategorize edilmeli ve düzenli olarak silinmelidir.
- Bilinmeyen ve şüpheli kaynaklardan dosya indirilmemelidir.
- Bilinmeyen kaynaklardan gelen CD/DVD, Usb disk ve benzeri depolama ünitelerine virüs tarama işlemi yapılmalıdır.
- Kritik data ve sistem konfigürasyonlarını düzenli aralıklar ile yedeklenmeli ve güvenli bir yerde tutulmalıdır.

2.7 Sunucu Güvenliği

Bu politikanın amacı kurumun sahip olduğu sunucularının temel güvenlik konfigürasyonları için standartları belirlemektir. Bu politikanın etkili kullanılması ile Prizma A.Ş. bünyesindeki bilgilere ve teknolojiye yetkisiz erişimler minimize edilecektir.

2.7.1 Sahip Olma ve Sorumluluklar

Kurum bünyesindeki bütün dâhili sunucuların yönetiminden sadece yetkilendirilmiş sistem yöneticileri sorumludur.

Bütün sunucular (kurumun sahip olduğu) sunucu envanterine kayıtlı olmalıdır ve aşağıdaki bilgileri içermelidir;

- Sunucuların yeri ve sorumlu kişi
- Donanım ve işletim sistemi
- Ana görevi ve üzerinde çalışan uygulamalar
- İşletim sistemi versiyonları ve yamalar

2.7.2 Uyumluluk

- Denetimler Kurum içi yetkililer tarafından belli aralıklarda yapılmalıdır.
- Denetimlerde kurumun işleyişine zarar vermemesi için maksimum gayret gösterilmelidir.

2.7.3 İşletim

- Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir.
- Sunucuların yazılım ve donanım bakımları 1 aylık sürelerde, sistem yöneticileri tarafından yapılmalıdır.
- Sistem odalarına yetkisiz girişler engellenmelidir. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalıdır.

2.8 Ağ Yönetimi

Kurumun bilgisayar ağında ve sistem odası içerisinde yer alan bilgilerin ve ağ alt yapısının güvenliği, gizlilik, bütünlük ve erişilebilirlik kavramları göz önüne alınarak sağlanmalıdır. Uzaktan erişim hususunda özel önem gösterilmelidir. Yetkisiz erişimle ilgili tedbirler alınmalıdır. Ağın güvenliği ve sürekliliğini sağlamak amacıyla bir takım kontroller gerçekleştirilmelidir. Ağ Yönetimi politikası bu gereksinimleri karşılayan kuralları belirlemek amacıyla geliştirilmiştir. Prizma A.Ş. network ağının sistem ve ağ yöneticileri, teknik sorumluları faaliyetlerini Ağ Yönetimi Politikasına uygun şekilde yürütmekle yükümlüdür.

- Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için özel kontroller uygulanmalıdır.
- Ağ servisleriyle ilgili standartlarda, erişimine izin verilen ağlar ve ağ servisleri ve ilgili yetkilendirme yöntemleri belirtilmelidir.
- Ağ üzerinde kullanıcının erişeceği servisler kısıtlanmalıdır.
- Sınırsız ağ dolaşımı engellenmelidir.
- İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden teknik önlemler alınmalıdır.
- Ağ erişimi gerek duyulduğunda VPN, VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılmalıdır.
- Farklı VLAN kullanılmak suretiyle sunucu ve yönetilebilir cihazlar, kullanıcılar için ayrı mantıksal alanlar oluşturulmalıdır.
- Gerek görülen uygulamalar için e-posta, tek yönlü dosya transferi, çift yönlü dosya transferi, etkileşimli erişim, güne ve günün saatine bağlı erişim gibi uygulama kısıtlamalarıyla ağ erişimi denetimi yapılmalıdır.
- Ağ üzerindeki yönlendirme kontrol edilmelidir.
- Bilgisayar ağına bağlı bütün makinelerde kurulum ve konfigürasyon parametreleri kurumun güvenlik politika ve standartlarıyla uyumlu olmalıdır.
- Sistem tasarım ve geliştirmesi yapılırken kurum tarafından onaylanmış olan ağ ara yüzü ve protokolleri kullanmalıdır.

- İnternet trafiği erişim ve kullanımı izleme politikası ve ilgili standartlarda anlatıldığı şekilde izlenebilecektir.
- Bilgisayar ağındaki adresler, ağa ait konfigürasyon ve diğer tasarım bilgileri 3.şahıs ve sistemlerin ulaşamayacağı bir şekilde saklanmalıdır.
- Ağ üzerindeki firewall üzerinde, ilgili konfigürasyon dokümanlarında belirtilen servisler dışında tüm servisler kapatılmalıdır.
- Bilgisayar ağıyla ilgili sorumlulukları desteklemek amacıyla ağ dokümantasyonu hazırlanmalı, ağ cihazlarının güncel konfigürasyon bilgileri saklanmalı ve yedeklenmelidir.

2.8.1 Ağ Cihazları Güvenliği

Bu politika kurumun ağındaki yönlendirici (router) ve anahtarların (switch) sahip olması gereken minimum güvenlik konfigürasyonlarını tanımlamaktadır. Kurum içerisinde kullanılan ve ağına bağlı olan tüm cihazlarda aşağıdaki standartlar geçerlidir.

- Bilgisayar ağında bulunan tüm cihazların IP ve MAC adres bilgileri envanter dosyasında yer almalıdır.
- Yönlendirici ve anahtarlar kurumun yönetim sisteminde olmalıdır.
- Yazılım ve firmware güncellemeleri önce test ortamlarında denendikten sonra çalışma günlerinin dışında üretim ortamına taşınacaktır.
- Bilgisayar ağında bulunan kabinetler, elektrik fişleri, aktif cihazlar, UTP kabloları, cihazların portları etiketlenecektir.
- Kritik cihazlarda "BU CİHAZA YETKİSİZ ERİŞİMLER YASAKLANMIŞTIR" ibaresi bulunmalıdır ve yetki dışı personelin bu cihazlara erişimi kesinlikle yasaklanmalıdır.

2.8.2Kablosuz Erişim

Tüm personelin kurum içerisinde kullandıkları kablosuz haberleşme cihazları veya kablosuz veri transferi sağlayabilen herhangi bir cihazın güvenlik adımlarının belirlenmesi gerekmektedir. Sadece bu güvenlik kriterlerine uyan cihazlar kurumun bünyesinde kullanılabilir.

2.9 Değişim Yönetimi

Değişim yönetimi kurumun bilgi sistemlerinde yapılması gereken konfigurasyon değişikliklerinin güvenlik ve sistem sürekliliğini aksatmayacak şekilde yürütülmesine yönelik politikaları belirlemektedir. Tüm bilgi sistemleri ve bu sistemlerinden işletilmesinden sorumlu personel bu politikanın kapsamında yer almaktadır.

- Bilgi sistemlerinde değişiklik yapmaya yetkili personelin ve yetki seviyeleri dokümante edilmelidir.
- Yazılım ve donanım envanteri oluşturularak yazılım sürümleri kontrol edilmelidir.
- Değişiklikler gerçekleştirilmeden önce güvenlik politikaları yöneticisi ve ilgili diğer yöneticilerin onayı alınmalıdır.
- Tüm sistemlere yönelik konfigürasyon dokümantasyonu oluşturulmalı, yapılan her değişikliğin bu dokümantasyonda güncellenmesi sağlanarak kurumsal değişiklik yönetimi ve takibi temin edilmelidir.

- Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanmalı ve ilgili yöneticiler tarafından onaylanması sağlanmalıdır.
- Yapılan değişiklikler sonrasında oluşabilecek güvenlik zafiyetleri Güvenlik Açıkları Tespit Etme politikası çerçevesinde kontrol edilmelidir.
- Teknoloji değişikliklerinin kurumun sistemlerine etkileri belirli aralıklarla gözden geçirilmelidir.

2.10 Bilgi Sistemleri Yedekleme Politikası

Bilgi sistemlerinde oluşabilecek hatalar karşısında sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için sistemler üzerindeki konfigurasyon, sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmesi gerekir. Bu politika yedekleme kurallarını tanımlamaktadır. Tüm kritik bilgi sistemleri ve bu sistemlerin işletilmesinden sorumlu personel bu politikanın kapsamında yer almaktadır.

- Bilgi sistemlerinde oluşabilecek hatalar karşısında; sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigurasyon, sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmesi gerekmektedir.
- Kurumsal kritik verilerin saklandığı sistemler ile sistem kesintisinin kritik olduğu sistemlerin bir varlık envanteri çıkartılmalı ve yedekleme ihtiyacı bakımından sınıflandırılarak dokümante edilmelidir.
- Yedekleri alınacak sistem, dosya ve veriler dikkatle belirlenmeli ve yedeği alınacak sistemleri belirleyen bir yedekleme listesi oluşturulmalıdır.
- Yedek ünite üzerinde gereksiz yer tutmamak üzere, kritiklik düzeyi düşük olan veya sürekli büyüyen izleme dosyaları yedekleme listesine dâhil edilmemelidir.
- Yedeklenecek bilgiler değişiklik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilmeli ve güncellenmelidir.
- Yeni sistem ve uygulamalar devreye alındığında yedekleme listeleri güncellenmelidir.
- Yedekleme işlemi için geçerli sayı ve kapasitede yedek üniteler seçilmeli ve temin edilmelidir. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilmelidir.
- Yedekleme ortamlarının düzenli periyotlarda test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanmalıdır.
- Olası hizmet kesintilerinin bitiş süresini hesaplamak için yedekten geri yükleme senaryoları oluşturulmalı ve bu senaryoların süreleri test edilmelidir.
- Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanmalıdır.
- Yedekleme standardı ile doğru ve eksiksiz yedek kayıt kopyalarının bir felaket anında etkilenmeyecek bir ortamda bulundurulması gerekmektedir.
- Veri Yedekleme Standardı; yedekleme sıklığı, kapsamı, gün içinde ne zaman yapılacağı, ne koşullarda ve hangi aşamalarla yedeklerin yükleneceği ve yükleme sırasında sorunlar çıkarsa nasıl geri dönüleceği, yedekleme ortamlarının ne şekilde işaretleneceği, yedekleme testlerinin

ne şekilde yapılacağı ve bunun gibi konulara açıklık getirecek şekilde hazırlanmalı ve işlerliği periyodik olarak gözden geçirilmelidir.

2.11 Bakım

Prizma A.Ş. bilgi sistemlerinde kullanılan Web hizmetleri, Mail hizmetleri ve buna benzer yönetimi Prizma A.Ş.'ye ait sistemlerin bakımı ile ilgili politikaları belirlemektedir.

- Kurum sistemlerinin tamamı periyodik bakım güvencesine alınmalıdır. Bunun için gerekli zaman planlamaları yapılmalıdır.
- Üreticilerden sistemler ile ilgili bakım prosedürleri sağlanmalıdır.
- Bakım yapıldıktan sonra tüm sistem dokümantasyonu güncellenmelidir.
- Sistem bakımlarının ilgili politika ve standartlar tarafından belirlenmiş kurallara aykırı bir sonuç vermediğinden ve güvenlik açıklarına yol açmadığından emin olmak için periyodik güvenlik ve uygunluk testleri yapılmalıdır.
- Sistem bakımından sonra bir güvenlik açığı yaratıldığından şüphelenilmesi durumunda " Prizma A.Ş. "Bilgi Güvenlik Politikaları" uyarınca hareket edilmelidir.
- Dış kaynak kullanarak yapılacak bakımlar mutlaka sistem yöneticisi gözetiminde yapılmalıdır.
- Bakım hizmetlerinden kaynaklı olası kesintilere karşı , gaz dağıtım firmaları, müşteriler ve çalışanlar mail, telefon ve web sitesinden yayınlanacak duyurularla uyarılmalıdır.

2.12 Personel ve Eğitim

Bilişim sistemlerinden kaynaklanan sorunların büyük bir kısmı insanlar tarafından yapılan hata, ihmal ve suiistimallerden kaynaklanmaktadır. Bu nedenle kurumların, personelin hata yapma riskini düşürecek kontroller kurmaları önem kazanmaktadır. Bu, uygun personel ve eğitim politikalarının benimsenmesi sayesinde başarılabilir.

Farklı kişiler tarafından yerine getirilmesi gereken görevlerin ayrılması, işlemlerin yetkilendirilmesi, kaydedilmesi ve varlıkların korunması açısından önemlidir. Görevlerin ayrılması, bir kişinin diğer bir kişinin yaptığı faaliyetleri kontrol etme imkânı vermesi nedeniyle de hata riskini düşürür. Bu politika, personel ve eğitim hakkındaki kriterleri ortaya koymaktadır.

- Eğitim stratejisi ile bilişim stratejisi birbiriyle aynı doğrultuda olmalıdır. Bu sayede bilişim stratejisinin başarılı bir şekilde uygulanması sağlanır.
- Personelin sisteme tanımlanması ve yetkilerinin belirlenmesi işlemi yönetim tarafından onaylanmış bir prosedür dâhilinde yapılmalıdır.
- Kurum yapısı içinde yetki ve sorumluluklar açıkça tanımlanmış olmalıdır.
- İşe alınan personel mevcut yapı ve güvenlik sistemleri hakkında bilgilendirilmelidir.
- Kurum tarafından, bilişim sistemini kuran, geliştiren ve kullanan personelin görev tanımları yapılmış olmalıdır.
- Personelin işe alınması, görev yerlerinin değiştirilmesi, görevlerine son verilmesi ve performanslarının değerlendirilmesinde güvenlik göz önünde bulundurulmalıdır.

- Kurum çalışanları işin gerektirdiği vasıflara sahip olmalı, yeterli seviyede eğitim almalı ve yeteneklerine uygun işlerde çalıştırılmalıdır.
- Bilişim alanında istihdam edilecek daimi personel ile sözleşmeli veya danışman olarak çalıştırılacak personelin seçiminde, bu kişilerin işin gerektirdiği öğrenim ve eğitimi almış yetenekli ve dürüst kişiler olmalarına azami dikkat gösterilmelidir.
- Bilişim yöneticileri, personelin bugün ve yakın gelecekte ihtiyaç duyulan yeteneklere sahip olup olmadıklarını bilmeli ve onlara bu ihtiyaçları karşılayacak eğitimi verdirmelidir. Bilişim eğitimi pahalı bir eğitim olduğu için eğitim planları ve bütçeleri kontrol edilmelidir.
- Eğitim programı yazılım ekibi için iş süreçleri gözetilerek yapılmalıdır, bu konuda online eğitim sistemleri alternatif olarak değerlendirilmelidir.
- Yazılım ekibinin kullandığı uygulamalarda versiyon takibi yapılmalı ve eğitim programına dahil edilerek gelişen teknolojilerin kullanılması sağlanmalıdır.
- Bilişim personelinin kurumun mevcut ve uzun vadeli politikaları ile paralellik gösteren bir şekilde sertifika programlarına katılımı ve sertifikasyonlarını tamamlaması gerekmektedir.
- Görevlerin ayrılması bir kişinin diğer bir kişinin yaptığı faaliyetleri kontrol etme imkânı verecek şekilde olmalıdır.
- Çalışanlar görev ve sorumluluklarının neler olduğunu bilmelidir.
- Yönetim, kullanılan kontrollerin ne derecede etkin olduğunu değerlendirmelidir.
- Personelin faaliyetleri, resmi çalışma prosedürleri, denetim ve gözden geçirme yollarıyla kontrol altında tutulmalıdır.
- Bütün çalışanlar aktif gözetim ve yönlendirmeye tabi tutularak desteklenmelidir.

2.13 Doküman Paylaşım ve Belgelendirme

Kurumun belgeleme politikalarının yetersiz olması, personelin hatalı veya yetkisiz işlem yapma riskini yükseltebilir. Ayrıca sistemde bir hata meydana geldiği zaman, işlemler yeterli bir şekilde belgelenmemişse, hatanın sebebinin tespiti de güçleşebilir.

- Bilişim sisteminin yapısı ile bütün iş ve işlemler açıkça belgelenmeli ve bu belgeleme inceleme amacıyla kolaylıkla ulaşılabilir durumda olmalıdır.
- İş akışları uygun şekilde belgelenmelidir.
- Belgeleme, tarih belirtilerek yapılmalı ve yedek kopyaları güvenli bir yerde muhafaza edilmelidir.
- Girdi türleri ve girdi form örnekleri belgelenmelidir.
- Ana dosyalar ile diğer dosyaların içerik ve şekilleri belgelenmelidir.
- Çıktı form örnekleri ve çıktıların kimlere dağıtılacağı belgelenmelidir.
- Programların nasıl test edildiği ve test sonuçları belgelenmelidir.
- Bütün program değişikliklerinin detayları belgelenmelidir.

2.14 Destek Ve Uzaktan Yardım

Destek ve uzaktan yardım merkezi kurumun müşterilerle bağlantı kurduğu ilk noktadır. Yazılım geliştirme, iş geliştirme ve problemlerin giderilmesi açısından çok önemli bir noktadır. Kurumun bilgi birikimi ve kurumsal hafızanın oluştuğu önemli noktalardandır.

Destek ve uzaktan yardım Merkezi personeli mesai saatleri içinde, e-mail ve telefonla ulaşan sorunların çözümü konusunda yetkilidir. İletilen sorunlar ve isteklere makul bir sürede cevap vermek, çözüm yollarını araştırmak, gerekli birimlerle iletişimi sağlamak, varsa yapılacak iyileştirmelerin zamanında yapılarak müşterilerin kullanımına açıldığını bildirmek ve Destek ve uzaktan yardım prosedürüne göre hareket etmek Destek ve uzaktan yardım personelinin sorumluluğundadır.