

Doküman Kodu: BGYS-0007

BİLGİ SİSTEMLERİ KABUL EDİLEBİLİR KULLANIM POLİTİKASI OLUŞTURMA KILAVUZU

SÜRÜM 1.00

18.04.2008

Hazırlayan: Doğan Eskiyörük

ÖNSÖZ

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'nin misyonu, "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında Türkiye'nin teknolojik bağımsızlığını sağlamak ve sürdürmek için, bilimsel ve teknolojik çözümler üretmek ve uygulamaktır". Bu ana hedef göz önünde bulundurularak belirlenen "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında yeni teknolojilerin geliştirilmesine öncülük eden uluslararası bilim, teknoloji ve üretim merkezi olmak" vizyonuna ulaşılabilmesi ve ülkenin ihtiyacı olan teknolojilerin geliştirilmesi için Enstitü'nün akredite test ortam ve laboratuvarlarında temel ve uygulamalı araştırmalar yapılmakta ve ihtiyaç sahiplerine teknik destek sağlanmaktadır.

Bu doküman, BGYS (Bilgi Güvenliği Yönetim Sistemi) kurmak isteyen kurumlar için yardımcı kaynak olarak hazırlanmıştır. Tüm kurum ve kuruluşlar bu dokümandan faydalanabilir.

Bu dokümanda anlatılanlar tamamen tavsiye niteliğindedir. UEKAE, yapılan uygulamalardan doğabilecek zararlardan sorumlu değildir. Bu doküman UEKAE'nin izni olmadan değiştirilemez.

BİLGİLENDİRME

Bu dokümanın oluşturulmasında emeđi geen Ađ Güvenliđi personeline ve dokümanı gözden geirip fikirlerini öne sürerek dokümanın olgunlaşmasına katkıda bulunan Ali Dinkan ve Fikret Ottekin'e teşekkürü bor biliriz.

İÇİNDEKİLER

1. GİRİŞ	5
1.1 Amaç ve Kapsam.....	5
1.2 Hedeflenen Kitle.....	5
1.3 Kısaltmalar.....	5
2. KABUL EDİLEBİLİR KULLANIM POLİTİKASI NEDEN GEREKLİDİR?	6
3. POLİTİKANIN OLUŞTURULMASI	7
4. KULLANICILARIN POLİTİKADAN HABERDAR EDİLMESİ VE EĞİTİLMESİ.....	8
5. POLİTİKANIN UYGULANMASI VE TEKNİK YÖNDEN DESTEKLENMESİ.....	8
6. POLİTİKANIN GÜNCELLENMESİ.....	9
7. ÖRNEK KABUL EDİLEBİLİR KULLANIM POLİTİKASI	9
7.1 Giriş	9
7.2 Kapsam	9
7.3 Sorumluluklar	9
7.4 Politika.....	10
7.4.1 Genel Kurallar.....	10
7.4.2 Kabul Edilebilir İnternet Kullanım Kuralları.....	10
7.4.3 Kabul Edilebilir E-posta Kullanım Kuralları.....	12
7.4.4 Kabul Edilebilir Telekomünikasyon Cihazları Kullanım Kuralları.....	14
7.4.5 Kabul Edilebilir Yazılım Kullanım Kuralları	15
7.4.6 Kabul Edilebilir Taşınabilir Bilgi İşleme Cihazları Kullanım Kuralları	16
7.5 Uygulama ve Ceza.....	17
7.6 Gözden Geçirme ve Onay.....	17
KAYNAKÇA	18

1. GİRİŞ

Bilgi sistemleri; iletişim, yeni müşteri bulma, yeni pazarlara açılma, iş ortaklarıyla daha yakından çalışma gibi pek çok konuda kurumlar için yenilikler ve avantajlar getirmektedir. Bu sebeple kurumlar internet ve iletişim alt yapısına büyük yatırımlar yapmaktadır. Büyük bütçeler ayrılarak gerçekleştirilen bu sistemlerin amacına uygun biçimde ve kurum çıkarları doğrultusunda kullanılmasını sağlamak için kabul edilebilir kullanım politikaları oluşturmak şarttır.

1.1 Amaç ve Kapsam

Bu kılavuzun amacı bilgi sistemleri için kabul edilebilir kullanım politikalarının doğru oluşturulmasını sağlamaktır. Bunun için bu politikaların neden gerekli olduğu, içerisinde neler bulunması gerektiği ve örnek politikalar bu kılavuzda yer almaktadır.

1.2 Hedeflenen Kitle

Bu kılavuz bilgi sistemleri için kabul edilebilir kullanım politikası oluşturmak isteyen veya mevcut politikalarını gözden geçirmeyi planlayan kişiler için oluşturulmuştur.

1.3 Kısaltmalar

BGYS : Bilgi Güvenliği Yönetim Sistemi

UEKAE : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

2. KABUL EDİLEBİLİR KULLANIM POLİTİKASI NEDEN GEREKLİDİR?

İnternet altyapısını kullanmak kurumlar için pek çok avantaj getirmektedir fakat aynı zamanda çalışanların zamanlarını işle ilgili olmayan konulara harcamaları için de çok elverişli bir ortam oluşturmaktadır. İnternette gezinmenin yol açtığı başlıca sorunlar şunlardır:

Çalışan verimliliği: Sosyal ağ sitelerinin, mesajlaşmanın, internet üzerinden alışverişin çok popüler olması ve çalışanların bu gibi iş dışı aktivitelere çalışma saatleri içerisinde zaman ayırmaları verimliliği oldukça olumsuz etkileyebilmektedir.

Ağ kaynaklarının kullanımı: Ağ kaynaklarının görüntü, ses ve resim indirmek gibi yüksek bant genişliğine ihtiyaç duyan işler için kullanılması kurumun iş yapmasını ve verimliliğini olumsuz yönde etkiler.

Güvenlik: Kurum kullanıcılarının interneti kullanması internet ortamındaki tüm saldırganlara ve zararlı yazılımlara maruz kalmasına olanak verir.

Yasal yükümlülükler: Çalışanların uygun olmayan sitelerde dolaşmaları veya kurum kaynaklarını kullanarak yasa dışı aktivitelerde bulunmaları kurumu yasal açıdan büyük sıkıntılara sokabilir.

Kurum itibarının zedelenmesi: Çalışanların internet üzerinde yasadışı veya uygunsuz sitelere bağlanması veya çalışanların kurum kimliğini kullanarak yaptıkları uygunsuz hareketler yüzünden kurum itibarı zedelenebilir.

Ayrıca yukarıda bahsedilen olumsuzluklara ek olarak taşınabilir cihazların çalınması, e-posta ve telefon sistemlerinin uygunsuz kullanılması ve bunlara benzer olumsuzluklar da eklenebilir. İşte tüm bunların önlenmesi için, kurumun ihtiyaçlarına uygun bir “Kabul Edilebilir Kullanım Politikası” oluşturulma, bu politika ilgili tüm kişi ve kurumlara duyurulmalı ve uygun teknik kontroller kullanılarak uygulanmalıdır.

3. POLİTİKANIN OLUŞTURULMASI

Kabul Edilebilir Kullanım Politikası'nın oluşturulma amacı aşağıdaki maddelerle özetlenebilir:

- Kurum varlıklarının ve internetin kullanımıyla ilgili kurum politikasını net bir şekilde ifade etmek.
- Farkındalığı arttırarak güvenlik tehditlerine karşı kurumu korumak.
- Kurumu olası yasal sorumluluklardan korumak.
- Kurum kaynaklarının kurum çıkarları doğrultusunda ve daha etkin bir şekilde kullanılmasını sağlamak.

Kabul Edilebilir Kullanım Politikası oluşturulurken bazı hususlar dikkate alınmalıdır. Bu hususlar şu şekilde özetlenebilir:

- Politikanın oluşturulması sırasında kurumun her bölümünün görüşü alınmalı ve kurumun tamamının iş gereksinimlerini karşılayacak bir politika oluşturulmalıdır.
- Politika açık ve anlaşılır olmalıdır. Kullanıcıların yapmaması gerekenler, uygulanabilecek cezalar, kullanıcıların hangi işlemlerinin izlendiği politikanın içerisinde yer almalıdır.
- Politikanın kimleri kapsadığı açıkça belirtilmelidir.
- Varlıkların mesai saatleri dışında kullanılması ile ilgili istisnalar belirtilmelidir. (Örneğin mesai saatleri içerisinde alışveriş sayfalarının izlenmesi yasakken mesai saatleri dışında bu sitelere girilmesine izin verilebilir.)
- Kullanıcılara güvenlikle ilgili hatırlatmalar yapılmalıdır. Örneğin internet üzerinden şifresiz olarak gönderilen bilginin ele geçirilebileceği, kurum için kritik olan verilerin ancak tanımlı prosedürler uyarınca paylaşılacağı gibi konular politikada yer almalıdır.
- Kullanıcının yaptıklarından kurum sorumlu tutulabilir. Bunun için kullanıcılara yaptıklarının yasal sorunlar doğurabileceği ve bu gibi durumlardan sorumlu oldukları hatırlatılmalıdır.
- Politika kullanıcılar tarafından erişilebilir olacak şekilde saklanmalıdır. Ayrıca yeni personelin işe başlamadan önce politikayı okuması sağlanmalıdır.

- Uygulanacak teknik kısıtlamalar politikada açıkça yer almalıdır. Örneğin e-posta eklentisi olarak hangi dosyalara izin verildiği, eklenti boyutunun en fazla ne kadar olabileceği gibi hususlar politikada yer almalıdır.

4. KULLANICILARIN POLİTİKADAN HABERDAR EDİLMESİ VE EĞİTİLMESİ

Her politika gibi “Kabul Edilebilir Kullanım Politikası”nın benimsenmesi ve uygulanması da zaman alır. Kullanıcılar, daha önce çalıştıkları yerlerde veya öğrenim gördükleri kurumlarda kaynakları daha rahat ve sonuçlarını pek düşünmeden kullanmaya alışmış olabilirler. Bu alışkanlıklarının değişmesi için zaman gerekir. Bu değişimi sağlamanın en iyi yolu politikayı kurum kültürünün bir parçası haline getirmek ve kurum politikaları ile ilgili periyodik eğitimler vermektir. Ayrıca zaman zaman politikanın önemli noktalarını hatırlatan e-postalar göndermek politikanın kullanıcılar tarafından unutulmamasını sağlayacaktır.

Politika aynı zamanda gerektiği zaman kolay ulaşılabilecek şekilde saklanmalı ve sergilenmelidir. Kurumun intranet sitesi bunun için en uygun ortamlardan biridir.

5. POLİTİKANIN UYGULANMASI VE TEKNİK YÖNDEN DESTEKLENMESİ

“Kabul Edilebilir Kullanım Politikası”nın oluşturulması politikada belirtilen kuralların uygulanması için yeterli değildir. Bu kurallar uygun teknik kontrollerle desteklenmeli ve gerektiğinde uyulması zorunlu kılınmalıdır. Bunun için mevcut pek çok yazılım mevcuttur.

Belirlenen politikaya uygun kontrolleri uygulayabilecek yazılımlar kullanılmalıdır. Kullanılacak yazılımlarda aşağıdaki özelliklerin bulunması avantaj sağlayacaktır:

- **Etkin raporlama:** Kullanılan yazılım, grafikler ve raporlar kullanarak belirlenen politikaya uymayan kullanıcıları, hangi işlemleri gerçekleştirdiklerini, bu işlemlerin ne zaman yapıldığı ve benzeri konuları raporlayabilmelidir.
- **Akıllı filtreleme:** Yazılımda tanımlanacak filtreler ve bu filtrelerin yapacakları açık olmalıdır. Gerektiğinde yasaklanan ve/veya izin verilen şeyler açıkça görülebilmelidir.
- **Esnek izleme seçenekleri:** Yazılım belirlenen politikaya uygun olarak günün değişik saatlerinde, değişik izleme seçenekleri sunabilmeli ve filtrelemeyi buna göre yapabilmelidir.

- **Güncellenebilirlik:** Engellenecek şeylerin (örneğin sitelerin) listesi yazılım üreticisi tarafından periyodik olarak güncellenmelidir.
- **Yüksek performans:** Yazılım, kullanıcıların çalışmalarını yavaşlatmadan ve ağ üzerine çok fazla yük getirmeden çalışabilmelidir.
- **Ölçeklenebilirlik:** Kurum büyüdükçe veya ihtiyaçlar değiştikçe yazılım yeni ihtiyaçlara cevap verebilecek şekilde ölçeklenebilmelidir.
- **Destek:** Kurum personeli tarafından giderilemeyen sorunlar oluşması veya yazılımda hatalar çıkması gibi durumlarda yazılım için satın alınan firmadan veya yazılımın üreticisinden destek alınabilmelidir.

6. POLİTİKANIN GÜNCELLENMESİ

Kurumun ihtiyaçları, iş yapma biçimi, kullandığı teknoloji, sahip olduğu altyapı ve bunlar gibi kullanıcıların kurum sistemlerini kullanma biçimlerini etkileyecek diğer unsurlar zaman içerisinde değişebilir. Bu durumda yeni ihtiyaçları göz önünde bulundurarak mevcut politikanın güncellenmesi gerekir. Politika gözden geçirme ve güncelleme işlemleri kurum tarafından periyodik olarak yapılmalı, bu işi yapmakla sorumlu personel ve güncelleme çalışmasının hangi sıklıkla yapılacağı da politika belgesinde açıkça belirtilmelidir.

7. ÖRNEK KABUL EDİLEBİLİR KULLANIM POLİTİKASI

7.1 Giriş

Kabul Edilebilir Kullanım Politikası, <Kurum Adı> (bundan sonra kurum olarak adlandırılacaktır) bilgi ve iletişim varlıklarının iş amaçlarına uygun kullanılması için gerekli kuralları belirler.

7.2 Kapsam

Tüm kurum çalışanları, geçici görevliler ve kurumun bilgi varlıklarına erişimine izin verilmiş olan diğer kurum/kuruluş/şirket çalışanları bu politikada belirtilen kurallara uymak zorundadır.

7.3 Sorumluluklar

Kabul Edilebilir Kullanım Politikasının geliştirilmesinden, uygulanmasından ve yenilenmesinden sorumludur.

Kabul Edilebilir Kullanım Politikasının kullanıcılar tarafından bilinmesini ve anlaşılmasını sağlamaktan, diğer tüm politika ve prosedürlerin bu politika ile tutarlı olmasından yönetim sorumludur.

Bu politikanın kapsamına dahil olan tüm kullanıcılar Kabul Edilebilir Kullanım Politikasını ve ilgili politika ve prosedürdeki kuralları bilmekten ve bu kurallara uymaktan, sorumludurlar.

7.4 Politika

7.4.1 Genel Kurallar

1. Kurumun bilgi ve haberleşme sistemleri ve donanımları (İnternet, e-posta, telefon, çağrı cihazları, faks, bilgisayarlar, mobil cihazlar ve cep telefonları da dahil olmak üzere) kurum işlerinin yürütülmesi için kullanılmalıdır. Bu sistemlerin yasa dışı, rahatsız edici, kurumun diğer politika, standart ve rehberlerine aykırı veya kuruma zarar verecek herhangi bir şekilde kullanımı bu politikanın ihlal edildiği anlamına gelir.
2. Kurum bu sistemleri ve bu sistemlerle gerçekleştirilen aktiviteleri izleme, kaydetme ve periyodik olarak denetleme hakkını saklı tutar.
3. Aşağıdaki kurallar uyulması gereken kuralların kapsamlı bir listesi olarak düşünülmemelidir. Gerçekleştirilen aktiviteler buradaki kurallarla tutarlı olmalıdır.

7.4.2 Kabul Edilebilir İnternet Kullanım Kuralları

7.4.2.1 Kurumsal Kullanım

1. Kurum internet kaynakları öncelikli olarak resmi ve onaylı kurum işlerinin gerçekleştirilmesi için kullanılmalıdır.
2. Kurum çıkarlarıyla çakışmadığı sürece internet kaynaklarının kişisel kullanımına kısıtlı olarak izin verilmektedir.
3. Kurum internet kaynakları kullanılırken ilgili yasa ve düzenlemelere uyulmalıdır.
4. Kullanıcılar kendi kullanıcı hesaplarıyla internet üzerinde gerçekleştirilen tüm işlemlerden sorumludur. Bunun için kullanıcılar kimlik bilgilerini uygun şekilde saklamalı ve başkaları ile paylaşmamalıdır.

7.4.2.2 Uygunsuz Kullanım

1. Kurum internet kaynakları hiçbir şekilde yasa dışı kullanılamaz, kurum çıkarlarıyla çelişemez ve kurumun normal operasyon ve iş aktivitelerini engelleyemez.
2. Kurum kaynakları uygunsuz içeriği saklamak, bağlantı olarak vermek, yer imi olarak eklemek, erişmek ve göndermek için kullanılamaz
3. Resmi kurum işlerinin yürütülmesi dışında sohbet guruplarına, forumlara, elektronik haber gruplarına katılmak yasaktır.
4. Kullanıcıların sistemi kullanmak için gerekli kimlik bilgilerini başkalarına vermeleri yasaktır.
5. Yazılı olarak izin verilmedikçe port taraması veya güvenlik taraması yapılamaz.
6. Yazılı olarak izin verilmedikçe ağın izlenmesi ve kullanıcının kendisi için olmayan veriyi almaya çalışması yasaktır.
7. Kurumun kritik bilgisinin ortaya çıkmasını veya kurum servislerinin ulaşılamaz hale gelmesini sağlayacak tüm aktiviteler yasaktır.

7.4.2.3 Tarayıcı (Browser) Yazılımı

1. Kullanıcılar sadece kurumun yetkili birimlerince onaylanmış tarayıcı yazılımlarını ve konfigürasyonlarını kullanabilirler.
2. Tarayıcı yazılımının mevcut güvenlik ayarlarını gevşetecek ayarlamalar yapılamaz.

7.4.2.4 İndirilen Yazılımlar

1. Kurumun internet kaynakları onaylanmamış, ücretsiz veya ticari hiçbir yazılımın dağıtılması, indirilmesi veya yüklenmesi için kullanılamaz.
2. İndirilen tüm yazılımlar kullanılmadan önce zararlı kodlara ve virüslere karşı taramadan geçirilmelidir.

7.4.2.5 İzleme

1. Kurum, internet sistemleri kullanılarak yapılan tüm işlemleri izleme hakkını saklı tutar.

2. Kurum, kullanıcının internet sisteminde gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü partilerle, emniyet kuvvetleriyle veya yargıyla kullanıcının izni olmadan paylaşma hakkını saklı tutar.

7.4.3 Kabul Edilebilir E-posta Kullanım Kuralları

7.4.3.1 Kurumsal Kullanım

1. Kurum e-posta kaynakları öncelikli olarak resmi ve onaylı kurum işlerinin gerçekleştirilmesi için kullanılmalıdır.
2. Kurum çıkarlarıyla çatışmadığı sürece e-posta kaynaklarının kişisel kullanımına kısıtlı olarak izin verilmektedir.
3. Kurum e-posta kaynakları kullanılırken ilgili yasa ve düzenlemelere uyulmalıdır.
4. Kullanıcılar kendi kullanıcı hesaplarıyla gerçekleştirilen tüm e-posta işlemlerinden sorumludur.
5. Kurum dışına gönderilen tüm e-postalarda aşağıdaki uyarı mesajı bulunmalıdır:

“Bu e-posta mesajı kişiye özel olup, gizli bilgiler içeriyor olabilir. Eğer bu e-posta mesajı size yanlışlıkla ulaşmışsa, içeriğini hiçbir şekilde kullanmayınız ve ekli dosyaları açmayınız. Bu durumda lütfen e-posta mesajını gönderen kullanıcıya haber veriniz ve tüm elektronik ve yazılı kopyalarını siliniz. <KURUM> bu e-posta mesajının içeriği ile ilgili olarak hiçbir hukuksal sorumluluğu kabul etmez.”

7.4.3.2 Uygunsuz Kullanım

1. Kurum e-posta kaynakları hiçbir şekilde yasa dışı kullanılamaz, kurum çıkarlarıyla çelişemez ve kurumun normal operasyon ve iş aktivitelerini engelleyemez.
2. Kurum e-posta kaynakları uygunsuz içeriği saklamak, bağlantı olarak vermek, yer imi olarak eklemek, erişmek ve göndermek için kullanılamaz
3. Kullanıcıların e-posta sistemini kullanmak için gerekli kimlik bilgilerini başkalarına vermeleri yasaktır.
4. Kurum e-posta kaynakları; “zincir e-postalar”, reklam, aldatma, karalama gibi istenmeyen mesajlar (SPAM) göndermek için kullanılamaz.

5. E-posta sisteminin izinsiz kullanımı ve mesaj içeriğinde veya başlığında sahtecilik yapılması yasaktır.

7.4.3.3 E-posta Yazılımı

1. Kullanıcılar sadece kurumun yetkili birimlerince onaylanmış e-posta yazılımlarını ve konfigürasyonlarını kullanabilirler.
2. E-posta yazılımının mevcut güvenlik ayarlarını gevşetecek ayarlamalar yapılamaz.
3. Kullanıcılar e-posta yazılımının gönderenin kimliğini gizleyecek özelliklerini kullanamazlar
4. Kullanıcılar e-posta yazılımının otomatik mesaj iletme özelliklerini kullanamazlar.

7.4.3.4 İndirilen Yazılımlar

1. Kurumun e-posta sistemi ücretsiz veya ticari hiçbir yazılımın alınması, gönderilmesi veya saklanması için kullanılamaz.
2. Tüm e-posta içerikleri ve eklentileri açılmadan önce zararlı kodlara ve virüslere karşı taramadan geçirilmelidir.

7.4.3.5 İzleme

1. Kurum, e-posta sistemleri kullanılarak yapılan tüm işlemleri izleme hakkını saklı tutar.
2. Kurum, kullanıcının e-posta sisteminde gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü partilerle, emniyet kuvvetleriyle veya yargıyla kullanıcının izni olmadan paylaşma hakkını saklı tutar.

7.4.3.6 E-posta Saklama Kapasite Sınırları

1. Güvenlik ve performans açısından e-posta eklenti boyutu en fazla 10MB olmalıdır.
2. Kullanıcının e-posta kutusunun üzerinde aşağıdaki limitler uygulanır.
 - a. E-posta kutusu boyutu 150MB'ı geçtiğinde kullanıcı uyarılır.
 - b. E-posta kutusu boyutu 200MB'ı geçtiğinde kullanıcı e-posta gönderemez.
 - c. E-posta kutusu boyutu 250MB'ı geçtiğinde kullanıcı e-posta gönderemez ve alamaz

3. Kullanıcılar gereksiz mesajları silmekle yükümlüdür.
4. Kurumla ilgili kritik verileri içeren e-posta mesajlarının uygun şekilde yedeklenebilmesi için kurum sunucuları üzerinde saklanması gerekir.

7.4.4 Kabul Edilebilir Telekomünikasyon Cihazları Kullanım Kuralları

7.4.4.1 Kurumsal Kullanım

1. Kurum telekomünikasyon cihazları öncelikli olarak resmi ve onaylı kurum işlerinin gerçekleştirilmesi için kullanılmalıdır.
2. Kurum çıkarlarıyla çakışmadığı sürece telekomünikasyon cihazlarının kişisel kullanımına kısıtlı olarak izin verilmektedir.
3. Kurum telekomünikasyon cihazları kullanılırken ilgili yasa ve düzenlemelere uyulmalıdır.
4. Kullanıcılar telekomünikasyon cihazları ile yaptıkları tüm iletişimden sorumludur.

7.4.4.2 Uygunsuz Kullanım

1. Kurum telekomünikasyon cihazları hiçbir şekilde yasa dışı kullanılamaz, kurum çıkarlarıyla çelişemez ve kurumun normal operasyon ve iş aktivitelerini engelleyemez.
2. Kurum telekomünikasyon cihazları uygunsuz içeriği saklamak, erişmek, indirmek ve iletmek için kullanılamaz.
3. Kullanıcıların telekomünikasyon cihazlarını kullanmak için gerekli kimlik bilgilerini başkalarına vermeleri yasaktır.

7.4.4.3 Kurum Telefon Sistemi

1. Kullanıcılar, kurum telefon sistemini izin verilmeyen veya takip edilemeyen sistemlere erişimi engelleyecek şekilde ayarlamalıdır.
2. Telefon konuşmaları sırasında hoparlörler, ses ve video kayıt cihazları, video konferans ve benzeri cihazlar kullanılmadan önce görüşmede yer alan herkese bildirilmeli ve herkesten izin alınmalıdır.
3. Şehirler ve milletler arası konuşmalar onaylı kullanıcılar tarafından yapılmalıdır.

4. Kuruma ait hassas bilginin yetkisiz kişilerin eline geçebileceği ortamlarda kullanıcılar bu bilgileri tartışmamalıdır. Ayrıca bu tip görüşmeler yapılırken kablosuz cihazlar veya cep telefonları kullanılmamalıdır.

7.4.4.4 Fakslar

1. Kurum adına gönderilen tüm faksların ilk sayfasında aşağıdaki ifade yer almalıdır:
“Bu faks <KURUM>’a ait özel, gizli veya telifli bilgi içeriyor olabilir. Bu faks sadece belirtilen alıcı içindir. Eğer bu faksın alıcısı siz değilseniz bu faksın içeriğini okumak, değiştirmek veya kopyalamak yasa dışı olabilir. Eğer bu faks size yanlışlıkla ulaşmışsa, içeriğini hiçbir şekilde kullanmayınız. Bu durumda lütfen faks gönderen kişiye haber veriniz ve tüm elektronik ve yazılı kopyalarını siliniz.”

7.4.4.5 Modemler

1. Modem kullanımı Uzaktan Erişim Politikası’nda belirtilen şekilde gerçekleştirilmelidir.

7.4.4.6 İzleme

1. Kurum, telekomünikasyon cihazları kullanılarak yapılan tüm işlemleri izleme hakkını saklı tutar.
2. Kurum, kullanıcının telekomünikasyon cihazlarıyla gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü partilerle, emniyet kuvvetleriyle veya yargıyla kullanıcının izni olmadan paylaşma hakkını saklı tutar.

7.4.5 Kabul Edilebilir Yazılım Kullanım Kuralları

7.4.5.1 Kurumsal Kullanım

1. Kullanıcılar yazılımlarla ilgili tüm telif hakkı yasalarına uymak zorundadırlar.
2. Kurum tarafından kullanılan tüm lisanslar yasal yollardan temin edilmiş olmalıdır.
3. Kuruma ait yazılımlar kullanılırken ilgili yasa ve düzenlemelere uyulmalıdır.

7.4.5.2 Uygunsuz Kullanım

1. Kuruma ait yazılımlar yasa dışı, kurum politikalarına aykırı veya kurum çıkarlarına ters düşecek şekilde kullanılamaz.

2. Kuruma ait yazılımların izinsiz çoğaltılması yasaktır.
3. Kurum haberleşme alt yapısı ücretsiz, deneme sürümü veya ticari hiçbir yazılımın izinsiz kopyalanması, gönderilmesi alınması veya çoğaltılması için kullanılamaz.

7.4.5.3 İzleme

1. Kurum, kullanıcıların bilgisayarlarında yüklü bulunan veya kullanılan yazılımları herhangi bir zamanda kontrol edebilir.
2. Kurum, kullanıcının yazılımlarla gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü partilerle, emniyet kuvvetleriyle veya yargıyla kullanıcının izni olmadan paylaşma hakkını saklı tutar.
3. Kurum yetkili personelince tespit edilen ve lisans anlaşmalarına uymayan yazılımlar kurum tarafından kullanıcıya haber vermeden kaldırılabilir.

7.4.6 Kabul Edilebilir Taşınabilir Bilgi İşleme Cihazları Kullanım Kuralları

7.4.6.1 Kurumsal Kullanım

1. Kurum bilgi kaynaklarına erişmek için sadece onaylanmış taşınabilir bilgi işleme cihazları kullanılmalıdır.
2. Kuruma ait taşınabilir bilgi işleme cihazları, öncelikli olarak resmi ve onaylı kurum işlerinin gerçekleştirilmesi için kullanılmalıdır.
3. Taşınabilir bilgi işleme cihazları gözetimsiz bırakıldıklarında mutlaka fiziksel olarak güvenli bir yerde veya şekilde saklanmalıdır.
4. Kurum çıkarlarıyla çakışmadığı sürece bu cihazların kişisel kullanımına kısıtlı olarak izin verilmektedir.
5. Bu cihazlar kullanılırken ilgili yasa ve düzenlemelere uyulmalıdır.

7.4.6.2 Uygunsuz Kullanım

1. Kuruma ait taşınabilir bilgi işleme cihazları hiçbir şekilde yasa dışı, kurum çıkarlarıyla çelişecek veya normal operasyon ve iş aktivitelerini engelleyecek şekilde kullanılamaz.
2. Kurum gizli bilgisi taşınabilir bilgi işleme cihazlarında şifresiz olarak saklanamaz. Kurum tarafından onaylanmış şifreleme yöntemleriyle korunmalıdır.

3. Kurum tarafından onaylanmış şifreleme yöntemleri ve iletim metotları kullanılmadan kurum bilgisi, taşınabilir bilgi işleme cihazlarından veya bu cihazlara kablosuz olarak aktarılamaz. Ayrıca bilgi, zararlı yazılımlara karşı taramadan geçirilmeden kurum ağına aktarılamaz.

7.4.6.3 İzleme

1. Kurum, taşınabilir bilgi işleme cihazları kullanılarak yapılan tüm işlemleri izleme hakkını saklı tutar.
2. Kurum, kullanıcının taşınabilir bilgi işleme cihazları ile gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü partilerle, emniyet kuvvetleriyle veya yargıyla kullanıcının izni olmadan paylaşma hakkını saklı tutar.

7.5 Uygulama ve Ceza

Kabul Edilebilir Kullanım Politikasına ve burada belirtilen diğer politika ve prosedürlere uymayanlar hakkında disiplin süreci başlatılır ve yasal işlem uygulanır.

7.6 Gözden Geçirme ve Onay

Kabul Edilebilir Kullanım Politikası altı (6) ayda bir tarafından gözden geçirilir ve varsa değişiklikler tarafından onaylanır.

KAYNAKÇA

- [1]. www.itgovernance.co.uk/files/Infosec_101v1.1.pdf
(Information Security and ISO27001 – An Introduction)
- [2]. www.niser.org.my/isms/docs/publications/information_security_management_committee.pdf
(The Importance of Setting up an Information Security Management Committee in Organization)
- [3]. <http://www.isms.jipdec.jp/en/isms/frame.html>
(How to Establish an ISMS Management Framework)
- [4]. http://www.lazarusalliance.com/horsewiki/index.php/International_Organization_for_Standardization_Security_Standard:
(International Organization for Standardization Security Standard Policy Samples)