BGYS POLİTİKASI

BGYS politikası, **Ankara Nallıhan Devlet Hastanesi Bağlı Birimler** bünyesinde yürütülen bilgi güvenliği yönetim sistemi çalışmalarının kapsamını, içeriğini, yöntemini, mensuplarını, görev ve sorumlulukları, uyulması gereken kuralları içeren bir dokümandır. Bu politikada tüm bölümleri ilgilendiren maddeler olduğu gibi sadece bazı bölümleri ilgilendiren maddeler de bulunmaktadır.

1. Amaç

Ankara Nallıhan Devlet Hastanesi'nin bilgi güvenliğini yönetmekteki amacı; tüm bilgi varlıklarımızın gizliliği, bütünlüğü ve gerektiğinde yetkili kişilerce erişilebilirliğini sağlamak ve kurumun dışardan veya içeriden gelebilecek, kasıtlı veya kasıtsız oluşabilecek tüm tehditlerden korunması, kurumdaki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve bilginin geniş çaplı tehditlerden korunmasını sağlamaktır. Bilgi; diğer kıymetli varlıklarımızın içinde en çok ihmal edilen fakat Kurum açısından en önemli varlıklardan biridir. Bilgi Güvenliği; Ankara Nallıhan Devlet Hastanesi ve bağlı birimlerinin sahip olduğu bilgi varlıklarının korunması ve uygun biçimde yönetilmesinin sağlanmasıdır.

2. Hedef

Bilgi Güvenliği Politika şartlarını yerine getirerek, çalışanların bilgi güvenliği farkındalığını arttırmak, teknik güvenlik kontrollerini uygulamak ve kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak (iş sürekliliği), kurumsal riskleri en alt seviyeye indirerek kurumun güvenliği ile güvenilirliğini ve temsil ettiği kurumun imajını korumaktır.

3. Kapsam

"Bilgi Güvenliği Yönetim Sistemleri Politikası" dokümanında yer alan kriterler, Ankara Nallıhan Devlet Hastanesi ve bağlı birimlerinde, çalışan tüm personel ile aşağıdaki varlık ve teknoloji kategorilerini kapsamaktadır.

a. Veri dosyaları, sözleşmeler ve benzeri tüm bilgi varlıkları,
b. Uygulama ve Sistem Yazılımları,
c. Güvenlik cihazları, sunucular (server),
d. Bilgisayarlar, iletişim donanımı ve veri depolama ortamları,
e. Tüm işlevlerin yerine getirilmesi için gerekli fiziksel varlıklar (aydınlatma, iklimlendirme, kablolama vs.),
f. Kurum tarafından üretilen, kullanılan ve geliştirilen tüm verileri kapsar.

4. Tanımlar Ve Kısaltmalar

Bağlı Birimler: Ankara Nallıhan Devlet Hastanesi bünyesinde bulunan tüm birimleri kapsar.
Varlık : Ankara Nallıhan Devlet Hastanesi iş süreçleri için değeri olan, kaybı halinde işlerin aksayacağı, insan, yazılım, donanım, itibar, bilgi gibi unsurların tümüdür.
Gizlilik: Bilginin sadece yetkili kişiler tarafından erişilebilir olmasıdır.
Bütünlük: Bilginin yetkisiz değiştirmelerden korunması ve değiştirildiğinde farkına varılmasıdır.
Erişilebilirlik: Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an erişilebilir olmasıdır
Bilgi güvenliği ihlal olayı: İş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olayı.
Bilgi 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. Yönetim sistemi, kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, prosedürleri, prosesleri ve kaynakları içerir.

5. Bilgi Güvenliği Hedefleri ve Prensipleri

Bilgi güvenliği yönetimi kapsamına alınan tüm süreçlerde ve varlıklarda gizlilik, bütünlük ve erişilebilirlik prensiplerine uyacak önlemler almak amacıyla aşağıda detayları belirtilen risk yönetimi faaliyetleri yürütülmektedir. Her bir varlık için risk seviyesinin kabul edilebilir risk seviyesinin altında tutmak hedeflenmektedir.
Risk yönetimi ve kontrollerin uygulanması sürekli bir faaliyettir ve kabul edilebilir risk seviyesinin altına inen riskler için de iyileştirme yapılması hedeflenmektedir.

6. Bilgi Güvenliği Yapısı ve Organizasyonu

Ankara Nallıhan Devlet Hastanesi bünyesinde bu politika metninde madde 1 ve 2 de tarif edilen kapsam dahilinde TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı gerekliliklerini yürütmek üzere BGYS KOMİSYONU kurulmuştur. **Bu komisyon en az altı (6) ayda bir toplanacaktır.**

a. ***BGYS Komisyonu***

- ✓ Hastane Başhekimi Uzm.Dr.Hakan ÇİME
- ✓ İdari ve Mali İşler Müdürü Ahmet BOZKURT
- ✓ İdari ve Mali İşler Müdür Yardımcısı N.Celil YANAR
- ✓ Bilgi Güvenliği Yetkilisi Yılmaz İLHAN

b. BGYS Komisyonu Görev, Yetki ve Sorumluluklar:

- Bilgi güvenliği politika ve stratejilerini belirler, gerektiğinde Bilgi Güvenliği Politikaları Yönergesine bağlı olarak hazırlanacak olan kılavuzlarla ilgili revizyon kararlarını verir,
- Bilgi güvenliği politikalarının uygulamasının etkinliğini gözden geçirir,
- Bilgi güvenliği faaliyetlerinin yürütülmesini yönlendirir,
- Bilgi güvenliği eğitimi ve farkındalığını sağlamak için plan ve programları hazırlar,
- Bilgi güvenliği faaliyetleri ve kontrollerinin tüm kurum ve kuruluşlarda koordine edilmesini sağlar.
- Yürütülen çalışmaların tabana yayılması hususunda planlanan çalışmalara katılır, bağlı oldukları birimlerde bu çalışmaların yayılmasına öncülük eder,

7. Bilgi Hassasiyeti ve Riskler

a. Bilgi Varlıklarımız

Ankara Nallıhan Devlet Hastanesi bünyesinde Madde 3 te belirtilen kapsam dâhilinde yer alan tüm fiziki alanlarda bulunan birimlerin yapmış oldukları işlerde üretilen bilgiler bilgi varlıklarımızı oluşturmaktadır.

Masaüstü bilgisayarlar, laptoplar, tabletler, telefonlar, CD, DVD ve USB Bellek ortamındaki veriler, evraklar, klasör ve evrak dolapları, sunucular gibi elektronik veya yazılı-baskılı ortamda bulunan veya iletim ortamında (internet, email, telefon vb.) yer alan tüm veriler kurumumuz için bilgi varlığı olarak tanımlanmıştır.

b. Varlık Sınıflandırılması

BİLGİ SINIFLANDIRMA KILAVUZU		Saklanma Yeri Dolap
Gizli	En kritik bilgilerdir, sadece yönetim kadrosunun erişimi vardır. Bu tür bilgilerin yetkisiz erişilmemesi, ifşa edilmemesi veya paylaşılmaması kurum açısından çok önemlidir. Gizlilik ön plandadır	Hazırlayan kişi tarafından kontrol edilen ve kapalı odalarda bulunan kilitli dolaplar ve kişisel bilgisayarlar
İç Kullanım	Sadece birimlere özel bilgilerdir. Departman çalışanları dışında hiçbir 3. taraf kurumun veya kişinin görmemesi gereken bilgilerdir. Gizlilik ön plandadır	Departmanın kilitli dolapları, kişisel bilgisayarlar
Kişisel	Birim çalışanlarının kişisel çalışmaları ile ilgili bilgilerdir. Kurum işlevleri için yapılan kişisel çalışmalar burada tutulabilir. PC, Laptop veya Dolaplarda işle ilgili olmayan diğer kişisel bilgiler tutulamaz. Erişilebilirlik ön plandadır	Çalışma masalarının kilitli çekmeceleri

Kuruma Açık	Bu bilgiler kurum çalışanlarının kullanımı içindir. Erişilebilirlik ve bütünlük ön plandadır. Departmanların kendi aralarında paylaştıkları bilgiler bu sınıfa girer.	Departmanın kilitli ortak dolapları
Halka Açık	Bu bilgiler T.C. Sağlık Bakanlığına bağlı tüm teşkilatına, tedarikçilere ve halka açık bilgilerdir. Bu bilgilerin erişilebilirliği önemlidir.	Dolaplar ve dolap dışlarında

Kurum içinde her çalışan bu sınıflandırma çerçevesinde kendi kullanımında olan veya kendi ürettiği bilgileri sınıflandırmalıdır. Bu sınıflandırmaya göre halka açık dokümanlar web sitesinde yayınlanan ve işlem için üçüncü taraflara verilen kağıt veya elektronik ortamdaki başvuru formu, duyurular vb. bilgilerdir.

8. Genel Kullanım Politikası

a. Her kullanıcı bilgisayarına, tabletine oturum şifresi koymak zorundadır.
b. Tüm kullanıcılar **kurumsal işlemlerde** resmi olarak tahsis edilen @saglik.gov.tr uzantılı e-posta adresini kullanmak zorundadırlar.
c. Bilgisayar başından uzun süreli uzak kalınması durumunda bilgisayar kilitlenmeli ve 3.şahısların bilgilere erişimi engellenmelidir.
d. Bütün kullanıcılar kendi bilgisayarlarının güvenliğinden sorumludur. Açık bırakılması halinde ve ya kullanıcı oturum şifrelerinin ikinci şahıslarca biliniyor olması durumlarında bu bilgisayarlardan kaynaklanabilecek, kuruma veya kişiye yönelik saldırılardan (Örneğin; elektronik bankacılık, hakaret-siyaset içerikli mail, kullanıcı bilgileri vs.) bilgisayarın sahibi sorumludur.
e. Kurumun bilgisayarları kullanılarak taciz veya yasadışı olaylara karışılmamalıdır.
f. Ağ güvenliğini (Örneğin; bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ trafiğini bozacak (packetsniffing, packetspoofing, denial of service vb.) eylemlere girişilmemelidir.
g. Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DOS saldırısı, port- network taraması vb. yapılmamalıdır.
h. Cihazlar, yazılımlar ve veriler izinsiz olarak kurum dışına çıkarılmamalıdır.
i. Kurumsal veya kişisel verilerin gizliliğine ve mahremiyetine özel önem gösterilmelidir. Bu veriler, Kurumumuzun bu konudaki ilgili mevzuat hükümleri saklı kalmak kaydıyla elektronik veya kâğıt ortamında üçüncü kişi ve kurumlara verilemez.
j. Kurumun kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programlar (Dergi CD'leri veya internetten indirilen programlar vs.) kurulmamalı ve kullanılmamalıdır. Lisansız yazılımı bilgisayarında barından personel ilgili mevzuat çerçevesinde kendisi sorumludur.
k. Personel, kendilerine tahsis edilen ve kurum çalışmalarında kullanılan masaüstü, dizüstü bilgisayarlarındaki ve tabletlerindeki kurumsal bilgilerin güvenliği ile sorumludur.
l. Bilgi İşlem Birimi tarafından yetkili kişiler kullanıcıya haber vermek kaydı ile yerinde veya uzaktan, çalışanın bilgisayarına erişip güvenlik, bakım ve onarım işlemleri yapabilir. Bu durumda uzaktan bakım ve destek hizmeti veren yetkili personel bağlanılan bilgisayardaki kişisel veya kurumsal bilgileri görüntüleyemez, kopyalayamaz ve değiştiremez.
m. Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/ kopyalanmamalıdır.
n. Bilgisayarlar üzerinde resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.
o. Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli, ivedilikle Bilgi İşlem Birimine haber verilmelidir
p. Kullanıcılar, bilgisayarlarında ya da sorumlusu oldukları sistemler üzerinde USB flash bellek ve/veya harici hard disk gibi removable media (taşınabilir medya) bırakmamalıdır.
q. Son kullanıcılar, mesai bitiminde bilgisayarlarını kapatmalıdır.
r. Kullanıcı bilgisayarlarında, güncel anti virüs bulunmalıdır. Hiç bir kullanıcı herhangi bir sebepten dolayı anti virüs programını sistemden kaldıramaz ve başka bir anti virüs yazılımını sisteme kuramaz.
s. Zararlı programları (virüs, solucan, truva atı , e-mail bombaları v.b)kurum bünyesinde oluşturmak ve dağıtmak yasaktır
t. Dizüstü bilgisayarın, tabletlerin veya telefonların çalınması/kaybolması durumunda en kısa sürede Sağlık Müdürlüğü İstatistik ve Bilgi İşlem Birimine haber verilmelidir.

9. İnsan Kaynakları Zafiyeti Yönetimi

a. Çalışan personele ait şahsi dosyalar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde olmamalıdır.
b. Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmelidir.
c. ÇKYS üzerinden kişiyle ilgili bir işlem yapıldığında (izin kağıdı gibi) ekranda bulunan kişisel bilgilerin diğer kişi veya kişilerce görülmesi engellenmelidir.
d. Diğer kişi, birim veya kuruluşlardan telefonla ya da sözlü olarak çalışanlarla ilgili bilgi istenilmesi halinde hiçbir suretle bilgi verilmemelidir.
e. İmha edilmesi gereken (müsvedde halini almış ya da iptal edilmiş yazılar vb.) kağıt kesme makinasında imha edilmelidir.

f. Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.
g. Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.
h. Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.
i. Görevden ayrılan personelin kimlik kartı alınmalı ve yazıyla kartları üreten ilgili şubeye iade etmelidir.

10. Sosyal Mühendislik Zafiyetleri

İnsanların zafiyetlerinden faydalanarak çeşitli etkileme, ikna ve kandırma yöntemleriyle istenilen (normalde paylaşmamaları gereken) bilgileri elde etmeye çalışmaktır.

a. Kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket edilmelidir.
b. Arkadaşlarımızla paylaştığımız bilgileri seçerken dikkat edilmelidir.
c. Telefon, e-posta veya sohbet yoluyla yapılan haberleşmelerde Kullanıcı adı ve özellikle şifre bilgileri paylaşılmamalıdır. Şifre kişiye özel bilgidir. Sistem yöneticileri dâhil telefonda veya e-posta yazışmalarında şifremizi paylaşmamalıyız. Sistem yöneticisi gerekli işlemi şifrenize ihtiyaç duymadan da yapabilmelidir.
d. eMule, torrent gibi dosya paylaşım yazılımları kullanılmamalıdır.
e. Sadece yetkili kişilerin kurum içerisindeki sınırlı bölümlere erişim izni olduğundan emin olmak için uygun erişim kontrol mekanizmaları olması gerekir.
f. Kurum Web Sayfasında kurum ile ilgili paylaşılan bilgilere son derece dikkat edilmeli ve bu sürekli izlenmelidir.
g. Elektronik posta ile yapılan yazışmalarda saglik.gov.tr uzantılı e-posta hesapları kullanılmalıdır.
h. E-Postalara gelen kaynağı belli olmayan, şüphe uyandıran e-postalar açılmamalı ve ilgili sorumlulara bilgi verilmelidir.
i. Sosyal medya hesaplarına giriş için kullanılan şifreler ile kurum içinde kullanılan şifreler farklı olmalıdır.
j. Kurum içi bilgiler, sosyal medyada paylaşılmamalıdır.
k. Kuruma ait hiçbir gizli bilgi ve yazı sosyal medyada paylaşılmamalıdır.

11. Bilgi Kaynakları Atık Ve İmha Yönetimi

a. Evraklar idari ve hukuki hükümlere göre belirlenmiş Evrak Saklama Planı'na uygun olarak muhafaza edilmesi gerekmektedir.
b. Yasal bekleme süreleri sonunda tasfiyeleri sağlanmalıdır. Burada Özel ve Çok Gizli evraklar "Devlet Arşiv Hizmetleri Yönetmeliği" hükümleri gereği oluşturulan "Evrak İmha Komisyonu" ile karar altına alınmalı ve imha edilecek evraklar kırpma veya yakılarak imhaları yapılmalıdır. İmha edilemeyecek evrak tanımına giren belgeler geri dönüşüme devirleri yapılmalıdır.
c. İmha işlemi gerçekleşecek materyalin özellik ve cinsine göre imha edilecek lokasyon belirlenmelidir.
d. Uygun şekilde kırılması ve kırılma sürecinden önce veri ünitelerinin adet bilgisi alınmalıdır.
e. Kırılan parçaların fiziksel muayene ile tamamen tahrip edilip edilmediğinin kontrolü yapılmalıdır.
f. Tamamen tahrip edilememiş disk parçalarının delme, kesme makinaları ile kullanılamaz hale getirilmelidir.
g. Hacimsel küçültme işlemi için parçalanmalıdır.
h. Çıkan metallerin sınıflarına göre ayrılarak, biriktirildikten sonra eritme tesislerine iletilmesi gerekmelidir.

12. Şifre Kullanım Politikası

a. Bütün kullanıcı seviyeli şifreler (örnek, e-posta, web, masaüstü bilgisayar vs.) en az altı ayda bir değiştirilmelidir. Tavsiye edilen değiştirme süresi her üç ayda birdir.
b. Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
c. Şifreler başkası ile paylaşılmamalı, kâğıtlara ya da elektronik ortamlara yazılmamalıdır.
d. En az sekiz karakterden oluşmalıdır.
e. Harflerin yanı sıra, rakam ve "?, @, !, #, %, +, *, %" gibi özel karakterler içermelidir.
f. Büyük ve küçük harfler bir arada kullanılmalıdır.
g. Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır. (Örneğin 12345678, qwerty, doğum tarihiniz, çocuğunuzun adı, soyadınız vb.)
h. Basit bir kelimenin içerisindeki harf veya rakamları benzerleri ile değiştirilerek güçlü bir parola elde edilebilir.(w3rhaba,1iki3 vb.)
i. Herhangi bir kişiye telefonda şifre verilmemelidir.

j. Şifreler, işten uzakta olunduğu zamanlarda iş arkadaşlarına verilmemelidir.

13. İşe Başlayış ve İşten Ayrılma Prosedürü

a. İşe Başlayış Prosedürü

1.a.1. İşe başlayan her personele (kadrolu ve hizmet alımı dâhil) bilgi güvenliği ve sosyal mühendislik zafiyetleri konularıyla ilgili eğitim verilmelidir.
1.a.2. Kullanıcılar kurumumuzca tanımlanmış ve yayınlanmış gizlilik sözleşmelerini imzalayarak kurum politikalarına uyacaklarını taahhüt ederler. Her çalışan personel "Bilgi Güvenliği Kullanıcı Sözleşmesi"ni (PC kullansın kullanmasın, kadrolu veya sözleşmeli tüm personel) imzalamakla yükümlüdür.
1.a.3. Var ise kullanacağı bilgi sistemlerine yönelik kullanıcı adı ve şifreleri tanımlanmalıdır.
1.a.4. EBYS üzerinden yazışma yapabilmesi ve ya yazışmaları takip edebilmesi için ilgili personele saglik.gov.tr uzantılı e-mail adresi tanımlanmalıdır. İl içi yer değişikliklerinde ise sistem üzerinden kurum/birim değişikliği tanımlaması yapılmalıdır.
1.a.5. Tüm personele kurum kimlik kartı çıkartılmalıdır.

b. İşten Ayrılma Prosedürü

1.b.1. Görevden ayrılan personelin kurum kimlik kartı ve yaka kartı alınmalıdır.
1.b.2. Kullandığı bilgi sistemlerine yönelik (ÇKYS/TSIM, EBYS vb.) kullanıcı adı ve şifreleri ilgili sistem yöneticileri tarafından iptal edilmeli ya da pasif hale getirilmelidir.
1.b.3. Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.
1.b.4. Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.
1.b.5. Görevden ayrılan personel "İŞTEN AYRILMA ONAY FORMU" nu doldurarak bağlı bulunduğu kurumun insan kaynakları birimine teslim etmelidir.
1.b.6. İlgili form doldurulmadan personelin kurum ile ilişiği kesilmez

14. Mal ve Hizmet Alımı Güvenliği

a. Kurum olarak mal ve hizmet alımlarında ilgili kanun, genelge, tebliğ ve yönetmeliklere aykırı olmayacak rekabeti engellemeyecek şekilde gerekli güvenlik düzenlemeleri Teknik şartnamelerde belirtilmelidir.
b. Dış kaynak kullanımı ve üçüncü taraf hizmet sunumunun diğer formları arasındaki farklılıkların bazıları; Sorumluluk, geçiş durumu planlama ve işlemler süresince potansiyel kesinti süresi, acil durum planlaması yönetmelikleri ve durum tespitinin gözden geçirilmesi, güvenlik olayları hakkında bilgi toplanması ve yönetimi konularında sorular içerecektir. Bu nedenle, dış kaynaklı bir yönetmelik geçişinde; kuruluş değişiklikleri yönetmek için uygun süreçlere ve anlaşmaların yeniden müzakere edilmesi ya da fesih edilmesi hakkına sahip olduğu için kuruluşun planlaması ve yönetimi önemlidir.
c. Üçüncü taraflarla yapılan anlaşmalar diğer tarafları içerebilir. Üçüncü taraflara erişim hakkı verilmeden önce, erişim hakkı ve katılım için diğer tarafların ve koşulların belirlenmesi amacıyla anlaşmaya varılması gerekir.

15. Bilgi Güvenliği Dökümanı ve İhlal Bildirimi

Kurum bünyesinde tüm çalışanların genel olarak uyması gereken kurallar doküman olarak hazırlanıp tüm personele dağıtılmıştır. Personel bu dokümanda önerilen uygulamaları takip etmeli, zayıflık ve tehditlere karşı farkında olmalıdırlar. Personel bu dokümanda tanımlanan bilgi güvenliği ihlallerini yapmamalı ve bu ihlalleri gözlemlediğinde mutlaka BGYS Komisyonuna veya http://ankaraism.saglik.gov.tr web adresindeki formu doldurarak bildirmelidirler.

16. Bilgi Güvenliği Sözleşmeleri

Kullanıcılar kurumumuzca tanımlanmış ve yayınlanmış gizlilik sözleşmelerini imzalayarak kurum politikalarına uyacaklarını taahhüt ederler. Taahhütname ve kurallar farklı dokümanlardır. Personel Bilgi Güvenliği Kullanıcı Sözleşmesi (Taahhütnamesi) işe alınan her çalışanın (PC kullansın kullanmasın, kadrolu veya sözleşmeli tüm personel) imzaladığı bir belgedir.

17. Bilgi Güvenliği Eğitimleri

Kurumumuzda gerekli görüldüğü hallerde eğitim verilecektir.

18. Desteklenen Politikalar

E-Posta Kullanım Politikası

Bilgi Güvenliği Disiplin Prosedürü

Temiz Masa Temiz Ekran Politikası

Bilgi Güvenliği İhlal Olayları Bildirim Prosedürü

Bilgi Güvenliği Kullanıcı Sözleşmesi

19. Formlar

İşten Ayrılma Formu

İhlal Olayları Bildirim Formu