AMAÇ

Bilgi Güvenliği Yönetim Sistemi Politikalarının amacı Kurum personelinin, sistemlerinin, bilgi ve varlıklarının; gizlilik, bütünlük ve erişilebilirlik bakımından yapılması, uyulması gereken iş kurallarını hedeflemek ve bu hedefler kapsamında iş sürekliliğini sağlamaktır.

Kurumun amacı herhangi kimse üzerinde kısıtlayıcı politikalar üretmek değil aksine açıklık, güven ve bütünlüğe yönelik kültürü yerleştirmektir. Kurum bilerek veya bilmeyerek yapılan yasadışı veya zararlı eylemlerine karşı personelin ve kurumun haklarını korumaya adamıştır. Bilişim ile alakalı sistemler kurumun sahip olduğu değerlerdir. Güçlü bir güvenlik, bütün personellerin dâhil olduğu takım çalışmasıyla oluşturulabilir.

1. KAPSAM

Bu politika **ETIQA** bilgi varlıklarının gizliliği, bütünlüğü ve erişilebilirliğini etkileyen tüm unsurları ve çalışma ortamlarını kapsamaktadır.

2. SORUMLULUK

BGYS politikalarının, gözden geçirilmesi ve güncellenmesinden BGYS Yönetim Temsilcisi ve BGYS Ekibi sorumludur. **ETIQA** yönetimi Bilgi Güvenliği Politikasını onaylar ve duyurulmasını sağlar. Bu politikalara uyulmasından iç ve dış tüm personeller sorumludur.

3. TANIMLAR

BGYS: Bilgi Güvenliği Yönetim Sistemi

4. POLİTİKA

ETIQA da uygulanmakta olan iç ve dış tüm personellerin uyması gereken temel kurallar aşağıda detaylandırılmıştır.

4.1. Kabul Edilebilir Kullanım Kuralları

a) ETIQA gizli olarak belirlediği tüm bilgilerin gizliliğine sıkı bir şekilde uyulacaktır. Kurumun iş gereksinimi dışında bu bilgilerin kopyalanması ve iletilmesi yasaktır.

b) Kurum personeli, kendilerine tahsis edilmiş tüm bilgisayar erişim bilgilerini ve kendisine verilmiş cihazların güvenliğini sağlamakla sorumludur. Erişim bilgileri herhangi birine söylenemez ve bu bilgiler başkaları ile paylaşılamaz.

c) Hiçbir personel, bilgisayarlarından antivirüs koruma yazılımını devre dışı bırakamaz.

d) Kaynağı belli olmayan ve üretici firması tarafından kopya edilmesi yasaklanmış bir bilgisayar yazılımını kopyalamak yasaktır.

e) Bilgisayarlara hiçbir surette lisanssız program yüklenmemelidir.

f) Kullanıcı herhangi bir bilginin çok kritik olduğunu düşünüyorsa o bilgi şifrelenmeli veya yetkili kişiler dışında erişilemeyecek alanlarda saklanmalıdır.

g) Bilgisayarlar üzerinden resmi belgeler, programlar ve eğitim belgeleri haricinde (müzik, film vb.) dosya alışverişinde bulunulmamalıdır.

h) Bilgisayarlarda oyun, eğlence vb. uygulamaların çalıştırılması ve kopyalanması yasaktır.

i) Kritik raporların dökümünü alan kullanıcı, rapor içeriğindeki bilginin uygun bir şekilde korunmasından sorumludur.

j) Herhangi bir kişi kendine ait olmayan kritik bir rapor bulur ise bu durumu Bilgi Güvenliği Yönetim Temsilcisine bildirmelidir.

k) *"Gizli"* kâğıt belgeleri kilitli dolaplarda muhafaza edilecektir.

l) Sunucu ve bilgisayarların saatleri kullanıcılar tarafından değiştirilemez, saatler sistem tarafından otomatik olarak yönetilmektedir.

m) Laptop bilgisayarlar güvenlik açıklarına karşı korunmalıdır. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmalıdır. Cihazların çalınması veya kaybolması durumunda hemen Bilgi İşlem ile iletişime geçilmelidir.

n) Herhangi bir kişi veya kurumun izinsiz kopyalama, ticari sır, patent veya diğer kurum bilgileri, yazılım lisansları vb. hakları kesinlikle ihlal edilmemelidir.

o) Kurum bilgileri kurum dışından üçüncü şahıslara iletilmemelidir.

p) Tüm personel, kendi alanlarına ait Güvenlik Politikalarına uymak zorundadır.

q) Kurum politika ve prosedürleri, İnsan Kaynakları ve ilgili yöneticiler tarafından Kurum personeline, yeni işe başlayanlara ve 3.taraflara duyurulacaktır. İlgili güvenlik politikalarına uyulacağı personel iş sözleşmesinde yer almalı ve personele imzalatılmalıdır.

r) ETIQA bilgisayarlarında kişisel verilerin barındırılması yasaktır. **Bu** ortamda tutulan ve iletilen tüm bilgiler **ETIQA** 'nin malıdır. **ETIQA** bu bilgileri izleme ve denetleme hakkına sahiptir.

s) Kaynağı belli olmayan ve üretici firması tarafından kopya edilmesi yasaklanmış bir bilgisayar yazılımını kopyalamak yasaktır.

t) Hiçbir personel izin almadan kendi bilgisayarı veya başka bir kaynak kullanarak, **ETIQA** 'nin bilişim ağını tarayamaz, izleyemez veya dinleyemez.

u) Hiçbir personel, kurum içinde kendilerine tahsis edilen bilgisayar yetkilerinin dışına çıkamaz ve bu konuda yetki aşma işlemine girişemez.

v) Sosyal medya erişimi verilen kullanıcılar görevlerinin dışında bu haklarını kullanmaları yasaktır.

w) Sosyal medya üzerinden kurumu rencide edici, karalayıcı paylaşımlar yapılmamalıdır. Kurumun hassas bilgileri sosyal medya üzerinden paylaşılmamalıdır.

x) Personeller zimmetlerini iade etmesi durumunda, zimmetlenen cihaz *(bilgisayar, cep telefonu, taşınabilir disk, usb bellek v.s)* üzerinde hiçbir kişisel veri bırakmamalıdır.

y) Tüm çalışanlar bilgi güvenliği ihlallerini önlemek maksadıyla güvenlik zayıflıklarını doğrudan kendi yönetimlerine ve Bilgi Güvenliği Ekibine mümkün olan en kısa sürede rapor verilmelidir.

z) ETIQA ağına uzaktan bağlantı gereken durumlarda, Bilgi İşlemin onayladığı bağlantı yöntemleri ile erişim sağlanmalıdır.

4.2. İnternet Kullanım Kuralları

a) Kurum bilgisayarları içerik denetimi yapan bir uygulama üzerinden internete çıkacaktır. Kurum kültürüne ve yasalara uygun olmayan siteler yasaklıdır. Ancak üst yönetimin yazılı izni ile yetkilendirilmiş kurum personeline internete çıkarken gerekli servisleri kullanma hakkı tanımlanmıştır. (FTP, sosyal medya)

b) 5651 sayılı kanun (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun) gereği kurum internet erişim kayıtları en az iki yıl arşivlenmektedir.

c) Bilgisayarlar üzerinden yasalara aykırı internet sitelerine girmek ve dosya (film, müzik, program vb.) indirilmemelidir.

d) Tunnel platformları *(VPN)*, proxy ve DNS değişiklikleri yapılarak internete bağlanılmamalıdır.

e) VPN bağlantılarında iki seviyeli güvenlik politikası kullanılmalıdır. VPN erişimi ile logo sunucusuna ofis dışından uzak bağlantı yolu ile erişilmelidir.

f) Başkalarının fikri haklarını ihlal edici materyal *(yazı, makale, kitap, film, müzik eserleri vb.)* dağıtılmamalıdır.

g) Sistem ve ağ güvenliğinin ihlal edilmesi cezai ve hukuki mesuliyetle sonuçlanabilir. **ETIQA**bu tür ihlallerin söz konusu olduğu durumları inceler ve eğer bir suç oluştuğundan şüphe duyulursa disiplin yönetmeliğini uygulayabilir veya yasa uygulayıcısı ile işbirliği yapabilir.

h) İnternet üzerinden kullanım amaçlarına uygunsuz, müstehcen, rahatsız edici materyaller ve başkalarına iftira, karalama mahiyetinde mesajlar yayınlanmamalı ve paylaşılmamalıdır.

i) Kullanıcıların internet üzerinden görevleri ile ilgisi bulunmayan, internet trafiğini kısıtlayabilecek veya zarar verebilecek online olarak yayın yapan televizyon, radyo, film, oyun vb. içerikli yayınlar kullanılmamalıdır.

j) ETIQA e-posta adresi ile internet üzerinde forum, alışveriş vb. sitelere üye olunmamalıdır.

k) ETIQA hesaplarına ait kullanıcı adı ve şifrenizin internet üzerinden paylaşılmamalıdır.

l) ETIQA içerisinde kullanılan kullanıcı adı ve şifreleri ile sosyal hayatta kullanılan kullanıcı adı ve şifreleri aynı olmamalıdır.

m) İnternet üzerinden yaptığınız kişisel işlemlerinizde (banka, alışveriş, mail vb.) oluşacak olumsuzluklardan kurumumuz sorumlu değildir. Ayrıca, kurum veya kişisel hesabınızı ele geçiren kişi veya kişiler sizin adınıza suç işleyebilir, bu işlemden sorumlu olabilirsiniz.

n) İnternette gezinirken reklam veya bilgi çalmak amaçlı *(tebrikler, ödül kazandınız, ödülünüzü almak için tıklayın vb.)* aldatıcı resim ve yazılara karşı dikkatli olunmalı ve tıklanmamalıdır.

o) Üçüncü şahıslar, **ETIQA** internet erişimleri kablosuz ağdan gerçekleşmektedir. Sisteme telefon numarası üzerinden kayıt yapılarak erişim sağlanmaktadır.

p) ETIQA personelinin internete girmek için kendisine verilen kurum kimliği ve şifresini başkalarıyla paylaşmamalıdır.

q) ETIQA network ağına kuruma ait olmayan cihazlar bağlanmamalıdır. Bu cihazların **ETIQA** ağına bağlanması gereken durumlarda Bilgi İşlem birimine haber verilmelidir.

4.3. E-Posta Kullanım Kuralları

a) ETIQApersonelinin kurumsal e-postalarından gönderdikleri, aldıkları veya sakladıkları e-postalar **ETIQA**bilgi varlığıdır. Bu yüzden yetkili kişiler gerekli durumlarda önceden haber vermeksizin e-posta mesajlarını denetleyebilir, yasal merciler ile paylaşabilir.

b) Bilinmeyen ve şüpheli bir kaynaktan gelen e-posta ve ekleri virüs içerebilir. Kesinlikle ekler indirilmemeli veya açılmamalıdır. Bu tür özelliklere sahip bir mesaj alındığında hemen Bilgi İşlem birimine veya Bilgi Güvenliği Ekibine haber verilmelidir. Yetkili kişiler müdahale edene kadar mesajın silinmemesi, yanıtlanmaması, iletilmemesi ve içeriğine tıklanmaması gerekmektedir.

c) ETIQA kurumsal e-posta hesapları kişisel amaçlar için kullanılmamalıdır.

d) ETIQA e-posta sistemi, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz. Bu tür özelliklere sahip bir mesaj alındığında hemen ilgili birim yöneticisine veya Bilgi Güvenliği Ekibine haber verilmesi ve daha sonra bu mesajın tamamen silinmesi gerekmektedir.

e) Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.

f) Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen Bilgi Güvenliği Ekibine haber verilmelidir.

g) Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.

h) Kullanıcıların kullanıcı kodu / şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal Bilgi Güvenliği Ekibine haber verilmelidir.

i) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir.

j) Kurum personeli kurumsal e-postaların herhangi bir kişi tarafından okunmamasını sağlamakla yükümlüdür.

k) **ETIQA** mail hesabı kurulu olan cep telefonlarında ekran kilidi özelliği aktif olmalıdır.

4.4. Parola Kullanım Kuralları

a) Parolalar bilgisayar güvenliği için önemli bir özelliktir. Parolalar kompleks olmalıdır. Kolay tahmin edilen *(memleket, çocuk ismi, doğum tarihi, ardışık rakam ve harfler, İstanbul, Ankara, 1qaz2wsx, qwerty vb.)* parolalar kullanılmamalıdır.

b) **ETIQA** içerisinde kullanılan genel kullanıcı bilgisayar şifreleri 90 günde bir değiştirilmesi zorunlu kılınmıştır.

c) Oluşturulacak şifre son 3 parola ile aynı olamaz.

d) Oluşturulacak parola içerisinde Türkçe karakter bulunmamalıdır.

e) Bilgisayar kullanıcı hesaplarının parolaları en az 8 karakter olmalıdır. Parola; büyük harf, küçük harf, rakam ve özel karakterden oluşmalıdır.

f) Kullanıcılar bilgisayar başından kalktığı zaman mutlaka oturumlarını kilitlemelidirler. *(Windows + L)* Genel kullanıcı bilgisayarları kullanılmadığı zaman otomatik olarak 10 dakika içerisinde şifreli ekran korumasına girecektir.

g) Parolanın 5 kez üst üste yanlış girilmesi sistemin kilitlenmesine sebep olmaktadır. Parola unutulması durumunda Bilgi İşlem Birimi ile iletişime geçilmelidir.

h) Kurumsal hesaplarınıza ait parolalarınız e-posta iletilerine, herhangi bir elektronik veya fiziksel bir ortama not alınmamalıdır.

i) Parola aile bireyleri dâhil kimseyle paylaşılmamalıdır.

j) Bilgi İşlem Birimi tarafından verilen yeni parolalar hemen değiştirilmelidir.

k) Bir kullanıcı hesabı birden çok kişi tarafından kullanılmamalıdır.

l) Kişisel Verilerin Korunması Kanunu'na istinaden **ETIQA** personelinin bizzat kendi talebi olmaksızın parolası sıfırlanamaz veya değiştirilemez.

m) Çok kritik veya kişisel verilerin üçüncü taraf kişi/kurumlar ile paylaşılması gereken durumlarda, bilgi şifrelenmeli ve şifre farklı bir yöntemle ilgili kişiye iletilmelidir.

4.5. Fiziksel Güvenlik Kuralları

a) 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.

b) Ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili görevliler gözetiminde gerçekleştirilmelidir.

c) Tanımlanan farklı güvenlik bölgelerine erişim yetkileri düzenli aralıklar ile kontrol edilmelidir.

d) Ofis girişleri ve koridorlar güvenlik açısından kamera ile kayıt altına alınmaktadır. Çalışma ortamlarının kapıları molalarda veya mesai bitimlerinde kapalı tutulmalıdır.

e) Açık ofislerde bulunan gizli bilgi varlıklarının olduğu dolaplar ve çekmeceler kilitli ve kontrol altında tutulmalıdır.

f) Bireysel kargo alınmamaktadır. Kurumsal kargolar fiziksel kontrol (X-Ray, gözlemleme vs.) cihazından geçirilip danışmaya teslim edilir.

g) Hasar / hırsızlık gibi oluşabilecek risklere karşı güvenlik sağlanmalıdır.

h) Ekipmanların kullanımı zimmetlenen kişiye aittir, bu ekipmanların güvenliğini sağlanması kişinin sorumluluğundadır.

i) Gizlilik derecesi yüksek dokümanların şehir içi teslimi görevlendirilen personel vasıtasıyla elden yapılmalıdır.

j) ETIQAdışına çıkarılan mobil cihazlar hırsızlık veya fiziksel hasara karşı uygun şekilde muhafaza edilmelidir.

4.6. Temiz Masa Temiz Ekran Kuralları

a) Çalışma sonunda kâğıt ortamında ya da elektronik cihazlar üzerinde tutulan *"gizli ya da çok gizli"* bilgiler güvenli ortamlarda *(çelik kasa, kilitli dolap ve çekmeceler vb.)* saklanmalıdır.

b) Her türlü haberleşmede kullanılan cihazlar *(telefon, faks, fotokopi makineleri)* yetkisiz erişimlere karşı korunmalıdır. Cihazlar üzerinde kurum bilgisi veya kişisel veri barındıran belge, doküman bırakılmamalıdır.

c) Sistemlerde kullanılan parola, telefon numarası ve T.C kimlik numarası vb. hassas bilgiler ekran üstlerinde veya masa üstünde bulunmamalıdır.

d) Her türlü bilgi, parolalar, anahtarlar ve bilginin sunulduğu sistemler, ana makineler *(sunucu)*, bilgisayarlar vb. cihazlar yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde bırakılmamalıdır.

e) Faks ve fotokopi makinelerinde gelen giden yazılar sürekli kontrol edilmeli ve makinede evrak bırakılmamalıdır. Hatalı baskı alınan dokümanlar müsvedde olarak kullanılmamalı, içeriği okunamayacak şekilde imha edilmelidir.

f) Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler kâğıt öğütücü, disk/disket kıyıcı, yakma vb. metotlarla imha edilmeli, bilginin geri dönüşümü ya da yeniden kullanılabilir hale gelmesinin önüne geçilmelidir.

g) Personelin kullandığı masaüstü veya dizüstü bilgisayarlar iş sonunda ya da masa terkedilecekse ekran kilitlenmelidir. Bu işlem Windows + L tuşuna basılarak yapılabilir.

h) Bilgisayarların masaüstlerindeki klasör ve dosyalar düzenli tutulmalıdır.

i) Parola, gizli veya çok gizli bilgiler, defter ve ajanda gibi ortamlara yazılmamalıdır.

4.7. Kişisel Veri Güvenlik Kuralları

a) Kişisel veriler amacı dışında kullanılmamalıdır. İşin gereği kadar kişisel veriler, veri sahibinden talep edilmelidir. Elde edilen kişisel veriler bütünlüğü sağlayacak şekilde korunmalıdır.

b) Kişisel veriler kullanım amacı haricinde 3. Taraflar ile paylaşılmamalıdır.

c) Kişisel veriler, kurumun onaylamış olduğu imha yöntemleri ile yok edilmelidir. Kişisel verilerin saklama süreleri en geç 6 ayda bir kontrol edilmelidir.

d) ETIQA'nin sorumlu olduğu kişisel veriler hiçbir hukuki şart, sözleşme ya da yasal dayanak yoksa kurum dışından üçüncü şahıslara iletilmemelidir. **ETIQA**'nin sorumlu olduğu kişisel veriler (çalışanlar, müşteriler,

tedarikçiler, acenteler vs.) ilgili kişinin izni olmadan 3. taraf kişiler ile paylaşılmamalıdır. Güvenilir kaynaklardan gelen talepler doğrultusunda işin gereği kadar veri paylaşılmalıdır.

e) Kişisel veriler 3.taraf kişi/kurumlara aktarılırken teknik ve idari tedbirleri alınmalıdır. 3. Taraflara kişisel veri aktarımında, kişisel veriler şifreli gönderilmelidir.

f) Kişisel verilerin kullanılmasını gerektiren sebeplerin ortadan kalkması hâlinde verilerin aktarıldığı 3.taraf kişi/kurumlar bilgilendirilmelidir.

g) Ortak kullanılan cihazların (yazıcı, fax, fotokobi vb.) üzerinde kişisel veri barındıran belgeler bırakılmamalıdır.

h) Temiz Masa Temiz Ekran kurallarına uyulmalı, kişisel veri bulunduran basılı doküman ve bilgi depolayan medyalar (usb bellek, harici disk, cd vb.) masaların üzerinde bırakılmamalıdır.

i) Kişisel verilerin bulunduğu ortamlar yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde başıboş bırakılmamalıdır.

j) Aşağıda belirtilen hususların yaşanması durumunda **ETIQA**İrtibat Kişisi aynı gün bilgilendirilmelidir;

- Kişisel veri ihlâlinin gerçekleşmesi durumunda oluşması durumunda,
- Kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde,
- Kurum içinde ihlale sebebiyet verebilecek/verebilen açıklıkların oluşşması durumunda,
- Saklama süresi dolan verilere aksiyon alınması gereken durumlarda,

k) Kurum içi ve kurum dışı kişisel veri sahiplerinin, işlenen kişisel verileri hakkında talepleri Aydınlatma Beyanında (web sayfasında mevcut) belirtilen yöntemlere göre alınmalıdır.

l) Veri sahiplerinden gelen kişisel veri talepleri olumlu yada olumsuz en geç 30 gün içinde veri sahibine dönüş yapılmalıdır. Veri sahibi talebinin kabul edilmesi durumunda ise cevap dönülmesinden itibaren en geç 30 gün içerisinde aksiyon tamamlanmalıdır.

m) ETIQA 'nin KVKK 'ya şikayet edilmesi durumunda en kısa sürede deliller toplanmalıdır. Talep ve şikayetlerin yönetimi için idari ve teknik tedbirlere göre uygun hareket edilmelidir.

n) Veri sahiplerinin kişisel verilerinin işlenmesi için açık rıza alınması gereken durumlarda, açık rıza alınmadan kişisel veriler kullanılmamalıdır.

o) Çalışanlar, birimlerinde yeni bir iş süreci oluşması ve/veya kişisel verilerin kullanma amaçlarının değişmesi durumunda, birim yöneticilerilerini ve **ETIQA** İrtibat Kişisi'ni bilgilendirmelidir.

p) İşten ayrılan bir personelin mail adresinin kendisine yönlendirilmesi durumunda, maile gelen kişisel içerikler amacı dışına kullanılmamalıdır.

4.8. Bulut Kullanım Kuralları

a) Bulut hizmetlerini kullanmadan önce, çalışanlarımızın uygulama politikalarını, kullanıcı politikalarını ve prosedürlerini anlamaları ve uygulamaları gerekmektedir.

b) Hassas veya gizli bilgileri bulut hizmetlerine yüklerken, şifreleme kullanarak veriler korunmalıdır.

c) Bulut hizmetlerindeki kullanıcı kimliklerini ve erişim yetkilerini düzenli olarak gözden geçirerek, yetkisiz erişimler önlenmelidir.

d) Bulut hizmetlerine erişimde çok faktörlü kimlik doğrulama (örneğin, şifre ve SMS doğrulama kodu) kullanılmalı.

e) Bulut hizmetlerinde güçlü şifreleme algoritmaları ve güvenli iletişim protokolleri kullanılmalıdır.

f) Bulut hizmetlerinde kaydedilen logları ve izleme verilerini düzenli olarak incelemeli ve anormal aktiviteleri tespit edilmeli.

g) Şirket çalışanları, şirketin onayladığı ve kuruma ait LOGO sunucusu üzerinde verilerini yönetmelidir.

h) LOGO sunucusu üzerinde gizli ve kişisel veriler içermemelidir.

i) LOGO sunucusuna erişimde kullanılan parolalar 3. kişiler ile paylaşılmamalıdır.

j) LOGO sunucusu üzerinde paylaşılan dosyalara erişimler hizmet bittiği zaman kaldırılmalıdır.

BGYS KULLANICI POLİTİKALARI KABUL ONAYI

Kurum Yönetim Sistemi Politikalarında ifade edilen tüm kurallara uymayı, iş bu güvenlik politikalarının ve revizyonlarının Bilgi Güvenliği Yönetim Sistemi'nde yayınlandığını bildiğinizi ve güncellemeleri takip ederek iş bu değişikliklere uygun davranacağınızı aksi takdirde hakkınızda disiplin ve yasal her türlü işlemin başlatılacağını bildiğinizi kabul ve taahhüt etmektesiniz.

İzlenecek Prosedür

1. Bilgi Güvenliği Politikasını okuyunuz.
2. Aşağıdaki belirtilen bölümlere bilgileri doldurup imzalayınız.
3. Bu sayfayı İnsan Kaynakları ve Eğitim Müdürlüğü'ne teslim ediniz.

Kullanıcı Taahhüdü

Bu forma imza atarak BGYS Kullanıcı Politikalarında yazan kurallara uyacağımı taahhüt ediyorum.

ETIQABGYS Kullanıcı Politikalarının kabul onayının bir kopyasını teslim aldım, okudum ve anladım.

Personelin;

İmza :

T.C. Kimlik/Pasaport No :

Ad ve Soyad :

Unvan :

Bölüm :

Tarih :