

HİZMETE ÖZEL



Bilgi Güvenliği Politika Bildirisi

TEI'nin kurumsal misyonu "Havacılıkta kullanılan güç sistemleri ve türevleri için küresel ölçekte, rekabetçi, sürdürülebilir ve özgün ürünler tasarlayan, üreten ve servis hizmeti veren lider motor şirketi olmak"; kurumsal vizyonu ise "Küresel olarak rekabetçi özgün güç sistemleri sahibi olmak"tır.

TEI'nin sahip olduğu bilginin ve bilgi varlıklarının kurumsal vizyonu doğrultusunda belirlediği stratejiler ve iş hedeflerine uygun şekilde korunması ve kullanılması diğer bir ifadeyle bilgi güvenliği gereksinimlerinin karşılanması kurumsal iş akışlarına yeni faaliyetlerin dahil edilmesini veya yeni düzenlemeler yapılmasını gerektirmektedir. Bu faaliyetlerin yönetilebilmesi etkin bir Bilgi Güvenliği Yönetim Sistemi ile mümkündür.

Bilgi güvenliği ve yönetimi konuları son yıllarda bütün dünyada büyük önem kazanmıştır. Kurumlar ve paydaşlar arasında ortak bir bilgi güvenliği anlayışı oluşturmak amacıyla teknik ve yönetsel tavsiyeler içeren ISO-27002 uluslararası standardı geliştirilmiştir. TEI de kurumsal yönetim stratejileri doğrultusunda bu ve benzeri uluslararası kabul görmüş uygulamalar paralelinde, risk bazlı ve etkin bir yapıda verimli ve güvenli bilgi yönetimi sağlayarak; daha kaliteli ve güvenilir bilişim çözümlerine ulaşmaktadır.

TEI'de bu sebeplerle, kurum çapındaki bilgi güvenliği altyapısının sistematik olarak yönetilmesi için ISO-27001 standardına uygun bir Bilgi Güvenliği Yönetim Sistemi kurulmuştur. Bu amaçla Kurumsal Bilgi Güvenliği Politikası, Bilgi Güvenliği Yönetim Sistemi El Kitabı ve işbu Bilgi Güvenliği Politika Bildirisi yayımlanmış ve gerek duyulduğunda da güncellenmekte olup, yürütülen farkındalık süreci ile tüm çalışanlarımızın bu dokümanlarda yer alan esasları benimsemesi, bu esaslara uygun hareket etmesi beklenmekte ve yönetimimiz tarafından en üst seviyede desteklenmektedir.

TEI, Bilgi Güvenliği Yönetim Sistemi'ne ait standartların gereklerini tüm çalışanları ile uygulayarak, sistemin düzenli olarak gözden geçirilmesi ve sürekli iyileştirme faaliyetlerinin desteklenmesi gerektiğinin bilincindedir.

TEI'de Bilgi Güvenliği Yönetim Sisteminin kurulmasını ve işlerliğe kavuşturulmasını takiben sistem, ISO-27001 kriterlerine uygun olarak dış denetime tabi tutulmuş ve Eylül 2009 tarihinde sertifikalandırılmıştır.

TEI'de Bilgi Güvenliği Yönetim Sisteminin kurulması çalışmalarını bilgi varlıklarımıza yönelik bir risk analizi ile başlatılmıştır. Bu çalışma sırasında öncelikle TEI'nin sahip olduğu tüm bilgi varlıklarının envanteri oluşturulmuş ve sahipleri belirlenmiştir. Varlıklar için gereken koruma düzeyi gizlilik, bütünlük ve erişilebilirlik açısından tanımlanmıştır. Bilgi varlıklarının maruz kalabilecekleri tehditler belirlenmiş ve gerçekleşme olasılıkları değerlendirilmiştir. Bu veriler ışığında risk seviyeleri hesaplanmış ve listelenmiştir.

Bu risklere karşı önlemler kararlaştırılırken, aşağıdaki hususlar gözönüne alınmıştır:

Bu doküman ve ekleri sadece yollanan kişinin kullanımı içindir ve TEI'ye ait gizli ve/veya özel bilgi içerebilir. Herhangi bir izinsiz inceleme, kullanım veya dağıtım yasaktır. Eğer dokümanın yollandığı kişi değilseniz, lütfen gönderen kişiyle temasa geçin ve orjinal dokümanı tüm kopyaları ve varsa ekleri ile beraber yok edin. Ayrıca bu dokümandaki ve/veya eklerindeki bilgiler uluslararası ihracat kontrol kurallarına tabii olabilir. Bu tip bilgiler öncelikle ilgili idari onaylar alınmadan yayınlanamaz ve üçüncü kişilerle paylaşamaz.

HİZMETE ÖZEL

HİZMETE ÖZEL



Gizlilik - Hassas bilgileri yetkisiz kişilerin erişimine karşı koruyarak,
Bütünlük - Bilgiyi yetkisiz kişilerin değiştirmesine ve tahrif etmesine karşı koruyarak,
Erişilebilirlik – Bilgiyi ihtiyaç duyulduğu anda ve yerde kullanıma hazır bulundurarak sağlar.

TEI iş faaliyetlerini yerine getirirken bir yandan ulusal ve uluslararası kanunlara diğer yandan Ortaklık Anlaşması hükümlerine, müşterileri ve tedarikçileri ile yaptığı sözleşme şartlarına uyumlu olmakla yükümlüdür. İlgili yasalardan ve anlaşmalardan doğan uyum gerekliliğinin TEI çalışanları tarafından kabul edilip, uygulanması için oluşturulan politika, yönetmelik ve uygulamalar bütününe Kurumsal İş Bütünlüğü adı verilmektedir.

Kurumsal İş Bütünlüğü, ISO27001 BGYS'nin bir alt bileşenidir.

TEI'de Kurumsal İş Bütünlüğünün alt başlıkları:

- Kurumsal Alt Yapı
- İş Etiği Uygulamaları
- Çıkar Çatışmalarının Önlenmesi
- Tedarikçilerle İlişkiler
- Uluslararası Ticaret Kurallarına Uyum
- Rekabetin Korunması
- Devlet Kuruluşları İle Çalışma
- Kurumsal Bilgi Güvenliği

şeklinde sıralanmaktadır.

TEI çalışanlarının Kurumsal İş Bütünlüğü ile ilgili tüm politikalar konusunda bilgi sahibi olmaları, TEI için yürüttükleri günlük çalışmalarında da bu politikaları yerine getirecek şekilde hareket etmeleri beklenmektedir.

TEI'de görev yapan her kademedeki yöneticiler, tüm çalışanlar, sözleşmeler çerçevesinde iş yapan kişi ve kuruluşlar; elektronik, kağıt ve diğer biçimlerdeki bilginin gizliliğini, doğruluğunu, erişilebilirliğini ve bütünlüğünü korumak, bilgi kaynaklarını her zaman ayakta tutabilmek konusundaki sorumluluklarını yerine getirmekle yükümlü olup, gerektiğinde bilgi güvenliğinde yaşanacak aksaklıklardan dolayı yetki ve sorumlulukları çerçevesinde hesap vereceğinin bilincinde olmalıdırlar.

Bu doküman ve ekleri sadece yollanan kişinin kullanımı içindir ve TEI'ye ait gizli ve/veya özel bilgi içerebilir. Herhangi bir izinsiz inceleme, kullanım veya dağıtım yasaktır. Eğer dokümanın yollandığı kişi değilseniz, lütfen gönderen kişiyle temasa geçin ve orjinal dokümanı tüm kopyaları ve varsa ekleri ile beraber yok edin. Ayrıca bu dokümandaki ve/veya eklerindeki bilgiler uluslararası ihracat kontrol kurallarına tabii olabilir. Bu tip bilgiler öncelikle ilgili idari onaylar alınmadan yayınlanamaz ve üçüncü kişilerle paylaşamaz.

HİZMETE ÖZEL

HİZMETE ÖZEL



TEI'nin Bilgi Güvenliği Yönetimi çalışmalarının koordinasyonu Bilgi Güvenliği Yönetim Komitesi tarafından yürütülmektedir. Bu Komite, Kurumsal Bilgi Güvenliği Politikası, Bilgi Güvenliği Yönetim Sistemi El Kitabı ve işbu Bilgi Güvenliği Politika Bildirisi'nde yer alan esasları oluşturmaktan ve sürekliliğinin sağlanmasından sorumludur.

Rol ve Sorumluluklar:

Bilgi güvenliği, kurumsal bir sorumluluktur. Kurumumuzda bilgi güvenliği süreçlerinin sağlıklı şekilde işletilmesi için gerekli roller, yetki ve sorumluluklar aşağıdaki gibidir:

Rol Adı : Üst Düzey Bilgi Güvenliği Yöneticisi

Atama : Genel Müdür

Sorumluluklar :

Kurum içinde Bilgi Güvenliği Yönetim Sisteminin tüm mekanizmalarıyla işler halde olduğunun denetimi, gerektiğinde ilgili hukuksal süreçlerin devreye alınması konuları, üst düzey yönetim tarafından sağlanmaktadır.

Bu rolü üstlenen kişi,

- Bilgi güvenliği ile ilgili kasten veya kazara ortaya çıkan vakaların ve acil durumların incelenmesini sağlamak,
- Bilgi Güvenliği Politika Bildirisi ve değişikliklerini onaylamak, bunların güncel durumlarıyla ilgili bilgi sahibi olmak,
- Kurum içinde çalışanların bilgi güvenliği yönetimi süreçlerine katkısı için gereken önlemlerin alınmasını, ödül ve ceza mekanizmalarının tanımlanmasını sağlamak,
- Üst düzey yönetici yetkisi gerektiren diğer bilgi güvenliği yönetimi işlerini yerine getirmek ile yükümlüdür.

Rol Adı : Bilgi Güvenliği Koordinatörü

Atama : İnsan Kaynakları Direktörü

Sorumluluklar :

- Birim yöneticileriyle koordinasyonu sağlamak, işleyişe ilişkin izleme ve değerlendirme faaliyetlerini yürütmek,
- Risk değerlendirmesi süreçlerinin aralıklarla tekrarlanmasını sağlamak,

Bu doküman ve ekleri sadece yollanan kişinin kullanımı içindir ve TEI'ye ait gizli ve/veya özel bilgi içerebilir. Herhangi bir izinsiz inceleme, kullanım veya dağıtım yasaktır. Eğer dokümanın yollandığı kişi değilseniz, lütfen gönderen kişiyle temasa geçin ve orjinal dokümanı tüm kopyaları ve varsa ekleri ile beraber yok edin. Ayrıca bu dokümandaki ve/veya eklerindeki bilgiler uluslararası ihracat kontrol kurallarına tabii olabilir. Bu tip bilgiler öncelikle ilgili idari onaylar alınmadan yayımlanamaz ve üçüncü kişilerle paylaşamaz.

HİZMETE ÖZEL

HİZMETE ÖZEL



- Raporlanan bilgi güvenliği ihlallerinin çözümlenmesi için gerekli görevlendirmeyi yapmak ve sonuçlandırmak,
- Birimine bağlı kullanıcılar, diğer birim yöneticileri ve üst düzey yönetimde yer alan kullanıcılara verilen yetki ve ayrıcalıkları ve yetki seviyelerinde talep edilen değişiklikleri onaylamak
- Acil Durum Ekibi'ninin başkanlık görevini üstlenmek,
- Bilgi Güvenliği Yönetim Sistemi El Kitabı'nda bulunan yönetmelikleri ve değişiklikleri onaylamak,
- Bilgi güvenliği ile ilgili bilinç ve duyarlılığı sürekli kılmak için eğitim programları düzenlenmesini sağlamak,
- Sorumluluğu altındaki konularda, Üst Düzey Yönetim'e rapor vermek.

Rol Adı : Bilgi Güvenliği Sistem Yöneticileri

Atama : Bilişim Teknolojileri Müdürü ve Sistem Network Takım Lideri

Sorumluluklar :

- Bilgi sistem ve servislerinin güvenli işleme izin verecek biçimde kurulmasını ve yapılandırılmasını sağlamak,
- Bilgi sistem ve servislerinin izlenmesini ve aykırı durumların tespitini sağlamak,
- Sorumluluğu altında bulunan bilgi varlıklarında bilgi güvenliği risklerini etkileyecek bir değişiklik olduğunda, risk değerlendirmesi yapılması için Bilgi Güvenliği Koordinatör'ünü bilgilendirmek,
- Teknolojik gelişmeleri takip ederek kuruma yarar sağlayacak yeniliklerle ilgili bilgi derlemek ve bu bilgilerin uygulanmasında bilgi güvenliği ile ilgili olabilecek hususlar hakkında Bilgi Güvenliği Yöneticisi'ni bilgilendirmek,
- Bilgi sistemlerin yetki yönetimlerinin Kurumsal İş Bütünlüğü ile ilgili TEI Politikaları, Kurumsal Bilgi Güvenliği Politikası ve Bilgi Güvenliği Yönetim Sistemi El Kitabı'nda bulunan yönetmelikler çerçevesinde yapılmasını sağlamak,
- Kurum bilgilerinin yedeklenmesini ve yedeklerin kullanıma hazır olduğunun test edilmesini sağlamak,
- Tespit ettiği bilgi güvenliği ihlal olaylarını Bilgi Güvenliği Yöneticisi'ne rapor etmek.

Bu doküman ve ekleri sadece yollanan kişinin kullanımını içindir ve TEI'ye ait gizli ve/veya özel bilgi içerebilir. Herhangi bir izinsiz inceleme, kullanım veya dağıtım yasaktır. Eğer dokümanın yollandığı kişi değilseniz, lütfen gönderen kişiyle temasa geçin ve orjinal dokümanı tüm kopyaları ve varsa ekleri ile beraber yok edin. Ayrıca bu dokümandaki ve/veya eklerindeki bilgiler uluslararası ihracat kontrol kurallarına tabii olabilir. Bu tip bilgiler öncelikle ilgili idari onaylar alınmadan yayınlanamaz ve üçüncü kişilerle paylaşamaz.

HİZMETE ÖZEL

HİZMETE ÖZEL



Rol Adı : Strateji Planlama Yöneticileri

Atama : Strateji ve Kalite Sistemleri Müdürü ve Endüstriyel Güvenlik Lideri

Sorumluluklar :

- Sanayi güvenliğiyle ilgili faaliyetleri (stratejik planının devamlılığının sağlanması, projelerin gizlilik derecelerine uygunluğu vb.) takip ve koordine etmek, gerekli değişiklik ve düzenlemeler için Bilgi Güvenliği Koordinatörü'nü bilgilendirmek,
- İş ve yer emniyeti kapsamında olası risklerin analiz edilerek tedbir alınması hususunu ilgili birimlerle koordine etmek, bu konuda alınması gereken önleyici tedbirleri geliştirmek, meydana gelen iş kazaları, acil durumlar ve personelin sağlık ve güvenliğini tehdit eden olayların olası sebeplerini analiz etmek ve alınması gereken tedbirleri geliştirerek, izlenebilir şekilde uygulanmasını sağlamak,

Rol Adı : Fiziki Güvenlik Yöneticileri

Atama : Tesisler ve Destek Hizmetler Müdürü ve Güvenlik Lideri

Sorumluluklar :

- Personel güvenliği, fiziki güvenlik önlemleri, yangın, sabotaj ve olağanüstü hal hizmetleri, evrak, döküman ve malzeme güvenliği, kontrollü oda ve kontrollü bölge güvenliği konularında uyulması gereken kural ve alınması gereken önlemleri belirlemek, konulan kuralların uygulanmasını sağlamak ve aksaklıklar için tedbir almak,
- Milli Savunma Bakanlığı tarafından oluşturulan Savunma Sanayi Güvenliği mevzuatında tanımlı tüm güvenlik önlemlerinin eksiksiz olarak uygulanmasını koordine etmek,

Rol Adı : Bilgi Güvenliği Yöneticileri

Atama : Sözleşmeler Müdürü ve Sözleşmeler ve Lisans Lideri

Sorumluluklar :

- Bilgi Güvenliği Yönetim Sistemi'nin etkinliğini ve uygulamanın Kurumsal İş Bütünlüğü ile ilgili TEI Politikaları, Kurumsal Bilgi Güvenliği Politikası ve Bilgi Güvenliği Yönetim Sistemi El Kitabı'nda bulunan yönetmelikler ile uyumlu yürütüldüğünü kontrol etmek,
- Bilgi güvenlik politika ve prosedürleriyle ilgili olarak, çalışanlardan gelen revizyon taleplerini değerlendirmek ve onaya sunmak,
- Bilgi güvenliği önlemlerinin iyileştirilmesi yönünde çalışmalar yapılmasını sağlamak, gerekirse yeni önlemler önermek,
- Diğer kurumlarla yapılan çalışmalara/anlaşmalara gereken bilgi güvenliği gereksinim ve kurallarını dahil etmek,

Bu doküman ve ekleri sadece yollanan kişinin kullanımı içindir ve TEI'ye ait gizli ve/veya özel bilgi içerebilir. Herhangi bir izinsiz inceleme, kullanım veya dağıtım yasaktır. Eğer dokümanın yollandığı kişi değilseniz, lütfen gönderen kişiyle temasa geçin ve orjinal dokümanı tüm kopyaları ve varsa ekleri ile beraber yok edin. Ayrıca bu dokümandaki ve/veya eklerindeki bilgiler uluslararası ihracat kontrol kurallarına tabii olabilir. Bu tip bilgiler öncelikle ilgili idari onaylar alınmadan yayınlanamaz ve üçüncü kişilerle paylaşamaz.

HİZMETE ÖZEL

HİZMETE ÖZEL



- Bilgi Güvenliği Yönetim Sistemi'nin çalışanlar tarafından benimsenmiş, kabul görmüş ve kullanılabilir durumda olduğunu izlemek,
- Sorumluluğu altındaki konularda, Bilgi Güvenliği Koordinatörü'ne rapor vermek.

Rol Adı : İnsan Kaynakları Yöneticisi

Atama : Kariyer Geliştirme ve Eğitim Müdürü ve Özlük ve Dokümantasyon Yönetim Lideri

Sorumluluklar :

- Kurumsal İş Bütünlüğü ile ilgili TEI Politikaları, Kurumsal Bilgi Güvenliği Politikası ve Bilgi Güvenliği Yönetim Sistemi El Kitabı'nda bulunan yönetmelikler çerçevesindeki yetki ve sorumlulukları, oryantasyon programı dahilinde işe yeni başlayan personele duyurmak,
- Kurumsal Bilgi Güvenliği Politikası ve Bilgi Güvenliği Yönetim Sistemi El Kitabı'nda bulunan yönetmeliklerine uygun davranmayan personel ile ilgili yaptırımların belirlenmesini ve uygulanmasını sağlamak,
- Kimlik yönetimine veri sağlayan insan kaynakları veritabanındaki değişikliklerin vaktinde, hızla gerçekleştirilmesini sağlamak,
- Bilgi Güvenliği Yöneticisi'nden gelen bilgi güvenliği farkındalık eğitimlerinin düzenlenmesi taleplerini değerlendirerek bu eğitimlerin gerçekleştirilmesini sağlamak.
- Raporlanan bilgi güvenliği ihlalleri ile ilgili Bilgi Güvenliği Yönetim Sistemi Komitesine bilgi vermek, Komite kararına göre hareket edilmesi,
- Yukarıdaki rollere atanan kişiler TEI Bilgi Güvenliği Yönetim Komitesi'nde görev almaktadır.

Rol Adı : Birim Güvenlik Sorumlusu

Atama : Birim Yöneticileri

Sorumluluklar :

- Birim içinde kullanılmak üzere, Kurumsal İş Bütünlüğü ile ilgili TEI Politikalarını, Kurumsal Bilgi Güvenliği Politikası ve Bilgi Güvenliği Yönetim Sistemi El Kitabı'nda bulunan yönetmeliklerini destekleyici ve birimin iş akışlarını kapsayan prosedürlerin hazırlanmasını ve güncel tutulmasını sağlamak,
- Birim çalışanlarının Kurumsal Bilgi Güvenliği Politikası ve Bilgi Güvenliği Yönetim Sistemi El Kitabı'nda bulunan yönetmeliklere uygun çalışmasını sağlamak,
- Sorumluluğu altında bulunan bilgi varlıklarında bilgi güvenliği risklerini etkileyecek bir değişiklik olduğunda, risk değerlendirmesi yapılması için Bilgi Güvenliği Koordinatörü'nü bilgilendirmek,
- Bilgi güvenliği eğitimlerine gerekli katılımı sağlamak,

Bu doküman ve ekleri sadece yollanan kişinin kullanımı içindir ve TEI'ye ait gizli ve/veya özel bilgi içerebilir. Herhangi bir izinsiz inceleme, kullanım veya dağıtım yasaktır. Eğer dokümanın yollandığı kişi değilseniz, lütfen gönderen kişiyle temasa geçin ve orjinal dokümanı tüm kopyaları ve varsa ekleri ile beraber yok edin. Ayrıca bu dokümandaki ve/veya eklerindeki bilgiler uluslararası ihracat kontrol kurallarına tabii olabilir. Bu tip bilgiler öncelikle ilgili idari onaylar alınmadan yayınlanamaz ve üçüncü kişilerle paylaşılmaz.

HİZMETE ÖZEL

HİZMETE ÖZEL



- Bilgi Güvenliği Koordinatörü'nün düzenlediği koordinasyon çalışmalarına katılmak,
- Birimine bağlı kullanıcılar ile birimine ait varlıklara erişim talebinde bulunan kullanıcılara verilen yetki ve ayrıcalıkları ve yetki seviyelerinde talep edilen değişiklikleri onaylamak
- Birimiyle ilgili güvenlik vakalarını değerlendirerek, Bilgi Güvenliği Yöneticisi'ne bildirilmesini sağlamak,
- Kimlik Yönetimi Sistemi'ni kullanarak birim çalışanlarının yetkileriyle ilgili değişikliklerin talep edilmesini sağlamak ve bu talepleri değerlendirerek uygun olanlarını onaylamak
- Biriminin diğer kurumlarla yaptığı çalışmalarda/anlaşmalarda bilgi güvenliği ile ilgili gereksinim ve kuralları Bilgi Güvenliği Yöneticisi'nden destek alarak belirlemek.

Rol Adı : Bilgi Sistemi Kullanıcısı

Atama : TEI Sistemleri Kullanıcıları

Sorumluluklar :

- Kurumsal İş Bütünlüğü ile ilgili TEI Politikalarına, Kurumsal Bilgi Güvenliği Politikası ve Bilgi Güvenliği Yönetim Sistemi El Kitabı'nda bulunan yönetmeliklerine, birim güvenlik yönetmelik ve standartlarına uygun hareket etmek,
- Bilgi güvenliğiyle ilgili eğitim eksikliği duyduğu durumlarda bu durumu Birim Güvenlik Sorumlusu'na bildirmek,
- Sorumluluğu altındaki bilgi varlıklarını uygun şekilde korumak,
- Bilgi güvenliği ilgili bir ihlal tespit ettiğinde, bu durumu Birim Güvenlik Sorumlusu'na duyurmak,
- Bilgi Güvenliği Yönetim Sistemi El Kitabı'nda bulunan yönetmeliklere ilişkin değişiklik önerilerini Birim Güvenlik Sorumlusu kanalıyla Bilgi Güvenliği Yöneticisi'ne iletmek.

Politika Uygunluğunun İzlenmesi :

Gerek TEI İç Denetleme ve Değerlendirme Kurulu Başkanlığı gerekse BGYS İç Denetçileri, Bilgi Güvenliği Yönetim Sistemi'nin uygun şekilde işletilmesini sağlamak için, gözetim ve denetim işlevlerini üstlenmiştir. Bilgi Güvenliği Yönetim Komitesi yılda en az bir kez toplanıp Kurumsal İş Bütünlüğü, Kurumsal Bilgi Güvenliği Politikası ve Bilgi Güvenliği Yönetim Sistemi El Kitabı'nda bulunan yönetmelikleri gözden geçirerek, sistemin uygulama süreçlerini iyileştirmek için gerekli önlemleri almaktadır.

Tüm TEI çalışanları Bilgi Güvenliği Yönetim Sistemi'nin uygun şekilde işletilmesini sağlamakla ve kural ve prosedürlerine uymakla yükümlüdür.

Bu doküman ve ekleri sadece yollanan kişinin kullanımı içindir ve TEI'ye ait gizli ve/veya özel bilgi içerebilir. Herhangi bir izinsiz inceleme, kullanım veya dağıtım yasaktır. Eğer dokümanın yollandığı kişi değilseniz, lütfen gönderen kişiyle temasa geçin ve orjinal dokümanı tüm kopyaları ve varsa ekleri ile beraber yok edin. Ayrıca bu dokümandaki ve/veya eklerindeki bilgiler uluslararası ihracat kontrol kurallarına tabii olabilir. Bu tip bilgiler öncelikle ilgili idari onaylar alınmadan yayınlanamaz ve üçüncü kişilerle paylaşamaz.

HİZMETE ÖZEL

HİZMETE ÖZEL



Bilerek veya bilmeden, TEI'de bilgi güvenliğini ihlal eden veya ihlal edilmesine neden olanlar hakkında TEI SOP125 İnsan Kaynakları Disiplin Yönetmeliğinin ilgili maddeleri uygulanır.

TEI Bilgi Güvenliği Yönetim Sisteminin başarısı tüm çalışanlarımızın katkıları ile mümkündür. Bu nedenle tüm yönetici ve çalışanların Bilgi Güvenliği Yönetim Sistemi için azami katkılarını rica ederim.

Prof.Dr.Mahmut Faruk Akşit
Genel Müdür

İmza :

A handwritten signature in blue ink, consisting of a large, stylized 'M' followed by a horizontal line extending to the right.

Tarih : 11.09.2017

Bu doküman ve ekleri sadece yollanan kişinin kullanımı içindir ve TEI'ye ait gizli ve/veya özel bilgi içerebilir. Herhangi bir izinsiz inceleme, kullanım veya dağıtım yasaktır. Eğer dokümanın yollandığı kişi değilseniz, lütfen gönderen kişiyle temasa geçin ve orjinal dokümanı tüm kopyaları ve varsa ekleri ile beraber yok edin. Ayrıca bu dokümandaki ve/veya eklerindeki bilgiler uluslararası ihracat kontrol kurallarına tabii olabilir. Bu tip bilgiler öncelikle ilgili idari onaylar alınmadan yayınlanamaz ve üçüncü kişilerle paylaşılamaz.

HİZMETE ÖZEL