



TALİMAT

SİSTEM TEMİN, GELİŞTİRME VE BAKIM

TALİMAT NO	:	T.789.00
İLGİLİ PROSEDÜR	:	
İLGİLİ SÜREÇ	:	

İLGİLİ BÖLÜM	:	TÜM BÖLÜMLER
ISO 27001	:	EK – A.14
HAZIRLANMA TARİHİ	:	17.04.2018
SAYFA SAYISI	:	3

1. AMAÇ: KAYALAR (Vana, Batarya, Flex, Plastik) bünyesinde güvenliğin bilgi sistemlerinin dâhili bir parçası olmasını sağlamak için güvenlik gereksinimleri ve açıklarının takibi ile ilgili yöntem oluşturmaktır.

2. UYGULAMA

2.1. Bilgi Güvenliği Gereksinimleri Analizi ve Belirtimi

Bilgi güvenliği ile ilgili gereksinimler, yeni bilgi sistemleri gereksinimlerine veya var olan bilgi sistemlerinin iyileştirmeleri; İç Tetkikler, Risk Analizi çalışmaları, yasal şartlar, olay gözden geçirmeleri ve Uygulanabilirlik Bildirgelerinin kontrol edilmesi ile belirlenir.

Yeni bilgi sistemlerine ihtiyaç oluşması durumunda gerekli kabul şartları belirlenir. Yeni sistemin kabulü sırasında sözleşme ve şartlar kontrol edildikten sonra uygulamaya alınır. Bu kabulün kayıtları sözleşme ve fatura üzerinde yapılır.

2.2. Halka Açık Ağlardaki Uygulama Hizmetlerinin Güvenliğinin Sağlanması

Firmamıza ziyaret, çalışma vb. nedenlerden dolayı gelen misafirlerimiz mevcut kullanıcıların dışında farklı bir ağa sadece internet erişimi için bağlanabilirler. Buradaki hizmetlerin güvenliği **T.785 Erişim Kontrolü Talimatı** doğrultusunda gerçekleştirilmektedir. Bu hizmetin dışında firmamızda halka açık ağ üzerinde herhangi bir uygulama bulunmamaktadır.

2.3. Uygulama Hizmet İşlemlerinin Korunması

Firmamızda ERP, MEYER gibi uygulama hizmetleri sadece yetkilendirilen kullanıcılar tarafından kullanılmaktadır. Uygulama hizmetlerin güvenliği kullanıcılar tarafından **T.785 Erişim Kontrolü Talimatı** 2.6 Maddesi doğrultusunda gerçekleştirilmektedir.

Tüm kullanıcılar ilgili uygulama hizmetlerine kendilerine özel kullanıcı adı ve parolalar ile erişim sağlamaktadır. Bu uygulamaların veri tabanları sunucu üzerinde bulunmakta olup fiziksel sunucu sunucu odasında bulundurulmaktadır. Bu sunucuya yetkisiz kişilerin erişimini engellemek amacıyla alınan önlemler **T.786 Fiziksel Alanlar ve Çevresel Güvenlik Talimatı** doğrultusunda gerçekleştirilmektedir.

2.4. Güvenli Geliştirme Politikası

Güvenli geliştirme faaliyetleri hizmet ve sistemin gelişimi açısından önemli bir gerekliliktir. Öncelikli olarak güvenli geliştirme ortamları oluşturulmalı ve gerekli testler yapıldıktan sonra tüm kullanıcılara yayılması sağlanmalıdır. Bu doğrultuda geliştirme ortamları şu şekildedir;

- ⇒ Yazılımın geliştirilmeleri, yazılımcının kendi bilgisayarında
- ⇒ Sistemlerin geliştirmeleri, Bilgi İşlem Sorumlusu tarafından sanal makineler üzerinde yapılmalıdır.

Bu dokümanın aslı sanal ortamdır. Bu doküman gizlilik taşıyan bilgiler içermektedir. Sadece KAYALAR (Vana, Batarya, Flex, Plastik) dâhilinde kalmalı, güvenli bir yerde saklanmalı ve fotokopiyle çoğaltılmamalıdır.

REVİZYON NO	REVİZYON TARİHİ	YAYIMLAMA TARİHİ	HAZIRLAYAN	KONTROL	ONAY
00	-	18.04.2018	Kalite Sistem	BGYS Temsilcisi	Genel Müdür Yrd.

Bu geliştirmelere ilişkin tasarım çalışmaları esnasında gerekli güvenlik gereksinimleri belirlenmeli ve gerekli kontrollerin yapılması sağlanmalıdır. Tüm geliştiriciler açıklıklardan kaçınma, açıklıkları bulma ve düzeltme konusunda kendilerini geliştireceklerdir.

2.5. Sistem Değişiklik Kontrolü Prosedürleri

Sistem değişikliklerine ilişkin talepler mevcut kullanıcılar ya da Bilgi İşlem Sorumlusu talebi ile ortaya çıkabilir. Bu talepler **FR.331 Proje Talep Formu** doldurularak kayıt altına alınmaktadır. Gelen taleplere ilişkin Bilgi İşlem Sorumlusu tarafından Bilgi İşlem İş Takip Programı üzerinden faaliyet planlaması yapılmaktadır. Geliştirme sistemleri üzerinde yapılacak değişiklikler yalnızca Bilgi İşlem Sorumlusu tarafından sanal bir işletim sistemi üzerinde test edildikten sonra yapılmaktadır. Bilgi İşlem İş Takip Programı üzerinde sistem değişikliği ile ilgili yapılan çalışmalara ilişkin bilgiler kayıt altına alınmaktadır.

2.6. İşletim Platformu Değişikliklerinden Sonra Uygulamaların Teknik Gözden Geçirmesi

İşletim sistemi güncellemeleri geliştirme ortamlarına zarar vermemesi için Bilgi İşlem Sorumlusu tarafından sanal ortamda test edildikten sonra yapılmaktadır.

2.7. Yazılım Paketlerindeki Değişikliklerdeki Kısıtlamalar

Mevcut ve yeni kullanıcıların bilgisayarlarına **T.787 İşletim Güvenliği Talimatı** doğrultusunda Bilgi İşlem Bölümü tarafından ilgili yazılımlar yüklenir. Bu yazılımların dışında kullanıcılar, işletim sistemi üzerinde local user modunda olduklarından dolayı herhangi bir yazılım kurulum işlemi gerçekleştirememektedirler.

2.8. Güvenli Sistem Mühendisliği Prensipleri

Bilinen güvenlik açıkları tüm iş, veri, uygulama ve teknolojik sistemlerimiz üzerinde zarara yol açmaması için web ortamında (forumlar, sosyal medya, mail grupları vb.) araştırmalar yapılarak sürekli gözden geçirilir. Gerekli görülmesi durumunda yeni sistemlerin kullanımı için kaynaklar sağlanır. Güvenli sistem mühendisliği prensipleri **PLTK – 09 Güvenli Geliştirme Politikası** ile belirlenmiştir.

2.9. Güvenli Geliştirme Ortamı

Firmamız, tüm sistem ve yaşam döngüsünü kapsayan geliştirme ve bütünleştirme girişimleri için güvenli geliştirme ortamlarını kurmuş ve bunların uygun bir şekilde korunması amacıyla parola, fiziksel olarak kilitli bir mekanda tutma gibi önlemler almaktadır.

2.10. Dışarıdan Sağlanan Geliştirme

Dışarıdan sağlanan geliştirme faaliyetlerinde (sadece ERP) tedarikçi değerlendirmeleri Bilgi İşlem Bölümü koordinasyonunda ilgili kullanıcıların geri dönüşleri doğrultusunda gerçekleştirilmektedir. Bunların dışında geliştirme faaliyetleri ile ilgili olarak yıllık periyotlarda Bilgi İşlem Sorumlusu tarafından tedarikçi değerlendirme raporu hazırlanarak kayıt altına alınmaktadır.

2.11. Sistem Güvenlik Testi

Sistem güvenlik testleri Bilgi İşlem Bölümü tarafından geliştirme süresince kontrol edilir ve **FR.388 Sistem Güvenlik ve Kabul Test Kayıt Formu** ile kayıt altına alınır. Güvenlik işlevselliğini etkileyebilecek açıklıklar Yönetim Gözden Geçirme Toplantılarında görüşülür.

Bu dokümanın aslı sanal ortamdır. Bu doküman gizlilik taşıyan bilgiler içermektedir. Sadece KAYALAR (Vana, Batarya, Flex, Plastik) dâhilinde kalmalı, güvenli bir yerde saklanmalı ve fotokopiyle çoğaltılmamalıdır.

REVİZYON NO	REVİZYON TARİHİ	YAYIMLAMA TARİHİ	HAZIRLAYAN	KONTROL	ONAY
00	-	18.04.2018	Kalite Sistem	BGYS Temsilcisi	Genel Müdür Yrd.



TALİMAT

SİSTEM TEMİN, GELİŞTİRME VE BAKIM

2.12. Sistem Kabul Testi

Sistem testlerinde her kabul için **FR.388 Sistem Güvenlik ve Kabul Test Kayıt Formu** ile kriterler belirlenir. Kriterlere uygun olarak sistem kabulü gerçekleştirilir. Bu işlem yeni bir sistem yükseltmesi ihtiyacı olduğunda ya da yeni sürüm kabulünde yapılmaktadır. Sistem kabul testleri Bilgi İşlem Bölümü tarafından yapılmaktadır.

2.13. Test Verisinin Korunması

Test verisi Bilgi İşlem Bölümü tarafından **FR.388 Sistem Güvenlik ve Kabul Test Kayıt Formu** ile kayıt altına alınmakta ve yerel sunucular üzerinde saklanarak korunmaktadır.

3. SORUMLULUKLAR:

BGYS Temsilcisi: Halka açık ağlardaki uygulama hizmetlerinin güvenliği ile ilgili çalışmaların denetlenmesi, güvenli geliştirme faaliyetlerinin yürütülmesi, sistem değişikliği faaliyetlerinin yürütülmesi, sistem güvenlik ve kabul testlerinin yapılması ve ilgili testlere ilişkin verilerin korumasından sorumludur.

Kullanıcılar: Uygulama hizmetlerinin güvenliğine uygun davranmaktan, herhangi bir şekilde yazılım kurulumu yapmamaktan sorumludur.

Bu dokümanın aslı sanal ortamdadır. Bu doküman gizlilik taşıyan bilgiler içermektedir. Sadece KAYALAR (Vana, Batarya, Flex, Plastik) dâhilinde kalmalı, güvenli bir yerde saklanmalı ve fotokopiyle çoğaltılmamalıdır.

REVİZYON NO	REVİZYON TARİHİ	YAYIMLAMA TARİHİ	HAZIRLAYAN	KONTROL	ONAY
00	-	18.04.2018	Kalite Sistem	BGYS Temsilcisi	Genel Müdür Yrd.