KAS	***TALİMAT***
	İŞLETİM GÜVENLİĞİ

TALİMAT NO	:	***T.787.01***
İLGİLİ PROSEDÜR	:	
İLGİLİ SÜREÇ	:	

İLGİLİ BÖLÜM	:	***TÜM BÖLÜMLER***
ISO 27001	:	***EK – A.12***
HAZIRLANMA TARİHİ	:	***10.04.2018***
SAYFA SAYISI	:	***4***

***1. AMAÇ**: KAYALAR (Vana, Batarya, Flex, Plastik) bünyesindeki bilgi işleme olanaklarının doğru ve güvenli işletimini sağlamak için yöntemlerin oluşturulmasıdır.*

2. UYGULAMA

2.1. Yazılı İşletim Dokümanları

*Firmamızda kullanılmakta olan yedekleme, bakım ve diğer talimatlar **P.01 Dokümante Edilmiş Bilginin Sağlanması Prosedürü'** ne uygun şekilde kullanıcılara sağlanmaktadır. Tüm yazılı işletim dokümanları personelin rahatlıkla ulaşabileceği şekilde ortak ağda yer alan bir klasör içerisinde bulundurulmaktadır.*

2.2. Değişiklik Yönetimi

Bilgi güvenliğini etkileyen, bilgi işleme olanakları ve sistemlerdeki değişiklikler aşağıdaki gibi yönetilmektedir;

2.2.1. İşletim Sistemi Değişikliği

- ⇒ *İşletim sistemlerinde versiyon ya da herhangi bir değişiklik yapılması düşünüldüğünde öncelikle sanal bir makinede yeni sistem BGYS Temsilcisi tarafından test edilmektedir.*
- ⇒ *Test aşamasında sanal makine üzerinde tüm yazılım geliştirme, veri tabanı ve ofis yazılımları kurularak gerekli testler yapılmaktadır.*
- ⇒ *Yapılan test sonuçları BGYS Temsilcisi tarafından bir rapor ile kayıt altına alınmakta ve Üst Yönetim bilgisine sunulmaktadır. Üst Yönetimin vereceği karar doğrultusunda gerekli uygulamalar gerçekleştirilmektedir.*

2.2.2. Yazılım Geliştirme Ortamı Değişikliği

*Kullanıcılar yazılım geliştirme ortamlarının versiyon değişikliği ile ilgili taleplerini **FR.331 Proje Talep Formu** ile Bilgi İşlem bölümüne iletmektedir. Bu talepler BGYS Temsilcisi tarafından ön değerlendirmeye tabi tutularak Üst Yönetim onayına sunulmaktadır. Üst Yönetimin vereceği karar doğrultusunda gerekli uygulamalar gerçekleştirilmektedir.*

2.2.3. Veri tabanı Değişikliği

Firmamızda Mysql ve Mssql veri tabanları kullanılmaktadır. Web tabanlı projelerde hangi veri tabanının kullanılacağına BGYS Temsilcisi tarafından karar verilmektedir. Masaüstü uygulamalarda veri tabanı kullanımı ile ilgili kararlar Üst Yönetimin vereceği karar doğrultusunda gerçekleştirilmektedir.

2.2.4. Diğer Değişiklikler

BGYS'yi etkileyebilecek diğer değişiklikler (fiziksel taşıma vb.) Üst Yönetim kararı ile yapılır ve değişiklik sonrası BGYS Temsilcisi tarafından BGYS şartlarına uyumu değerlendirilir.

REVİZYON NO	*REVİZYON TARİHİ*	*YAYIMLAMA TARİHİ*	*HAZIRLAYAN*	*KONTROL*	*ONAY*
01	*27.03.2019*	*11.04.2018*	*Kalite Sistem*	*BGYS Temsilcisi*	*Genel Müdür Yrd.*

2.3. Kapasite Yönetimi

BGYS Temsilcisi tarafından sistem performansını etkileyebilecek durumları izlemek ve ayarlamak amacıyla mevcut sunuculara ilişkin; ram, işlemci, hard disk kullanım oranı, network bağdaştırıcısının durumu vb. veriler izlenmektedir. Sistem performansını etkileyebilecek durumlar tespit edilmesi durumunda BGYS Temsilcisi tarafından ***T.559 Bilgi İşlem Talimatı*** *doğrultusunda müdahale edilmektedir.*

2.4. Geliştirme, Test ve İşletim Ortamlarının Birbirinden Ayrılması

Geliştirme, test ve işletim ortamlarındaki değişiklikler Bilgi İşlem personellerinin bilgisayarlarında yapılmaktadır. Son kontroller tamamlandıktan sonra sunucuya yüklenmektedir.

2.5. Kötücül Yazılımlara Karşı Kontroller

Firma içerisinde windows işletim sistemleri üzerinde "securtiy end poing (uç nokta güvenlik) sistemi" kullanılmaktadır. Firmamızda Linux işletim sistemi kullanılan çok sayıda bilgisayar bulunmakta olup bu bilgisayarlarda virüs içeren kötücül yazılımlar çalışmamaktadır. Dolayısıyla Linux işletim sistemleri kullanılan bilgisayarlarda bu tür virüs programları kullanılmamaktadır. E-posta ile gelen oltalama saldırılarına karşın kullanıcıya farkındalık eğitimleri verilmektedir.

2.6. Bilgi Yedekleme

Kayalar, yedek alma işlemleri ile ilgili olarak ***PLTK – 07 Yedekleme Politikası*** *hazırlamış ve uygulamaktadır. Bilgi, yazılım ve sistem imajlarının yedekleme kopyalarının alınması işlemleri* ***T.03 Yedekleme Talimatı*** *doğrultusunda gerçekleştirilmektedir.*

2.7. Olay Kaydetme

- ⇒ *Firma içerisinde olay kaydet işlemini* ***SIEM (Security Information and Event Management)*** *programı yapmaktadır.*
- ⇒ *İşletim sistemlerinin üretmiş olduğunu anlık olayların bildirimleri kendilerine yüklü bulunan bir agent yazılımı ile SIEM ürününe aktarılmakta ve raporlanabilmektedir.*
- ⇒ *Günlük, haftalık, aylık ve yıllık raporlar alınabilmekte olaylar analiz edilebilmektedir. Özel durumlar için kurallar yazılabilmekte ve e-posta ile bildirim yapılabilmektedir.*
- ⇒ *ERP yazılımları olay kayıtları veri tabanında tutulmaktadır.*
- ⇒ *Arşiv, Güvenlik, Depo vb. alanlarda kamera ile sürekli izlenmektedir. Buralarda bilgi güvenliğini tehlikeye atacak durumlar tutanaklar ile kayıt altına alınmaktadır.*

Yukarıda bahsedilen alanlarda herhangi bir kural dışı durum oluşursa ***T.791 Bilgi Güvenliği İhlal Olayı Yönetimi Talimatı'*** *na uygun olarak çalışmalar gerçekleştirilmektedir.*

2.8. Kayıt Bilgisinin Korunması

Kullanıcılar kayıtlarını ağ üzerindeki klasörlerde tutarlar. Ağ üzerindeki kayıtların korunması ***T.785 Erişim Kontrolü Talimatı*** *ve* ***T.03 Yedekleme Talimatı*** *doğrultusunda gerçekleştirilmektedir.*

2.9. Yönetici ve Operatör Kayıtları

Kurum içerisinde bulunan Saldırı tespit sistem üretmiş olduğu logları wazuh agent aracılığı ile SIEM ürününe gönderir. Aynı zamanda sunucularda yüklü olan bu agent sistem konuları ile ilgili üzerinde yapılan işlemlerin bilgilerini SIEM ürününe gönderip kayıt edilmesini sağlamaktadır. Bilgi işlem personelinin sunucularda yaptıkları başarılı başarısız oturumları, uzak bağlantı işlemleri, kayıt altında alınmaktadır. Bu ürün dışarıdan destek alınan bir firma tarafından kontrol edilmektedir. Bilgi işlem personelleri bu ürün üzerinde veriyi bozabilecek herhangi bir işlem yapamamaktadır.

2.10. Saat Senkronizasyonu

Firmamızda kullanılmakta olan tüm bilgisayarlar NTP server üzerinden eşitlenmektedir.

2.11. İşletimsel Sistemler Üzerine Yazılım Kurulumu

Yeni kullanıcılar, işletimsel sistemler üzerinde yazılım kurulum taleplerini e-posta ile destek@kas.com.tr adresine iletmektedir. Gelen talepler Bilgi İşlem Bölümü tarafından değerlendirilerek gerek görülmesi durumunda yazılım kurulumu işlemi gerçekleştirilmektedir.

Mevcut kullanıcılar ihtiyaç duydukları yazılımlara ilişkin taleplerini ***FR.337 - Bilgisayar-Donanım-Yazılım Talep Formu*** *aracılığıyla Bilgi İşlem Bölümüne iletirler. Talep edilen yazılıma ilişkin gerekli onaylar alındıktan sonra Bilgi İşlem Sorumlusu tarafından yazılımın temin edilmesi sağlanır.*

Oluşturulan her kullanıcı standart user olduğundan program kurulumu yapamamaktadırlar. Bilgi işlem personelinin özel durumlarda uygun gördüğü bazı kullanıcılar local admin seviyesinde çalışabilmektedir.

Bu durumda olan kullanıcıların bilgisayarlarında yaptıkları işlemlerin bilgileri bilgisayarlarında yüklü olan wazuh agent sayesinde sistem yöneticisi e-mail ile bilgilendirilmektedir.

2.12. Teknik Açıklıkların Yönetimi

Kullanılmakta olan bilgi sistemlerinin teknik açıklıklarına dair bilgiler, tedarikçi destek siteleri, www.usom.gov.tr, www.bilgiguvenligi.gov.tr adreslerinden BGYS Temsilcisi tarafından takip edilmektedir. Bu tür açıklıklara karşı zafiyeti değerlendirilerek ve ilgili riskin ele alınması için uygun tedbirler alınmaktadır.

- ⇒ *Tedarikçi destek sitelerinden teknik açıklıklara ilişkin elde edilen veriler mevcut kullanıcılarımızın bilgilendirilmesi amacıyla e-mail yoluyla tüm kullanıcılara gönderilmektedir.*
- ⇒ *www.usom.gov.tr tarafından yayımlanan .txt zararlı alan adlarına ilişkin bilgiler belirli zaman aralıkları ile otomatik olarak güvenlik duvarımız ile senkronize edilmektedir.*

2.13. Yazılım Kurulumu Kısıtlamaları

Kullanıcıların bilgisayarlarına yazılım yükleme ve kaldırma işlemleri, sadece bilgi işlem personeli veya onun gözetiminde ayrıcalıklı kullanıcı haklarına sahip kişi/kişiler yapılabilir. Ayrıcalıklı kullanıcılar hariç birçok kullanıcı local user modda olduğu için bilgisayarlarına herhangi bir yazılım kurma işlemi yapamamaktadırlar.

2.14. Bilgi Sistemleri Tetkik Kontrolleri

Bilgi sistemlerinin tetkiki iş proseslerinde herhangi bir kesinti oluşturmamaktadır.

3. SORUMLULUKLAR:

BGYS Temsilcisi: *İşletim sistemi, yazılım geliştirme ortamı, veri tabanı vb. değişikliklerin yönetimi, sunuculara ilişkin kapasite yönetimi, kötücül yazılımlara karşı gerekli kontrollerin gerçekleştirilmesi, olayların izlenmesi ve gerekli müdahalelerin yapılması, saat senkronizasyonu işlemlerinin yürütülmesi, teknik açıklıkların yönetiminden sorumludur.*

Kullanıcılar: *Yazılım geliştirme ortamlarının geliştirilmesine yönelik taleplerde bulunmaktan, bilgi güvenliğini ihlal edecek olaylardan kaçınmaktan, yaptıkları çalışmalara ilişkin kayıtları ağ üzerinde saklamaktan, işletimsel sistemler üzerine izinsiz yazılım kurulumu yapmamaktan sorumludur.*