KAS	***TALİMAT***
	İŞ SÜREKLİLİĞİ YÖNETİMİNİN BİLGİ GÜVENLİĞİ HUSUSLARI

TALİMAT NO	:	***T.792.02***
İLGİLİ PROSEDÜR	:	
İLGİLİ SÜREÇ	:	

İLGİLİ BÖLÜM	:	***TÜM BÖLÜMLER***
ISO 27001	:	***EK – A.17***
HAZIRLANMA TARİHİ	:	***27.04.2018***
SAYFA SAYISI	:	***6***

***1. AMAÇ**: KAYALAR (Vana, Batarya, Flex, Plastik) bilgi güvenliği sistemin işleyişine ait kayıtların tanımlanması, tasnifi, dosyalanması, muhafaza edilmesi, ulaşılabilirliğinin sağlanması ve imhası için uygulanacak yöntemlerin ve sorumlulukların belirlenmesi, bu kapsamda iş idaresinin devamlılığı için İş Sürekliliği Planının hazırlanmasıdır.*

2. UYGULAMA

2.1. Bilgi Güvenliği Sürekliliği

2.1.1. Bilgi Güvenliği Sürekliliğinin Planlanması

Aşağıdaki etkenlere bağlı olarak Bilgi Güvenliği Sisteminin sürekliliği olumsuz etkilenebilir;

Doğal Afetler (deprem, Sel), Yangın, Adli Olaylar, Donanım arızası/kaybı, Ana Ağ Anahtarı, Sunucular, Yazılımsal Hatalar, Yazılım güncellemesinden kaynaklanan, Yazılım hatasından kaynaklanan, Altyapı kaybı, Ana iletişim hatlarında meydana gelen arızalar, Ara iletişim hatlarında meydana gelen arızalar, Elektrik şebekesinden kaynaklanan arızalar, Sistem Çökmesi, Kritik Personel Kaybı vb.

İş sürekliliğinde kesintiye sebep olabilecek durumlar ve alınacak önlemler aşağıda belirtilmiştir;

İş sürekliliği Kesintileri	***Olasılık***	***Alınabilecek Önlemler***	***Tehlike/Etki***	***Aksiyon***
Verilerin silinmesi, bozulması ya da hasar görmesi	*1*	*Otomatik yedekleme sistemleri ile belirli periyotlarda (günlük, haftalık, aylık) düzenli olarak verinin korunmasını sağlar*	*Verilerin zarar görmesi sistemin işleyişine direk olumsuz etki eder. Geçici ya da sürekli sisteme zarar verir.*	*Sistemde en kritik kesintilerdendir. Güncel yedek, veri kaybı işleminden sonra en kısa sürede, ilgili sistem ya da ana bilgisayara indirilip, veri güvenliği kontrol edilmelidir.*
Elektrik Kesintisi	*2*	*UPS güç kaynağı ve Jeneratör ile sistemin kapanmaması*	*Kısa süreli kesintilerde problem teşkil etmez.*	*UPS, sistemin kapanmasına ve her türlü elektrik akımına karşı koruma sağlar.*
İnternetin Kesilmesi	*3*	*Yedekleme amacı ile başka bir internet hattı bulundurmak.*	*İnternetin kesilmesi sonucunda dış network tamamen devre dışı kalır.*	*Ana hattın kesilmesi durumunda yedek hat otomatik devreye girecektir. Bu sayede internet kesintisinden etkilenme minimum seviyede olacaktır.*

Networkün Kesilmesi	*3*	*Yedek donanım cihazları ve kabloların bulundurulması.*	*Şirket içinde veri alışverişi sağlanamaz. Erişim kopar.*	*Arıza tespitinden sonra parçaların otomatik olarak değiştirilmesi sağlanacaktır.*
Kullanıcıların bilgisayarlarının arızalanması	*1*	*Yedekte kullanılmayan bir pc bulundurulup, her hangi bir arıza durumunda ilgili kullanıcıya devredilmesi sağlanır.*	*Kullanıcının kısa sürelide olsa işinin aksaması, veri iletişiminin kesilmesi anlamına gelmektedir.*	*Zarar gören kullanıcı bilgisayarının verileri güvenli bir şekilde serverda bulunduğundan yapılan işler serverdan çekilip çalışmalara devam edilmektedir.*
Dışarıdan gelen güvenlik saldırısı (Hacker Attack)	*2*	*Şirket içinde kullanılan sistemdeki güvenlik duvarı yazılım ve donanım ile korunmalıdır.*	*Şirketlerde olmaması gereken kriterlerdendir. Güvenlik saldırısı sonucunda verilerin güvenliği ve şirket çalışanlarının bilgi güvenliği tehlikeye girer.*	*Dışarıdan herhangi bir network saldırısı ya da networkü meşgul eden spam saldırısı geldiğinde network cihazları tarafından tespit edilip içeriye girmesi engellenir.*
Sistemdeki network cihazlarının fiziksel olarak arızalanması	*3*	*Arızalanan network cihazlarının en kısa sürede yenilenmesi ya da arızanın giderilmesi sağlanır.*	*Şirket içi networkü yada şirket dışı networkünün göçmesi anlamına gelmektedir.*	*Arızalanan network ürününün en kısa sürede yenisinin temin edilmesi ya da arıza yapan ürünün tamirinin yapılması.*
Şirket içindeki network kablolarının arızalanması	*2*	*Kullanıcı öncelikle kendi network kablosunu kontrol eder.*	*Erişim koptu anda şirket için iletişim kopukluğu yaşanır.*	*Arızalanan kablo yenisi ile değiştirilir.*
Yangın, deprem, su baskını gibi doğal afetler	*2*	*Bilgi işlem odasının yangın güvenliği için uygun söndürme sisteminin yer alması, fiziksel olarak bina güvenliği ve sağlamlığı sağlanmalı.*	*Yangın, deprem, sel felaketi gibi doğal afetler sonucunda sistem kısmen ya da tamamen devre dışı kalabilir. Olma ihtimali düşükte olsa kuvvetli zararları olabilir.*	*Şirket içinde gerekli söndürme cihazlarının yer alması ve müdahale yöntemleri, yangında öncelikli kurtarılacak olan sistemlerin belirlenmesi herhangi bir felaket senaryosu anında sistemin devamlılığın en kısa sürede sağlanması.*
Sunucuların arızalanması	*4*	*Yedek sunucunun bulundurulması*	*Şirket içi ve dışı veri alışverişi sağlanamaz.*	*Şirket içinde o sunucudan bir tane daha bulundurmak gerekir.*

Tablo: *İş Sürekliliği Planı*

Olasılık Değeri

- ⇒ ***1: Düşük***
- ⇒ ***2: Orta***
- ⇒ ***3: Yüksek***
- ⇒ ***4: Çok Yüksek*** *olarak değerlendirilmiştir.*

İş sürekliliğinin sağlanması ile ilgili yapılacak çalışmaların koordinasyonu (dış kuruluşlardan alınacak yardım ve hizmetler, kurum içi görevlendirmeler vb.) Bilgi Güvenliği Yönetim Sistemi Temsilcisi tarafından gerçekleştirilir.

Bu olumsuz durumların herhangi birinin gerçekleşmesi beklenmeden iş sürekliliğin sağlanması için önceden yapılması gereken çalışmalar ve alınması gereken önlemler aşağıda belirtilmiştir;

- ⇒ *Servis kesintisine yol açabilecek tüm durumlar için ilk olarak yapılması gereken düzenli bir biçimde sistemdeki tüm kritik yazılım ve sunucular yedeklenecektir.*
- ⇒ *Hangi sistemlerin ne ölçüde kimin tarafından hangi sıklıkla nereye ve hangi yöntemle yedeğinin alınacağı belirlenmeli, yedekleme işlemi buna göre yapılmalı ve alınan yedeklerin sağlamlığı düzenli olarak kontrol edilmelidir.*
- ⇒ *Donanım arızalarına karşın kritik sistemlerin donanım olarak yedekleri tutulmaktadır.*
- ⇒ *Elektrik kesintileri için UPS destek sistemi ve Jeneratör kurulmuştur.*
- ⇒ *Herhangi bir felaket sonucunda kullanılan binanın hasar görmesi durumunda başka lokasyona alınan yedekler kullanılacaktır.*
- ⇒ *Acil bir durumda yapılacak işler ve sorumlular belirlenmiştir.*

Firmanın BİM Serverlarının bulunduğu ortamda ve firma içinde oluşabilecek olağanüstü bir durumda Bilgi işlem sunucularında bulunan bilgilerin zarar görmemesi için önlem alınır.

Sistemin hiçbir şekilde çalışmaması ve İş Süreklilik Planında belirtilen önlemlerin kullanılamaması halinde, iş sürekliliği ve kayıtların tutulması için işlemler manuel şekilde yürütülecektir.

- ⇒ *Ticari kayıtlar ile eşyaya ilişkin ERP de tutulması gereken kayıtlar kâğıt ortamında tutulacaktır.*
- ⇒ *Finans ve muhasebe birimlerince eşya ile ilgili sisteme aktarılamayan tüm kâğıt ortamında ki veriler ayrı dosyalanacak, ERP'nin çalışması ile birlikte sisteme kaydedilecektir.*
- ⇒ *Satınalma, lojistik, depo, ihracat, üretim, kalite birimlerinde tutulan kayıtlar için "üretim fişleri, kalite formları, satınalma formları, depo fişleri" tutulacak ve ERP'ye girişleri için dosyalanacaktır. ERP'nin tekrar aktif hale getirilmesi ile birlikte sisteme aktarılacaktır.*
- ⇒ *Kayıtların tutulması esnasında Bölüm Amirleri bizzat kâğıt ortamındaki evrakların tutulup tutulmadığını denetleyecek, ,ihtiyaca göre kayıtların tutulması için yeni formlar oluşturulacaktır.*
- ⇒ *Tüm kayıtlar ERP'nin yeniden devreye sokulması ile birlikte 5 iş günü içerisinde sisteme aktarılacak olup, olağan dışı durumlar için ek süre istenebilecektir.*

2.1.1.1. İş Etki Analizi

İş Etki Analizi, sunucularda oluşabilecek herhangi bir sorununu firma içerisindeki işleyişe etkisini belirlemektedir. Örneğin; ERP veritabanında oluşabilecek bir sorunda ya da barındırıldığı sunucuda oluşabilecek bir sorunda ERP programını kullanan bütün bölümlerin çalışamayacağı hali ile iş kaybı yaşanacağı öngörülmektedir. Bu ve benzeri durumların sürelerini olabildiğinde kısaltmak için yapılacak çalışmayı kapsamaktadır. Aşağıdaki tablolarda yer alan Kurtarma Seviyeleri şu anlamı ifade etmektedir.

⇒ ***1. Öncelik:*** *Kritik Etki "Derhal Müdahale edilmeli"*
⇒ ***2. Öncelik:*** *Yüksek Etki "Müdahale edilmeli"*
⇒ ***3. Öncelik:*** *Orta Etki "Müdahale edilmeli aciliyet durumu yok"*
⇒ ***4.Öncelik:*** *Düşük Etki "Aciliyet durumu yok" öncelik sırası gözetilerek müdahale edilmeli.*

a. Etki Alanı

Sistem	Etki alanı	Kurtarma seviyesi
DbServer	ERP programını kullanan herkesi kapsar.	1.Öncelikli
Terminal Server	ERP Programını kullanan herkesi kapsar.	1.Öncelikli
Fileserver	Tüm kullanıcılara dosya paylaşım hizmeti veren sunucudur.	2.Öncelikli
Firewall (Pfsense)	Bütün kullanıcıların networkte dolaşmasını ve internete çıkmasını sağlar.	1.Öncelikli
Meyer	İK bölümüne hizmet veren sunucu	2.Öncelikli
Redmine	Bigli işlem bölümüne iş takip hizmeti veren sunucu	3.Öncelikli
Nas Server	Yedekleme ünitesi	2.Öncelikli

Tablo:*Etki tablosu*

b. Felaket Kurtarma Süresi / Recovery Time Objective (RTO)

İşletmenin çalışamaz durumda bulunan bir süreci tekrar çalışır duruma getirmek için öngördüğü süredir.

Sunucu	Kabul Edilebilir Minimum Kurtarma Süresi	Kesintiden Etkilenecek Kişi Sayısı	Kurtarma Seviyesi (Müdahale Önceliği)
Harmonydb	3 saat	100 - 150	1.Öncelikli
Terminal Server	3 saat	100 -150	1.Öncelikli
Meyer ik	3 Saat	1-5	2.Öncelikli
Fileserver	3 Saat	30-50	2.Öncelikli
Nas Server	3 Saat	1	3.Öncelikli
Bilgisayarlar	3 Saat	1	4.Öncelikli
Redmin	3 saat	1	4.Öncelikli

Tablo:*RTO tablosu*

c. Felaket Kurtarma Noktası / Recovery Point Objective (RPO)

Bir sürecin kesintiye uğradığı zaman noktası ile sürece tekrar işlerlik kazandırıldığı zaman noktası arasında geçen süredeki azami kayıp.

Sunucu	Kabul edilebilir Maksimum Geri Yükleme Süresi	Kesintiden Etkilenecek Kişi Sayısı	Risk Seviyesi (Müdahale Önceliği)
Harmonydb	1 Gün – 24 Saat	100-150	1.Öncelikli
Terminal Server	1 Gün – 24 Saat	100-150	1.Öncelikli
Meyer ik	1 Gün – 24 Saat	2	3.Öncelikli

Fileserver	*1 Gün -- 24Saat*	*100*	*2.Öncelikli*
Nas Server	*1 Gün – 24 Saat*	*1*	*3.Öncelikli*
Bilgisayarlar	*1 Gün – 24 Saat*	*1*	*4.Öncelikli*

Tablo:*RPO tablosu*

FELAKET KURTARMA YÖNETİM EKİBİ			
AD SOYAD	***UNVANI***	***İLETİŞİM***	***SORUMLULUK***
Mehmet YALÇIN	*Bilişim Sistem Yöneticisi*	*507 088 57 85*	*Kriz Yönetim Ekip Lideri Sunucu Sistemleri Network Sistemleri Veri yedekleme ve depolama Güvenlik Sistemi (FW)*
Ozan YILDIZ	*Bilgi işlem sorumlusu*	*549 803 27 12*	*Kriz Yönetim Ekip Lideri Yrd. Kullanıcı Destek ve Kontrol*
Fatih BÖLÜKBAŞ	*Veritabanı Yöneticisi*	*543 801 71 02*	*Erp Harmony Programı Db Admin*
Ertuğrul DUMAN	*Veritabanı Yöneticisi*	*533 261 42 15*	*Erp Harmony ik modülü*
Vedat KAMER	*Sistem Yöneticisi*	*555 311 78 38*	*Pfsense Fw Proxmox Sunucu FreeNas Sunucu*
Önder NARMAN	*Destek Ekibi*	*532 420 59 54*	*Mail Sunucuları yönetimi*
MEYER	*Sistem destek sorumlusu*	*216 999 24 99*	*Meyer Firması Parmak okutma cihazları*

d. Krokiler ve Genel Bilgi

Talimat kapsamında hazırlanan planlarda;

Fabrika yerleşkesi, bulunduğu adres yer alacaktır. Olası durumlarda, dış çevre tesisler, güvenlik birimleri, diğer acil durum müdahale birimlerinin, konum ve irtibat bilgileri yer almalıdır. Bu kapsamda, emniyet, jandarma, ambulans, itfaiye gibi birimler dikkate alınmalıdır.

Firmanın, bilgi güvenliği açısından kritik noktaları ve odaları, iş sürekliliğinin devamı için araç gereç ve donanımların bulunduğu alanlar, jeneratör ve güç kaynağı gibi yardımcı araçlar, server odası vb diğer noktalar krokide belirtilir.
Krokiler İş Sürekliliği Planında belirtilen kritik ve müdahale edilmesi gereken noktalar düşünülerek hazırlanır. Krokilerde kat bilgisi, merdivenler, ilgili oda ve alanlar belirlenerek yazılır. Hareket yönleri de açık olarak görülmelidir.

Fabrika bünyesinde ortalama olarak çalışan personel sayıları, hâlihazırda çalışan Bilgi Güvenliği personeli sayıları belirlenmelidir. Acil durumlarda, daha fazla personele ihtiyaç durulması halinde çalışan personellerden destek alınması için kişiler belirlenecektir. Bu yönde destek alınacak personel bulunmaması halinde her departman sorumlusu görevli kılınacaktır.

2.1.2. Bilgi Güvenliği Sürekliliğinin Uygulanması

*Bilgi Güvenliği Sürekliliği uygulamalarına ilişkin çalışmalar yukarıda yer alan **Tablo: İş Sürekliliği Planı** doğrultusunda yapılacak olan faaliyetler ile belirlenmekte ve yıllık periyotlarda uygulamaya alınmaktadır.*

2.1.3. Bilgi Güvenliği Sürekliliğinin Doğrulanması, Gözden Geçirilmesi ve Değerlendirilmesi

Yapılan kontrollere ilişkin değerlendirmeler Bilgi Güvenliği Yönetim Sistemi Temsilcisi tarafından raporlandırılmakta ve Yönetimin Gözden Geçirme Toplantıları ile gözden geçirilmekte ve değerlendirilmektedir.

2.2. Yedek Fazlalıklar

2.2.1. Bilgi İşleme Olanaklarının Erişilebilirliği

*Masaüstü bilgisayar, dizüstü bilgisayar ve personelin iş sürekliliği sağlaması için gerekli olan telefon vb. cihazlar yedekli olarak bulundurulmaktadır. Yedek fazlalıklar **FR.307 Makine-Kritik Ekipman Listesi**'nde belirlenmiştir.*

3. SORUMLULUKLAR:

BGYS Temsilcisi: *İş sürekliliğinin sağlanması ile ilgili yapılacak çalışmaların koordinasyonu, bilgi güvenliği sürekliliğinin doğrulanması, gözden geçirilmesi ve değerlendirilmesine yönelik kontrolleri raporlandırmak, yedek fazlalıklara ilişkin Makine-Kritik Ekipman Listeleri hazırlamak ve güncellemekten, sorumludur.*