ZER YAĞ

BG-PT-01

Bilgi Güvenliği Politikası

İlk Yayın Tarihi: 15.05.2015

HİZMETE ÖZEL

ISO REFERANSLARI

ISO27001 Ref. Madde No
5.2 Politika

DEĞİŞİKLİK KAYITLARI

Rev. No	Tarih	Hazırlayan	Değişiklik Nedeni /Sayfa No	Onaylayan	İmza
0	15.05.2015	Tuncay KAHRAMAN	İlk Kayıt	Hüsamettin SELÇUK	
1	15.05.2015	Tuncay KAHRAMAN	Tuncay KAHRAMAN	Hüsamettin SELÇUK	
2	15.05.2015	Tuncay KAHRAMAN	Tuncay KAHRAMAN	Hüsamettin SELÇUK	
3	18.10.2021	Tuncay KAHRAMAN	Tuncay KAHRAMAN	Hüsamettin SELÇUK	

İçindekiler

KISALTMALAR TABLOSU 5
1. AMAÇ 7
2. KAPSAM 7

3. SORUMLULUK VE YETKİ 8
4. BİLGİ GÜVENLİĞİ NEDİR ? 8
5. BİLGİ GÜVENLİĞİ HEDEFLERİ VE AMAÇLARI 8
6. BILGI GÜVENLIĞININ YAPISI VE ORGANIZASYONU 9
6.1. BGYS Takımı ve Yetkileri 9
6.2 BGYS Komisyonu 9
6.3 Organizasyon Şeması 10
7. RISK YÖNETIM ÇERÇEVESI 11
7.1.Risk Analizi ve Yönetim Stratejisi 11
7.2. SOA – Uygulanabilirlik Bildirgesi 12
8. ROL VE SORUMLULUKLAR 12
9. BİLGİ HASSASİYETİ VE RİSKLER 14
9.1. Bilgi Varlıklarımız 14
9.2.Varlık Sınıflandırılması 14
9.3.Kritik varlıklar 14
10. BGYS YGG (BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ GÖZDEN GEÇİRME) TOPLANTILARI 15
11. BİLGİ GÜVENLİĞİ POLİTİKASI 15
11.1 Genel Esaslar 15
11.2 Temel BGYS Prensipleri 16
11.3 Uyulması Gereken BGYS Kuralları 16
12. YAPTIRIM 20
13. YÖNETİMİN SORUMLULUĞU 20
13.1. Yönetimin Taahhüdü 20
14. YÖNETİMİN GÖZDEN GEÇİRMESİ 21
15. ÜÇÜNCÜ ŞAHISLARIN BİLGİYE ERİŞİMİ 21
16. DIŞ KAYNAK SAĞLANMASI 21
17. BİLGİ GÜVENLİĞİ POLİTİKA DOKÜMANI GÜNCELLENMESİ VE GÖZDEN GEÇİRİLMESİ 21
18. BİLGİ GÜVENLİĞİ İÇ DENETİMLERİ 22

19. SÜREKLİ İYİLEŞTİRME VE DÜZELTİCİ FAALİYETLER 22
20. İLGİLİ DÖKÜMANLAR 22
- Tüm BGYS Dokümantasyonu 22

KISALTMALAR TABLOSU

a. **BGYS**: Bilgi Güvenliği Yönetim Sistemi
b. **Varlık** : Kuruluş İçin Değeri Olan Herşey
c. **Kullanılabilirlik** : Yetkili bir varlık tarafından talep edildiğinde erişilebilir kullanılabilir olma özelliğidir.
d. **BTHYS**: Bilgi Teknolojileri Hizmet Yönetim Standardı
e. **Bütünlük** : Varlıkların doğruluğunu ve tamlığını koruma özelliği
f. **Risk Yönetimi**: Bilgi güvenliği risklerinin analizi, değerlendirilmesi, işlenmesi ve sürekli iyileştirilmesi amacıyla yürütülen yönetimsel faaliyetler.
g. **Risk Analizi**: Tehdit ve iş etkisinin çarpımı olan risk puanının bulunması amacıyla her bir bilgi varlığı için zayıflıkların, tehditlerin, iş etkilerinin bulunması ve hesaplanması çalışması.
h. **Risk Değerlendirme**: Risk analizi sonucunda bulunan değerlerin yorumlanması ve derecelendirilmesi.
i. **Risk İşleme**: Risk değerlendirme sonuçlarına bağlı olarak kaçınma, kabul, kontrol, transfer seçeneklerinden birinin seçilmesi ve uygulama planı.
j. **Artık Risk**: Risklerin işlemesinden sonra kalan riske denir.
k. **Risk Derecelendirmesi:** Riskin önemini tayin etmek amacıyla tahmin edilen riskin, verilen risk kriterleri ile karşılaştırılması sürecidir.
l. **Riskin Kabulü/Kabul edilebilir Risk**: Bir riski kabul etme kararı. Bir riskin zararını (negatif sonuçlarını) kabullenme.
m. **Bilgi Güvenliği**: Bilginin gizliliği, bütünlüğü ve erişilebilirliğinin korunmasıdır. Ek olarak, doğruluk, açıklanabilirlik, inkâr edememe ve güvenilirlik gibi diğer özellikleri de kapsar.
n. **Bilgi Güvenliği İhlal Olayı**: İş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olayı.
o. **Bilgi Güvenliği Yönetim Sistemi (BGYS)** : Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır. Yönetim sistemi, kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, prosedürleri, prosesleri ve kaynakları içerir.
p. **Uygulanabilirlik Bildirgesi (SOA-Statement of Applicability**): Kuruluşun BGYS ile ilgili ve uygulanabilir kontrol amaçlarını ve kontrolleri açıklayan dokümante edilmiş bildirgedir. Kontrol amaçları ve kontroller, risk değerlendirme ve risk işleme proseslerinin sonuçları ve çıkarımlarını, yasal ve düzenleyici gereksinimleri, anlaşma yükümlülüklerini ve kuruluşun bilgi güvenliği için iş gereksinimlerini temel alır.
q. **Etki**: İş hedeflerinin başarısını etkileyen değişim.
r. **Bilgi Güvenliği Riski**: Açıklıklardan fayda sağlamak suretiyle kuruluşa zarar verebilecek varlık ya da varlık gruplarının potansiyel tehdididir. Bir olayın ve sonucunun olasılığının

kombinasyon koşulları olarak ölçülür.

s. **Riskten Kaçınma**: Riski oluşturan durumdan kaçınma kararıdır.
t. **Risk İletimi:** Karar verici veya diğer ortaklar arasında risk hakkındaki bilgiyi paylaşım ya da değişimdir.
u. **Riski Belirleme**: Riski oluşturan öğelerin ortaya çıkartılması, tasnif edilmesi ve özelliklerinin belirlenmesini içeren süreçtir.
v. **Riski Transfer Etme**: Bir riskin kayıplarını diğer paydaşlarla paylaşma. (Sigorta yaptırma gibi)
w. **YGG**: Yönetimin Gözden Geçirilmesi
x. **PUKÖ**: Planla, Uygula, Kontrol Et, Önlem Al
y. **EYS**: Entegre Yönetim Sistemi
z. **Retina** : Retina Yazılım
aa. **ABGYS :** Retina Yazılım Akıllı Bilgi Yönetim Sistemi
bb. **BİM :** Bilgi İşlem Müdürlüğü
cc. **ZER YAĞ :** ZER YAĞ SAN ve TİC A.Ş.

1. AMAÇ

Bilgi güvenliği yönetim sisteminin amacı tüm bilgi varlıklarımızın gizliliği, bütünlüğü ve gerektiğinde yetkili kişilerce erişilebilirliğini sağlamaktır. Bilgi, diğer kıymetli varlıklarımızın içinde en çok ihmal edilen fakat kurum açısından en önemli varlıklardan biridir. Bilgi güvenliği yönetim sistemimiz TS ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi Standardına uygun olarak kurulmuş ve bu standardın gerekliliklerini karşılayacak şekilde PUKÖ (Planla, Uygula, Kontrol Et, Önlem Al) sürekli iyileştirme döngüsü çerçevesinde bir süreç olarak uygulanmaktadır.

Bilgi güvenliği sadece bilgi teknolojileri çalışanlarının sorumluluğunda değil tüm çalışanların eksiksiz katılımı ile başarılabilecek bir iştir. Ayrıca bilgi güvenliği sadece bilgi teknolojileri ile ilgili teknik önlemlerden oluşmaz. Fiziksel ve çevresel güvenlikten, insan kaynakları güvenliğine, iletişim ve haberleşme güvenliğinden, bilgi teknolojileri güvenliğine kadar birçok konuda çeşitli kontrollerin risk yönetimi metoduyla seçilmesi uygulanması ve sürekli ölçülmesi demek olan bilgi güvenliği yönetim sistemi çalışmalarımızın genel özeti bu politikada verilmektedir. Uygulama detay bilgileri için sistem dokümantasyonuna, ilgili prosedürlere, rehberlere, planlara ve raporlara bakılmalıdır. Aynı zamanda Retina ABGYS yazlımı üzerinden yönetimi ve sürekliliği sağlanmaktadır. Bu politika bilgi güvenliği politikası ve detaylı kullanım politikalarını da kapsayan bir üst dokümandır.

Yönetim tarafından onaylanmış ve yayınlanmıştır. Yönetim tarafından düzenli olarak gözden geçirilmektedir.

2. KAPSAM

ZER Yağ bünyesinde bulunan bilgi sistemleri varlıklarını, bilgi sistemlerine erişim sağlayan personelleri, yazılım geliştirme, satış, kurulum, destek, entegrasyon, eğitim, danışmanlık hizmetlerinin iş süreçlerini kapsar.

Aşağıda verilen konumdaki çalışma ortamları BGYS sertifikası kapsamındadır.

ZER Yağ**, 3. Organize Sanayi Bölgesi Mehmet Batallı Bulvarı No:99 Şehitkamil / **Gaziantep / Türkiye

3. SORUMLULUK VE YETKİ

Bilgi Güvenliği Politikasının güncelliğinin ve sürekliliğinin sağlanmasından BGYS Yöneticisi sorumludur. Bilgi Güvenliği politikasında yapılacak güncellemeler Yönetim Gözden Geçirme toplantılarında belirlenir ve BGYS Yöneticisi tarafından dokümana yansıtılır. Her güncellemede doküman Üst Yönetim tarafından onaylanır.

4. BİLGİ GÜVENLİĞİ NEDİR ?

Bilgi, diğer önemli ticari ve kurumsal varlıklar gibi, bir işletme ve kurum için değeri olan ve bu nedenle uygun olarak korunması gereken bir varlıktır. Bilgi güvenliği iş sürekliliğini sağlamak, kayıpları en aza indirmek için tehlike ve tehdit alanlarından işletmeyi korur.

Bilgi güvenliği, bu politikada aşağıdaki bilgi niteliklerinin korunması olarak tanımlanır:

- **Gizlilik:** Bilginin sadece erişim yetkisi verilmiş kişilere erişilebilir olduğunu garanti etmek,
- **Bütünlük:** Bilginin ve işleme yöntemlerinin doğruluğunu ve yetkisiz değiştirilememesini temin etmek,
- **Erişilebilirlik:** Yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara en hızlı şekilde erişebileceklerini garanti etmek.

Bilgi güvenliği politikası dokümanı, yukardaki korumaları ve gereksinimleri sağlayabilmek için oluşturulmuş denetimlerin uygulanması sırasında kullanılacak en üst seviyedeki prensiplerin belirtildiği dokümandır.

5. BİLGİ GÜVENLİĞİ HEDEFLERİ VE AMAÇLARI

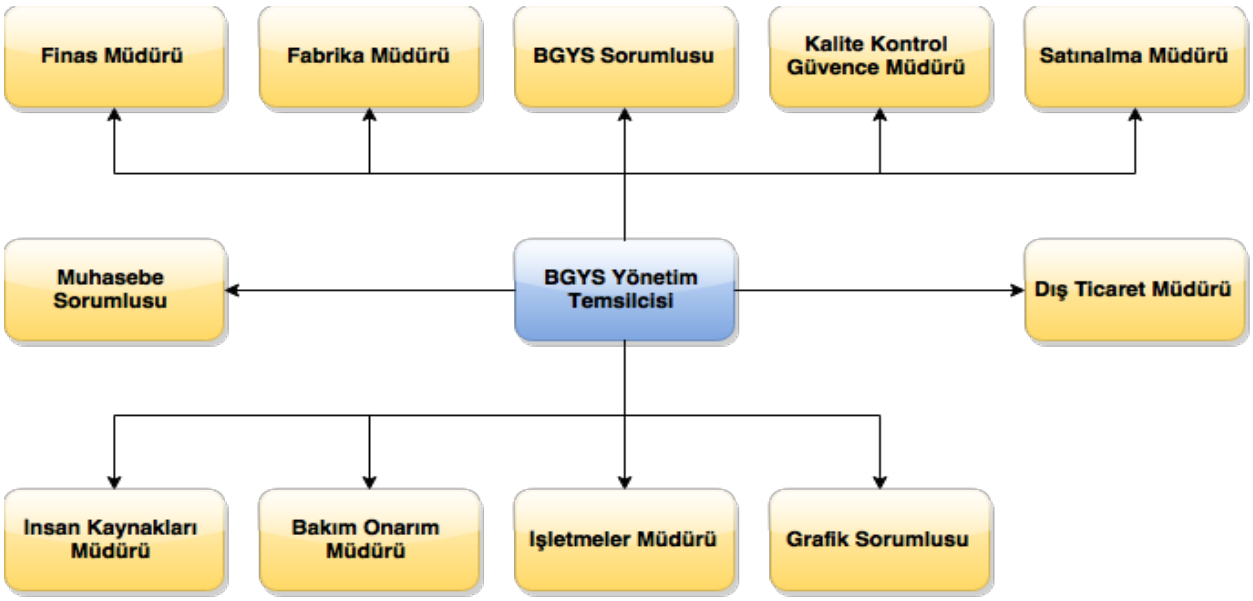
Bilgi Güvenliği Politikası, ZER Yağ çalışanlarına firmanın güvenlik gereksinimlerine uygun şekilde hareket etmesi konusunda yol göstermek, bilinç ve farkındalık seviyelerini artırmak ve bu şekilde firmada oluşabilecek riskleri minimuma indirmek, firmanın güvenilirliğini ve imajını korumak, üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak, teknik güvenlik kontrollerini uygulamak, firmanın temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak amacıyla firmanın tüm işleyişini etkileyen fiziksel ve elektronik bilgi varlıklarını korumayı hedefler.

6. BILGI GÜVENLIĞININ YAPISI VE ORGANIZASYONU

6.1. BGYS Takımı ve Yetkileri

ZER YAĞ bünyesinde bu politika metninde tarif edilen kapsam dahilinde TS ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi Standardı gerekliliklerini yürütmek üzere BGYS KOMİSYONU kurulmuştur.

6.2 BGYS Komisyonu



BYGS Yönetim Temsilcisi : Tuncay KAHRAMAN (Bilgi İşlem Müdürü)

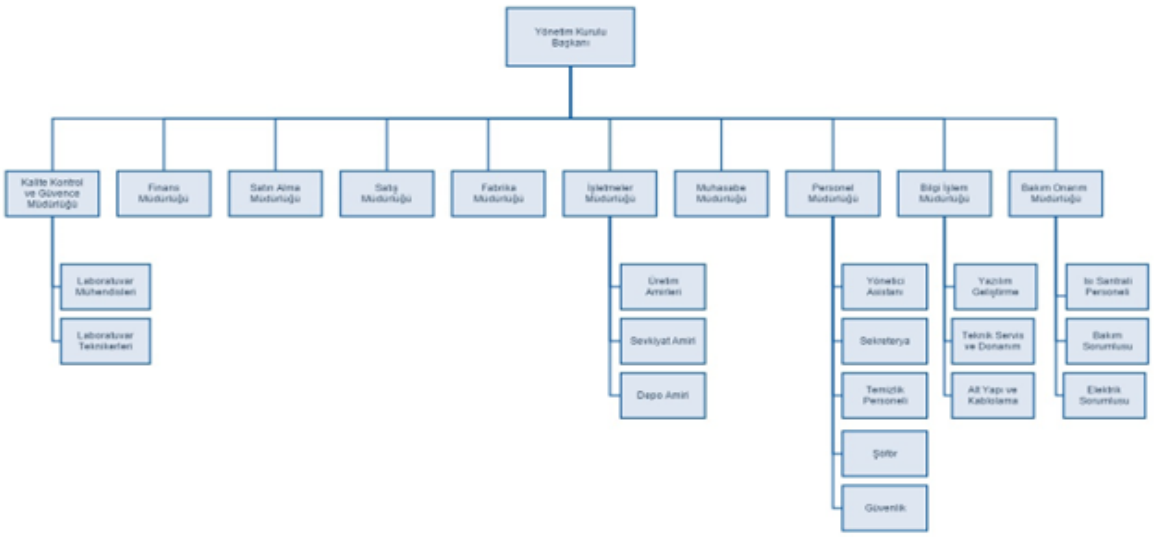
BGYS Sorumlusu : İbrahim Adem AKÇİÇEK (BGYS Sorumlusu)
Hasan Aziztan AYIK(BGYS Sorumlusu)
Mehmet Duran YILMAZ(BGYS Sorumlusu)

Birim Müdür / Sorumluları : Mehmet BOZKURT (Fabrika Müdürü)
Nagehan ÇOŞKUN (Kalite Kontrol ve Güvence Müdürü)
Mehmet BOZKURT (İşletmeler Müdürü)

Hüsamettin SELÇUK (Dış Ticaret Müdürü)
Musa EROL(Finans Sorumlusu)
Cemal SAVCI (Muhasebe Müdürü)
Hacer KALKAN (Satınalma Müdürü)
İbrahim ECİM (İnsan Kaynakları Sorumlusu)
Zekeriya BAŞKUŞ (Grafik Sorumlusu)
Rıza YANIK (Bakım Onarım Müdürü)
Bülent KURTARAN(Planlama Müdürü)

6.3 Organizasyon Şeması

ZERYAĞ SAN. VE TİC. A.Ş. ORGANİZASYON ŞEMASI



7. RISK YÖNETIM ÇERÇEVESI

7.1.Risk Analizi ve Yönetim Stratejisi

Risk analizi için aşağıdaki metot uygulanmaktadır. Bu faaliyetler ilgili kayıtlar risk değerlendirme raporunda tutulmaktadır. Kapsam dahilindeki ve bilgi ile ilişkisi olan her varlığın tespiti için varlık keşif çalışması yapılır. Varlık envanteri ile her kullanıcının sahip olduğu (kullandığı ve yönettiği) varlıklar tespit edilir ve varlıkların sorumluları atanır.

Risk analizi çalışması Tehdit Olasılığı ve İşe Etkisi boyutlarında değerlendirilecektir. Risk hesaplama formülü kullanılarak her bir varlık için risk değeri hesaplanır. Risk takip tablosunda tanımlanan her bir risk için 6 aylık risk durum değerlendirmeleri yapılarak son durum hesaplanır. Risk değerleri için risk değerlerine göre işleme seçeneklerinden uygun olanı seçilir. Kontroller TS ISO/IEC 27001:2013'in Ek-A maddesinden seçilerek uygun olanlar her bir riske atfedilir. Kontrolün nasıl uygulanacağı, kim tarafından uygulanacağı Risk İşleme Takip Tablosunda (ABGYS Yazılımı üzerinden) izlenir. 6 Aylık periyotlarla risk işleme faaliyetlerinin durumu varlık sahiplerinin de katıldığı BGYS komisyonunda değerlendirilir.

7.2. SOA – Uygulanabilirlik Bildirgesi

Risk işleme seçenekleri standardın EK-A bölümünde verilen A.5'den A.18'e 14 kontrol ailesi, 35 farklı başlık ve 113 farklı kontrol olarak verilen listeden seçilebilir. Seçilen kontrollerin her birinin seçilme amacı, kontrolün içeriği, kontrolün uygulanma biçimi ve uygulanmıyorsa nedeni kısa adı SOA (Statement of Applicability) olan dokümanda belirtilmektedir. SOA Gizli bilgi sınıfındadır. BGYS Komisyonunun erişimine açıktır.

Bilgi güvenliği amaçları ve uygulamaları SOA'da detaylandırılmıştır. Risk İşleme planı ve SOA paralel dokümanlardır. Risk işleme planında seçilen kontrollerin isimleri veya EK-A'dan seçilmişlerse A.X.X şeklinde kontrol numarasına atıf yapılırken SOA'da kontroller detaylandırılmıştır. Uygulanan ve uygulanacak tüm kontroller SOA'da kaydedilir. Bu doküman risk işleme planı ile çapraz kontrol sağlayarak herhangi bir kontrolün atlanmamasını sağlamaktadır.

8. ROL VE SORUMLULUKLAR

Bu Bölümde ZER Yağ için bilgi güvenliği sorumlulukları tanımlanmaktadır.

Taraflar	Sorumluluklar
BGYS Yönetim Temsilcisi	- Bilgi Güvenliği Yönetim Sistemi'nin kurulması ve işletilmesi için gerekli kaynak ve sorumluluk tahsislerini gerçekleştirmek, - BGYS altyapısını desteklemek ve işleyişini devam ettirmek, - Çalışanların BGYS hakkında bilgilenmelerini sağlayacak mekanizmaların işletilmesini sağlamak, - Çalışanların bilgi güvenliğine ilişkin olarak karşılaşabileceği riskleri anlaması ve tanıması için eğitici yöntemlerin kullanımını sağlamak, - Bilgi güvenliğini sağlamaya yönelik olarak tespit edilen ihtiyaçların karşılanmasını planlamak ve sağlamak, - Güvenlik Politikasını hazırlamak ve firma içinde uygulanmasını sağlamak, - BGYS kapsamlı dokümanları onaylamak, - BGYS kapsamlı risk analizi sonucunda ortaya çıkan artık riskleri onaylamak.
BGYS Sorumlusu (Yöneticisi)	- Bilgi Güvenliği Yönetim Sistemi'nin kurulması ve işletilmesini sağlamak, - Yönetim Gözden Geçirme toplantılarını koordine etmek, - BGYS dokümanlarının revizyonunu ve kontrolünü yapmak, - BGYS kapsamlı dokümanları onaylamak, - Çalışanların bilgi güvenliği farkındalık eğitimlerinin koordine

	edilmesi ve eğitim etkinliklerinin değerlendirilmesi, - Risk analizi sonuçlarını değerlendirmek, kontrollerin belirlenmesi ve uygulanmasını koordine etmek, - Bilgi Güvenliği İhlal olaylarını değerlendirmek ve takibini yapmak, - Bilgi Güvenliği'ne ilişkin düzeltici faaliyetleri takip etmek ve kayıtları onaylamak, - Bilgi Güvenliği Politikası'nı belirlenen aralıklarla gözden geçirmek ve BGYS Yönetim Temsilcisi'nin onaylamasını sağlamak.
Birim Müdürleri	- Bilgi Güvenliği Politikası'nı uygulamak ve çalışanlarının esaslara bağlılıklarını sağlamak, - Üçüncü taraf bilgi sistemleri kullanıcılarının politikadan haberdar olmasını sağlamak, - Fark ettiği veya kendisine iletilen bilgi sistemleri ile ilgili güvenlik ihlal olaylarını BGYS Yöneticisine bildirmek, - Sahibi olduğu bilgi varlığını korumak ve gerektiğinde güncellemelerde bulunmak, - Faaliyet gösterdikleri konularla ilgili olarak otoritelerle iletişimi sağlamak.
Tüm Çalışanlar	- Bilgi Güvenliği Politikasını bilmek ve uymak, - BGYS kapsamında belirlenen uyulması gereken davranışlara riayet etmek, - BGYS'nin sağlıklı işlemesi için gerekli görülen önerileri ilgilisine iletmek ve sistemin iyileştirilmesine katkıda bulunmak, - Fark ettiği bilgi sistemleri ile ilgili güvenlik ihlal olaylarını Birim Müdürüne bildirmek, - Bilgi güvenliği farkındalık eğitimlerine katılmak.
Üçüncü Taraflar	- Bilgi Güvenliği Politikasını bilmek ve uymak, - BGYS kapsamında belirlenen uyulması gereken davranışlara riayet etmek, - Taahhüt ettiği Gizlilik Sözleşmelerine riayet etmek, - BGYS'nin sağlıklı işlemesi için gerekli görülen önerileri ve ihlal olaylarını ilgili kişiye iletmek.

9. BİLGİ HASSASİYETİ VE RİSKLER

9.1. Bilgi Varlıklarımız

ZER Yağ bünyesinde Madde 1-2 de belirtilen kapsam dâhilinde yer alan tüm fiziki alanlarda bulunan birimlerin yapmış oldukları işlerde üretilen bilgiler bilgi varlıklarımızı oluşturmaktadır.

Masaüstü bilgisayarlar, laptoplar, CD ve DVD ortamındaki veriler, evraklar, klasör ve evrak dolapları, sunucular gibi elektronik veya yazılı-basılı ortamda bulunan veya iletim ortamında (internet, email, telefon vb.) yer alan tüm veriler kurumumuz için bilgi varlığı olarak tanımlanmıştır.

9.2.Varlık Sınıflandırılması

BİLGİNİN SINIFLANDIRMA KLAVUZU		SAKLANMA YERİ
Gizli	En kritik bilgilerdir, sadece yönetim kadrosunun erişimi vardır. Bu tür bilgilerin yetkisiz erişilmemesi, ifşa edilmemesi veya planlanması kurum açısından çok önemlidir. Gizlilik ön plandadır.	Hazırlayan kişi tarafından kontrol edilen ve kapalı odalarda bulunan kilitli dolaplar ve kişisel bilgisayarlar
İç Kullanım	Sadece birimlere özel bilgilerdir. Departman çalışanları dışında hiçbir 3. taraf kurumun veya kişinin görmemesi gereken bilgilerdir. Gizlilik ön plandadır.	Departmanın Kilitli Dolapları
Kişisel	Birim çalışanlarının kişisel çalışmaları ile ilgili bilgilerdir. Kurum işlevleri için yapılan kişisel çalışmalar burada tutulabilir. PC, Laptop veya dolaplarda işle ilgili olmayan diğer kişisel bilgiler tutulamaz. Erişilebilirlik ön plandadır.	Çalışma masaları kilitli çekmeceler
Kuruma Açık	Bu bilgiler kurum çalışanlarının kullanımı içindir. Erişilebilirlik ve bütünlük ön plandadır. Departmanların kendi aralarında paylaştıkları bilgiler bu sınıfa girer.	Departmanın Kilitli Dolapları
Halka Açık	Bu bilgiler tüm birimlere, tedarikçilere ve halka açık bilgilerdir.	Dolaplar ve dolap dışlarında

9.3.Kritik varlıklar

Varlık Kritik Değer Tablosundaki 7 – 11 arası varlıklar kritik varlık olarak kabul edilecektir. Bu varlıklar risk değerlendirme tablosundan faydalanılarak oluşturulacaktır.

10. BGYS YGG (BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ GÖZDEN GEÇİRME) TOPLANTILARI

BGYS biriminin ve üst yönetimin bilgi güvenliğinin uygunluğunu, verimliliğini, risk yönetiminin işlevselliğini, tetkik sonuçlarını, düzeltici ve önleyici faaliyetleri ele aldığı yılda en az bir defa düzenlenen bir toplantıdır. Bu toplantıda yönetim risk kabul kriterlerini ve kaynak ihtiyaçlarını değerlendirir. Çalışmaların, risk değerlendirme ve işleme faaliyetlerinin verimliliğini inceler.

Bu toplantılarda standarda göre girdi ve çıktılar Toplantı Tutanağı Formu kullanılarak kayıt altına alınmaktadır.

11. BİLGİ GÜVENLİĞİ POLİTİKASI

11.1 Genel Esaslar

- Bu politika ile çerçevesi çizilen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar, BGYS prosedürleri ile düzenlenir. ZER Yağ çalışanları ve 3. taraflar bu prosedürleri bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdür.
- Bu kural ve prosedürlerin, aksi belirtilmedikçe, basılı veya elektronik ortamda depolanan ve işlenen tüm bilgiler ile bütün bilgi sistemlerinin kullanımı için dikkate alınması esastır.
- Bilgi Güvenliği Yönetim Sistemi, TS ISO/IEC 27001 "Bilgi Teknolojisi Güvenlik Teknikleri (Information Technology Security Techniques) ve Bilgi Güvenliği Yönetim Sistemleri Gereksinimler (Information Security Management Systems Requirements)" standardını temel alarak yapılandırılır ve işletilir.
- BGYS'nin hayata geçirilmesi, işletilmesi ve iyileştirilmesi çalışmalarını, ilgili tarafların katkısıyla, Danışmanlık Hizmetleri Müdürlüğü yürütür. BGYS dokümanlarının gerektiği zamanlarda güncellenmesi BGYS Yöneticisi sorumluluğundadır. Ek, form, talimat gibi dokümanların güncellenmesi ise ilgili müdürlüklerin sorumluluğundadır.
- Firma tarafından çalışanlara veya 3. taraflara sunulan bilgi sistemleri ve altyapısı ile bu sistemler kullanılarak üretilen her türlü bilgi, belge ve ürün aksini gerektiren kanun hükümleri veya sözleşmeler bulunmadıkça firmaya aittir.
- Kritik iş süreçlerini büyük felaketlerin ve işletim hatalarının etkilerinden korumak amacıyla iş sürekliliği yönetimi uygulanır.
- Çalışanların bilgi güvenliği farkındalığını artıracak ve sistemin işleyişine katkıda bulunmasını sağlayacak eğitimler düzenli olarak mevcut firma çalışanlarına ve yeni işe başlayan çalışanlara verilir.
- Bilgi güvenliğinin gerçek ya da şüpheli tüm ihlalleri rapor edilir; ihlallere sebep olan uygunsuzluklar tespit edilir, ana sebepleri bulunarak tekrar edilmesini engelleyici önlemler alınır.

11.2 Temel BGYS Prensipleri

- Gerekli durumlarda çalışanlar ve üçüncü taraflarla kurumun gizlilik ihtiyaçlarını güvence altına almayı amaçlayan gizlilik anlaşmaları yapılır.
- Dış kaynak kullanım durumlarında oluşabilecek güvenlik gereksinimleri analiz edilerek güvenlik şart ve kontrolleri şartname ve sözleşmelerde ifade edilir.
- Bilgi varlıklarının envanteri bilgi güvenliği yönetim ihtiyaçları doğrultusunda oluşturulur ve varlık sahiplikleri atanır.
- Kurumsal veriler sınıflandırılır ve her sınıftaki verilerin güvenlik ihtiyaçları ve kullanım kuralları belirlenir.
- İşe alım, görev değişikliği ve işten ayrılma süreçlerinde uygulanacak bilgi güvenliği kontrolleri belirlenir ve uygulanır.
- Güvenli alanlarda saklanan varlıkların ihtiyaçlarına paralel fiziksel güvenlik kontrolleri uygulanır.
- Firmaya ait bilgi varlıkları için firma içinde ve dışında maruz kalabilecekleri fiziksel tehditlere karşı gerekli kontrol ve politikalar geliştirilir ve uygulanır.
- Kapasite yönetimi, üçüncü taraflarla ilişkiler, yedekleme, sistem kabulü ve diğer güvenlik süreçlerine ilişkin prosedür ve talimatlar geliştirilir ve uygulanır.
- Ağ cihazları, işletim sistemleri, sunucular ve uygulamalar için denetim kaydı üretme konfigürasyonları ilgili sistemlerin güvenlik ihtiyaçlarına paralel biçimde ayarlanır. Denetim kayıtlarının yetkisiz erişime karşı korunması sağlanır.
- Erişim hakları ihtiyaç nispetinde atanır. Erişim kontrolü için mümkün olan en güvenli teknoloji ve teknikler kullanılır.
- Sistem temini ve geliştirilmesinde güvenlik gereksinimleri belirlenir, sistem kabulü veya testlerinde güvenlik gereksinimlerinin karşılanıp karşılanmadığı kontrol edilir.
- Bilgi güvenliği ihlal olayları ve zayıflıklarının raporlanması için gerekli altyapı oluşturulur. İhlal olay kayıtları tutulur, gerekli düzeltici önleyici faaliyetler uygulanır ve düzenlenen farkındalık eğitimleri vasıtasıyla güvenlik olaylarından öğrenme sağlanır.
- Kritik altyapı için süreklilik planları hazırlanır, bakımı ve tatbikatı yapılır.
- Yasalara, iç politika ve prosedürlere, teknik güvenlik standartlarına uyum için gerekli süreçler tasarlanır, sürekli ve periyodik olarak yapılacak gözetim ve denetim faaliyetleri ile uyum güvencesi sağlanır.

11.3 Uyulması Gereken BGYS Kuralları

- BGYS Politika, Prosedür, Talimatları, çalışanlar ve 3. taraflar için kurum iş süreçlerinde ve ilgili çalışmalarında bilgi depolama, iletim ve kullanım biçimleri ile ilgili uyulması gereken kuralları belirler.
- Aşağıda yer alan davranışlar; aksi yönde açık ve net bir iş tanımı, talimat veya

prosedür bulunmadıkça Bilgi Güvenliği Politikası'nın ihlali olarak değerlendirilir.

- Firma tarafından sağlanan bilgi işlem sistemleri ve uygulamalar iş amaçlı olarak kullanılır. İş süreçlerini engellemeyecek düzeyde ve Bilgi Güvenliği Politikası'nı ve BGYS prosedürlerini ihlal etmeyen kişisel kullanımlar kabul edilebilir kapsamda değerlendirilir.
- Çalışma alanlarında, "Temiz Masa ve Temiz Ekran" prensiplerine uygun olarak, Genel özellikteki bilgiler dışında bilgilerin başkalarınca görülmesine imkan verilmeyecek şekilde önlemler alınmalıdır;
    - Genel olmayan belgeler, masalarda bırakılmamalıdır. Genel olmayan dosyalar üzerinde çalışılırken bilgisayar ekranları herkesin görebileceği konumda bırakılmamalıdır.
    - Genel olmayan dokümanlar diğer kişilerce görülmesini engellemek amacıyla, kullanılmadığı zamanlarda masa üstlerinden kaldırılıp gerekli korumaları alınmış çekmece ve dolaplarda saklanmalıdır.
    - Genel olmayan belgeler dışında doğrudan işle ilgili olarak kendisine ulaştırılmayan ya da teslim edilmeyen firma belgelerini incelememeli, değiştirmemeli, saklamamalı, kopyalamamalı, silmemeli ve paylaşmamalıdır.
    - Firma tarafından açıkça belirtilen durum ve yöntemler dışında 3. taraflar ile kurum bilgilerini paylaşmamalı, satmamalı, aktarmamalı, yayınlamamalı ve internet ortamında paylaşmamalıdır.
    - Birim çalışanları çalıştıkları ortamdaki masa ve dolap çekmecelerini kilitli tutmalı ve anahtarları sorumlu kişiler haricinde kimseyle paylaşmamalıdır.
    - Bilgisayarlar, aktif kullanım dışında iken şifreli ekran koruyucular devreye alınmalıdır.
    - Mesai zamanları dışında bilgisayar sistemleri kapalı tutulmalıdır.
    - Çalışanlar, kendilerine verilmiş olan kullanıcı adı ve şifreleri sadece kendileri kullanmalıdır.
    - Çalışanlar, kendilerine verilmiş olan kullanıcı adı ve parola bilgilerini yetkilendirilmemiş kişilerin ele geçirmesine imkan verecek şekilde söylememeli, yazmamalı, kaydetmemeli, ve elektronik ortamda depolamamalıdır.
- Firmanın, bilgi ve haberleşme sistemleri ve donanımları (İnternet, e-posta, telefon, çağrı cihazları, faks, bilgisayarlar, mobil cihazlar ve cep telefonları vb.) firma işlerinin yürütülmesi için kullanılmalıdır. Bu sistemler yasadışı, firmanın diğer politika, standart ve rehberlerine aykırı veya firmaya zarar verecek herhangi bir şekilde

kullanılmamalıdır.

- Firmaya ait bilgi sistemleri üzerindeki kaynaklara erişecek tüm bilgisayarlar etki alanına dahil edilerek kullanılmalıdır.
- Gerekmedikçe bilgisayar kaynaklarını paylaşıma açılmamalıdır. Kaynakların paylaşıma açılması halinde sadece ilgili kişilere yetki verilmelidir.
- Gizli ve hassas bilgiler elektronik ortamda firma içine ve özellikle firma dışına gönderilmeden önce şifrelenmelidir.
- Gizlilik dereceli bilgiler içeren belgeleri, elektronik ortamları ve bilgi işlem sistemlerini korumak için gerekli fiziksel önlemleri **"Fiziksel Güvenlik Prosedürü"**ne uygun şekilde yerine getirmelidir.
- Firmaya ait bilgi işlem sistemlerini, veritabanlarını, dosyaları, ağ topolojilerini, cihaz konfigürasyonlarını ve benzeri kaynakları, firma tarafından açıkça yetkilendirilmedikçe 3.taraflar ile paylaşmamalıdır.
- Firma çalışanları, çalıştıkları sürece veya firmadan ayrılmaları (emeklilik, istifa, vs.) durumunda firma bilgilerini gizlilik prensibine uygun olarak korumaktan sorumludur.
- Taşınabilir sistemlerin kullanıcıları, bu sistemlerin güvenliğini sağlamak üzere "BG.PT.08 Taşınabilir Cihazlar Kullanım Politikası"ne uymalıdırlar.
- Başta kullanıcı bilgisayarları ve sunucular olmak üzere mümkün olan tüm sistemler, zararlı yazılımlara karşı korunması için "BG.PT.09 Virus ve Zararlı İçerikten Korunma Politikası"ne uygun şekilde kullanılmalıdır.
- Gizlilik dereceli bilgiler elektronik ortamda işlenirken, depolanırken, aktarılırken "İşletim Güvenliği Prosedürü"ne uygun şekilde davranılmalıdır.
- Gizlilik dereceli bilgilerin ve bilgi içeren ortamlarının imhasında "Varlık İmha Prosedürü"ne uygun şekilde davranılmalıdır.
- Herkese açık sistemler (örn. genel internet sayfaları) hariç tüm bilişim sistemlerine erişim parola korumalı olmalıdır. Parolalar **"BG.PT.05 Parola Kullanım Politikası"**na uygun şekilde tanımlanmalı ve kullanılmalıdır.
- Gizlilik dereceli bilgilerin posta, faks, telefon, e-posta ve benzeri elektronik yöntemlerle iletiminde "BG.PT.02 E-Posta Kullanım Politikası"ne uygun davranılmalıdır.
- Herkese açık bilgiler dışındaki bilgileri internet üzerinde, haber gruplarında, posta listelerinde ve forumlarda paylaşmamalıdır.
- Yeni bilgi sistemlerinin devreye alınması ve geliştirilmesi "BG.P.38 Sistem Temini

Geliştirme ve Bakımı Prosedürü"ne uygun yapılmalıdır.

- Çalışanlara ve gerekli görülen durumlarda 3. taraflara tahsis edilen e-posta hesapları, "BG.PT.02 E-Posta Kullanım Politikası"ne uygun şekilde kullanılmalıdır.
- Bilgi işlem sistemlerinin teknik güvenlik gereksinimlerine uygun durumda bulunup bulunmadığı, "BG.P.33 İsletim Güvenliği Prosedürü (Değişim Yönetimi)"ne uygun şekilde kontrol edilmelidir.
- Firmaya ait bilgi işlem sistemlerini izinsiz olarak kullanım dışı bırakılmamalı, yeri değiştirilmemeli ve firma dışına çıkartılmamalıdır.
- Kullanım gerekliliği firma tarafından yazılı olarak belirtilen güvenlik yazılımlarını (örn. antivirüs, kişisel güvenlik duvarı, vb.) bilgi işlem sistemlerden kaldırmamalı veya devre dışı bırakmamalıdır.
- İstemciden istemciye dosya paylaşım programlarını (P2P) kurum bilgisayarlarına yüklememeli ve kullanmamalıdır.
- Firmaya ait bilgisayarlara, firmanın yasakladığı yazılımları yüklememeli ve çalıştırmamalıdır.
- Firma tarafından lisanslanmış yazılımları çoğaltmamalı, paylaşıma açmamalı ve firma dışına çıkarmamalıdır.
- Etki alanına dahil olmayan sistemler ile etki alanına dahil olan sistemler arasında bilgi aktarımı yapılmamalıdır.
- 3. Taraflar ile gizlilik sözleşmesi imzalanmadan ve yetkili firma çalışanınca nezaret edilmeden kurum bilgi işlem sistemlerine ve donanımlarına bağlanmamalı ve çalışmalarına izin verilmemelidir.
- Sunucu sistemleri üzerinde, kişisel bilgisayar uygulamaları (örn; e-posta programları, ofis uygulamaları, yazılım geliştirme araçları, network test araçları, vb.) kurulmamalı ve kullanılmamalıdır.
- İş süreçleri için gerekmeyen ve kullanılmasına izin verilmeyen sunucu hizmetleri (örn; HTTP, Telnet, SSH, vb.) bilgi işlem sistemleri üzerinde çalıştırılmamalıdır.
- Firma tarafından sağlanan ve kullanım amaç ve biçimleri yazılı olarak bildirilen kurum ağ bağlantı yöntemleri dışında bir yöntemle (örn; ADSL modem, 3G modem, GPRS, vb.) internete veya başka ağlara bağlanmak için kullanılmamalıdır.
- Çalışanlar, firma içi ya da firma dışı bilgi sistemlerine yetkisi olmadığı halde zorla girmeye çalışmamalıdır.
- Firmaya ait bilgi işlem sistemlerine şifreleme ve parola mekanizmalarını kırmaya yönelik program ve araçları yüklenmemeli ve kullanılmamalıdır.

- Firmaya ait bilgi sistemleri üzerinde, firmanın bilgisi ve izni olmadan değişiklik, yükseltme, genişletme yapılmamalıdır.
- İşle ilgili olmayan veya telif hakları ile korunan dosyaları (örn. müzik, film, kitap dosyaları, vb.) firma bilgisayarlarına ve bilgi sistemlerine indirilmemeli, depolanmamalı, çoğaltılmamalı ve paylaşıma açılmamalıdır.
- Firma bilgi işlem sistemleri iş dışında, eğlence amaçlı (oyun vb.) kullanılmamalıdır.
- Firma e-posta hesabı ile zincirleme e-posta gönderilmemelidir.

Firma bilgi işlem sistemlerinde veya süreçlerinde gözlenen güvenlik zafiyetlerini, açıklarını veya oluşmuş saldırıları **BG.PR.06 Bilgi Güvenliği İhlal Olayı Yönetimi Prosedürü**'nde belirtilen "bildirme" yöntemi ve muhatapları dışında ilgili olmayan kişilere iletilmemeli, açıklanmamalı, yayınlanmamalı veya bu zafiyetleri yetkisi dışındaki sistem ve bilgilere erişmek için veya kendi yetkilerini arttırmak için kullanılmamalıdır

12. YAPTIRIM

ZER Yağ politika ve prosedürlerine uyulmadığının tespit edilmesi halinde, bu ihlalden sorumlu olan çalışan yada 3. taraf için geçerli olan usul, esas ve sözleşmelerde geçen ilgili maddelerinde belirlenen yaptırımlar uygulanır.

13. YÖNETİMİN SORUMLULUĞU

13.1. Yönetimin Taahhüdü

ZER Yağ belirlediği hedef ve politikalarını gerçekleştirmek için Bilgi Güvenliği Yönetim Sistemini ISO/IEC 27001:2013 'de belirtilen gereksinimleri yerine getirecek şekilde kurarak yürütür.

ZER Yağ Yönetimi, tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan Bilgi Güvenliği Yönetim Sistemine uyacağını ve sistemin verimli şekilde çalışması için gerekli olan kaynakları tahsis edeceğini, etkinliğini, sürekli iyileştireceğini ve bunun tüm çalışanlar tarafından anlaşılmasını sağlayacağını taahhüt eder. Bu taahhüdün sonucu olarak, firma genelinde bilgi güvenliği farkındalık programları düzenler ve alt yapı yatırımlarını sürdürür.

BGYS kurulurken üst yönetim tarafından BGYS Yönetim Temsilcisi ve BGYS Sorumlusu (Yöneticisi), atama yazısı ile atanır. BGYS Yönetim Temsilcisi ve BGYS Yöneticisi değiştiğinde, işten ayrıldığında üst yönetim tarafından doküman revize edilerek atama tekrar yapılır. BGYS Yöneticisini belirlemek ve değiştirmek üst yönetimin yetkisindedir.

Yönetim kademelerindeki yöneticiler güvenlik konusunda alt kademelerde bulunan personele sorumluluk verme ve örnek olma açısından yardımcı olurlar. Üst kademelerden başlayan ve uygulanan bir güvenlik anlayışıyla, firmanın en alt kademe personeline kadar inilmesi zorunludur. Bu yüzden firmadaki yöneticiler, gerek yazılı gerekse sözlü olarak

bilgi güvenliği prosedürlerine uymaları ve bu konularda yürütülen çalışmalara katılmaları konusunda personele destek olurlar.

ZER Yağ üst yönetimi, bilgi güvenliği kapsamlı çalışmalar için gerek duyulan bütçeyi oluşturur.

14. YÖNETİMİN GÖZDEN GEÇİRMESİ

Yönetim Gözden geçirme toplantıları BGYS Komisyonu tarafından yapılır. Bu komisyon BGYS Yönetim temsilcisi başkanlığında yılda en az bir kez veya ihtiyaç duyulduğunda Bilgi Güvenliği Yönetim Sisteminin uygunluğunun ve etkinliğinin periyodik olarak değerlendirilmesi için toplanır.

Toplantılar Yönetimin Gözden Geçirmesi Prosedürü'ne uygun olarak yapılır.

15. ÜÇÜNCÜ ŞAHISLARIN BİLGİYE ERİŞİMİ

ZER Yağ çalışanı olmayan 3. tarafların, bilgi sistemlerini kullanma ihtiyacı olması durumunda (ör: firma dışı bakım onarım personeli) BGYS Yöneticisi, bu kişilerin firma ile ilgili bilgi güvenliği politikalarından haberdar olmalarından sorumludur. Bu amaçla geçici ya da sürekli çalışma sözleşmelerinde sözleşme imzalanmadan önce kararlaştırılmış ve onaylanmış güvenlik anlaşmaları yapılmalıdır. Gerektiği takdirde üçüncü taraf personelinin politikaya uyması için süre tahsis edilmelidir.

16. DIŞ KAYNAK SAĞLANMASI

Bilgi ağı ve/veya kullanıcı bilgisayarı ortamlarının yönetimi dış kaynaklara verilirken, bilgi güvenliği ihtiyaçları ve şartları her iki taraf arasında kabul edilmiş bir sözleşmede açıkça yer almalıdır.

17. BİLGİ GÜVENLİĞİ POLİTİKA DOKÜMANI GÜNCELLENMESİ VE GÖZDEN GEÇİRİLMESİ

Politika dokümanının sürekliliğinin sağlanmasından ve gözden geçirilmesinden BGYS Yöneticisi sorumludur.

Bilgi Güvenliği Politikası organizasyonel değişiklikler, iş şartları, yasal ve teknik düzenlemeler vb. nedenlerle günün koşullarına uyumluluk açısından değerlendirilir.

Bilgi Güvenliği Politikası dokümanı, en az yılda bir kez gözden geçirilmelidir. Bunun dışında sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra da gözden geçirilmeli ve herhangi bir değişiklik gerekiyorsa versiyon değişimi olarak kayıt altına alınmalı ve her versiyon üst yönetime onaylatılmalıdır. Her versiyon değişikliği tüm kullanıcılara e-mail, sunucu üzerinden ya da yazılı olarak yayımlanmalıdır.

Gözden geçirmelerde;

- Politikanın etkinliği, kaydedilmiş güvenlik arızalarının yapısı, sayısı ve etkisi aracılığıyla gözlemlenmelidir.

- Politikanın güncelliği teknolojik değişimlerin etkisi vasıtasıyla gözlemlenmelidir.
- Politika, sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra gözden geçirilmelidir.
-

18. BİLGİ GÜVENLİĞİ İÇ DENETİMLERİ

Kurulan bilgi güvenliği yönetim sisteminin standarda ve tanımlanan politika ve prosedürlere uygunluğunun tespiti için düzenli olarak gerçekleştirilecek iç tetkikler planlanmıştır. İç tetkiklerin nasıl gerçekleştirileceği İç Tetkik Prosedüründe tanımlanmıştır ve bu prosedüre uygun olarak düzenli iç tetkikler yapılarak sistemdeki uygunsuzluklar tespit edilmektedir.

19. SÜREKLİ İYİLEŞTİRME VE DÜZELTİCİ FAALİYETLER

İç tetkiklerde, ihlal olaylarıyla veya personelin kendi gözlemleriyle tespit ettikleri uygunsuzlukların tespitinde ve standarda, politikalarımıza, prosedür ve kurallarımıza uymayan durumların tespitinde ortaya çıkan uygunsuzluğun nasıl giderileceği ve potansiyel uygunsuzlukların henüz ortaya çıkmadan önce nasıl önleneceğine ilişkin Düzeltici Faaliyetler Prosedürü hazırlanmış ve uygulanmaktadır. Tüm personel düzeltici faaliyetlere katılmakla sorumludur

20. İLGİLİ DÖKÜMANLAR

- Tüm BGYS Dokümantasyonu

Firma yönetimi olarak, "Bilgi Güvenliği Politikası"nın uygulanmasının ve kontrolünün yapılmasının, güvenlik ihlallerinde de gerekli yaptırımın icra edilmesinin yönetim tarafından desteklendiğini beyan ederim.

ZER Yağ San. Ve Tic. A.Ş.
Yönetim Kurulu Başkanı
Şerif SELÇUK