

KİŞİSEL VERİLERİN KORUNMASI KANUNU BİLGİ GÜVENLİĞİ PROSEDÜRLERİ (YÖNETİM)

KONU BAŞLIKLARI	SAYFA NO
1. GİRİŞ	1
2. GENEL GÜVENLİK PROSEDÜRÜ	1
2.1. Amaç	1
2.2. Uygulama	1
3. İÇ DENETLEME PROSEDÜRÜ	2
3.1. Tanımlar	2
3.2. İç Denetim Esasları	2
3.2.1. Dış Çevre Denetimleri	2
3.2.2. Donanımsal Denetimler	3
3.2.3. Yazılımsal Denetimler	3
3.2.4. Sunucu Bazlı Denetimler	3
3.2.4.1. Domain Controller	3
3.2.4.2. Mail Server	3
3.2.4.3. File Server	3
3.2.4.4. Proxy/Firewall Server	4
3.2.4.5. IIS Server	4
3.2.4.6. Database Server	4
3.2.5. Ağ Güvenliği Denetimleri	4
3.3. İç Denetim İlkeleri	4
4. TEDARİKÇİ SEÇME VE DEĞERLENDİRME PROSEDÜRÜ	5
4.1. Amaç	5
4.2. Kapsam	5
4.3. Sorumluluklar	5
4.4. Uygulama	5
4.4.1. Tedarikçi Seçme İşlemi	5
4.4.1.1. Hammadde, Malzeme ve Ticari ürün Tedarikçisi Seçme Kriterleri ve İşlemi	6
4.4.1.1.1. Ticari Satın Alma Ürün Grubu İçindir	6
4.4.1.1.2. Hammadde Satın Alma Grubu İçindir	6
4.4.1.2. Makine Yedek Parça Tedarikçileri Seçme Kriterleri ve işlemi	6
4.4.1.3. Mamul ve Sevk Depo Hizmet Tedarikçileri Seçme işlemi	7
4.4.1.4. Hizmet Tedarikçileri Seçme İşlemi	7
4.4.2. Tedarikçi Değerlendirme İşlemi	8
4.4.2.1. Hammadde, Malzeme ve Ticari ürün Tedarikçileri Değerlendirme	8
4.4.2.2. Makine Yedek Parça Tedarikçileri Değerlendirme	9
4.4.2.3. Mamul ve Sevk Depo Hizmet Tedarikçileri Değerlendirme	9
4.4.2.4. Hizmet Tedarikçileri Değerlendirme	9
4.4.2.5. Tedarikçileri Ziyaretleri ve Denetimi	10
5. VARLIK BELİRLEME, SINIFLANDIRMA VE ETİKETLEME PROSEDÜRÜ	10
5.1. Tanımlar	10
5.2. İlgili Dokümanlar	10
5.3. Sorumluluklar ve Uygulama	11
5.3.1. Varlık Envanterinin çıkarılması	11
5.3.1.1. Varlık Sınıflandırması	11
5.3.1.1.1. Yüksek Derece	11
5.3.1.1.2. Orta Derece	11
5.3.1.1.3. Düşük Derece	11
5.3.2. Bilgi Etiketleme ve İşleme	11
5.4. Varlık Belirleme ve Sınıflandırma	12
5.4.1. Varlık Sınıflandırması	12
5.4.2. Varlık Envanterinde Her Bir Varlık İçin Toplanacak Bilgiler Bilgi Varlıkları	12
5.4.2.1. Yazılım Varlıkları	13
5.4.2.2. Fiziksel Varlıklar	13
6. YETKİ PROSEDÜRÜ	14

6.1. Kapsam ve Uygulama	14
7. ACİL DURUM YÖNETİM PROSEDÜRÜ	15
8. BİLGİ GÜVENLİĞİ GÖZDEN GEÇİRME PROSEDÜRÜ	15
9. VERİ ANALİZİ PROSEDÜRÜ	16
9.1. Prosedür Detayı	16
9.2. Analiz Periyotlarına Göre Performans Kriterleri	17
10. YÖNETİMİN GÖZDEN GEÇİRME PROSEDÜRÜ	17
10.1. Gözden Geçirme Periyotları	17
10.2. Toplantının Gündemi	17
10.3. Toplantının Girdileri	17
10.4. Toplantının Çıktıları BGYS etkinliğini iyileştirme	17
10.5. Toplantının Kayıt Altına Alınması	18
11. RİSK DEĞERLENDİRME PROSEDÜRÜ	18
11.1. Tanımlar	18
11.2. Sorumluluklar ve Uygulama	18
11.2.1. Üst Yönetimin Sorumlulukları	18
11.2.2. Birim Yönetimlerinin Sorumlulukları	18
11.2.3. Risk Yönetimi Uzmanlarının Sorumlulukları	18
11.2.4. İç Denetim ve Kontrol Uzmanlarının Sorumlulukları	18
11.2.5. Tüm Çalışanların Sorumlulukları	19
11.3. Risk Etki Oranı Hesaplaması	19

1. GİRİŞ

Bu doküman; bilgi güvenliğinin sürekli gelişimini sağlamak için;
Bilgi varlıklarını tanımlamayı bu varlıkların;

- **İş Etkisini:** Varlığı yerine koyma maliyeti, bilginin gizliliği, imaja olan etkisi, yasal ve hukuki yükümlülükler bakımından yaratacağı zararı gibi konuları ele alarak,
- **Tehdit Olasılığını:** Zayıflıkların çokluğu ve var olan kontrollerin bu zayıflıkları ne kadar kapatabildiği, saldırgan motivasyonu, bilginin rakipler için cazibesi, erişim kontrollerindeki açıklar ve bilginin bütünlüğüne ilişkin tehlikeleri ele alarak,

bilginin gizliliği, bütünlüğü ve erişimine ilişkin riskleri belirlemeyi, değerlendirmeyi, kabul edilebilir seviyenin üzerinde bulunan tüm varlıklar için gerekli kontrolleri uygulamayı, bilgi güvenliği süreçlerinin yönetimini, zayıflıklarımızı ve tehditleri alt yapı, çalışma ortamı, donanım, yazılım ve eğitim yatırımlarıyla en aza indirmeyi, işimizin, müşterilerimizin ve yasal şartların gerektirdiği güvenlik şartlarını karşılamayı, amaçlamaktadır.

Uyulması gereken bilgi güvenliği esasları prosedürlerini kapsamaktadır.

2. GENEL GÜVENLİK PROSEDÜRÜ

Genel Güvenlik Talimatı bünyesinde çalışan tüm personelleri kapsayan ve uyulması zorunlu olan kuralları içermektedir. Bu kuralların ihlali durumunda gerekli yasal işlemlerin başlatılması esastır.

2.1. Amaç

Günümüzde artan nüfusla orantılı olarak bilgi ve doküman sayısı da artmaktadır ve bu artış, bilginin akıcılığını ve işlevselliğini kaybetmemek ve daha da arttırmak amacıyla dijitalleştirme ihtiyacı doğurmuştur. Dijitalleştirme ile fiziksel ortamdaki kazanım sağlanmış ve özellikle geriye dönük evrakların kaybolma ihtimalleri ciddi oranda azaltılmıştır. Fakat bu durum fiziksel ortamdaki evrakların güvenlik tedbirine dijitallerinin de güvenli korunmasını eklemiştir. Büyüyen teknoloji ve bilgiyle birlikte güvenlik sorunları en önemli konuma gelmiş ve bilgi teknolojileri departmanın yanı sıra tüm şirket çalışanlarının başlıca dikkat etmesi gereken bir durum haline gelmiştir.

ÖZEL SALİHLİ GÜVEN SAĞLIK HİZMETLERİ A.Ş. güvenliğinin en önemli unsur olduğunun bilinciyle tüm personelleri bilgilendirmektedir. Tüm personellerin bilgi güvenliğinin önemine hakim olması sağlanarak güvenliğinin en üst seviyeye çıkartılıp görülen açıkların tamamen kapatılmasını amaçlamaktadır.

2.2. Uygulama

- Personeller çalıştıkları bilgisayarların donanımsal, sistemsel ve yazılımsal güvenliğinden sorumludur.
- Personeller işlemekte oldukları fiziksel ve dijital dokümanların güvenliğinden sorumludur.
- Oluşturulan yeni kullanıcıların şifrelerini bilgi teknolojileri departmanı genel şifre olarak belirler, kullanıcı sisteme ilk defa giriş yapacağı zaman şifreyi değiştirir ve o andan itibaren şifre güvenliği sorumluluğu tamamen kullanıcıya aittir.
- Kullanıcı tarafından oluşturulacak şifre en az 8 karakterli olup büyük harf, küçük harf ve sayı barındırır.
- Kullanıcı, **ÖZEL SALİHLİ GÜVEN SAĞLIK HİZMETLERİ A.Ş.** bünyesinde oluşturduğu şifreleri herhangi şirket dışı bir yerde kullanamaz.
- Kullanıcı şifrelerini yöneticisi dahil hiç kimseye paylaşmamakla yükümlüdür ve şifresinin öğrenildiğini düşündüğü anda sistem yöneticisine başvurup şifre değişim talebinde bulunmalıdır.
- Kullanıcı şifre süreleri en uzun **90** gündür. Bu süre sonunda şifresi kullanım dışı kalan veya şifresini unutan personeller sistem yöneticisine başvurmalıdır.
- Kullanıcılar şifrelerini **3** defa yanlış girebilirler. Daha fazla deneme durumunda hesapları **10** dakikalığına kilitlenir. Şifre kabul etmemesi veya hesap kilitlenmesi durumunda kullanıcılar durumu sistem yöneticisine bildirmelidir.
- Kullanıcılar bilgisayarlarını açtıktan sonra herhangi bir nedenden dolayı bilgisayarlarının başından kalkma durumunda kalırlarsa bilgisayarlarını kilitleme moduna almak zorundadırlar. Bu durumun ciddi tehlikeler yaratmaması adına tüm bilgisayarların ayarları işlem yapılmaması durumunda **10** dakika sonra otomatik kilitlenecek şekilde ayarlanmıştır.

- Kullanıcılar şirket mail adreslerini sadece iş gereği ve iş ahlakına uygun olarak kullanmakla yükümlüdürler. Ayrıca gereksiz maillerini ve spam maillerini düzenli olarak silmeli ve haber akışı kaynaklarına kesinlikle üyelik yapmamalıdır.
- Standart kullanıcılar, ağ paylaşım alanında sadece kendi departmanlarının klasörlerine ve sistem yöneticisinin izin verdiği klasörlere erişmelidir, bunların dışındaki herhangi bir klasöre erişebilmesi durumunda sistem sorumlularına bildirmekle yükümlüdür.
- Her bilgisayarın kendine ait bir IP adresi olmalıdır ve standart kullanıcılar IP adreslerini değiştirmek için herhangi bir eğilim göstermemelidirler.
- Sistem yöneticisinin belirlediği bilgisayarlar dışında hiçbir bilgisayar internete açık olmamalıdır. Kullanıcılar tarafından internete açık olduğu tespit edilen bilgisayarları kullanıcılar sistem sorumlularına bildirmekle yükümlüdürler.
- İnternete açık olan bilgisayar kullanıcıları sadece onlara bildirilen alanlarda iş yapmalıdır. Bu alanların dışında çalışma yapan personeller olduğunda durum sistem yöneticisi tarafından anlaşılacak personel uyarılır, tekrarlama durumunda gerekli yasal işlemler yapılır.
- Kullanıcılar ağ üzerinde işlemlerini tamamladıktan sonra o bölümden çıkıp ağı gereksiz meşgul etmemelidirler.
- Personeller gerek fiziksel gerek dijital ortamdaki evrakları kesinlikle çıkartamaz veya şirkete ait olmayan bir dokümanı şirketi içerisine dahil edemez. Bu durumun tespiti halinde gerekli yasal işlemler zaman kaybetmeden yürütülür.
- Standart kullanıcıların uygulama yükleme, kaldırma, güncelleme yetkileri yoktur, bu işlemleri yapma eğiliminde olan personeller uyarılır.
- Standart kullanıcıların kesinlikle usb bellek, cd, dvd vb. harici bellekleri kullanma yetkisi yoktur. Aksi bir durumla karşılaşan kullanıcılar sistem sorumlularını uyarmakla yükümlüdür.
- Yetkili kullanıcılar harici bellekleri kullanmadan önce anti virüs uygulamaları aracılığıyla taratmak zorundadır.
- Personeller mesai bitiminden kısa bir süre önce masalarında bulunan tüm evrakları toparlayarak düzeni sağlamakla yükümlüdür. Herhangi bir evrak kaybı durumunda gerekli yasal işlemler başlatılır.

3. Yetkili personeller mesai bitiminde masalarında fiziksel veya dijital olarak hiçbir evrak veya dış medya yürütücüsü bırakmamalıdır.İÇ DENETLEME PROSEDÜRÜ

3.1. Tanımlar

İç Denetim Esasları genel anlamda 5 ana denetim alanına ayrılır.

Dış Çevre Denetimleri: Genel Olarak sistemin bulunduğu ortamın, Bilgi İşlem Sistem Odasının denetimini içerir.

Donanımsal Denetimler: Sistemlerin içerisindeki parçaların (RAM, Hard Disk, Ekran Kartı), kapalı kutu donanımların (Firewall, Switch) ve genel kablolama sisteminin denetimini içerir.

Yazılımsal Denetimler: Sistem içerisinde bulunan tüm yazılımların denetimini içerir.

Sunucu Bazlı Denetimler: Sunucunun kurumdaki işlevine göre yapılan denetimleri içerir. (DC, FileServer, WebServer)

Ağ Güvenliği Denetimleri: Dış Network ve İç Network Güvenliğini içerir.

3.2. İç Denetim Esasları

3.2.1. Dış Çevre Denetimleri

Şirket içerisinde veri bulunduran herhangi bir sunucu barındırılmamaktadır. Şirketin tüm verileri Cloud üzerinde tutulmaktadır. Şirket içinde olan sistem odasında sadece network cihazları ve kamera kayıt üniteleri bulunmaktadır.

Sistem odasının giriş çıkışlarının sorunsuz yapıldığı, kart sisteminin sorunsuz çalıştığı ve giriş kapısında herhangi bir sorunun olmadığı denetlenir.

Sistem odasında bulunan güvenlik kameralarının düzenli çalıştığı ve açıların doğru noktalara ayarlı olduğu, giriş ve çıkışların görülebildiği, güvenlik kayıtlarının düzenli şekilde tutulup tutulmadığı denetlenir.

Sistem odasının sıcaklığı ve nemi uygun düzeyde oldukları denetlenir.

Odadaki sıcaklık ve nem ölçer sensörlerinin düzenli çalıştığı denetlenir.

Duman sensörünün üzerinde bulunan led lerin yanıp söndüğü ve sistemde bulunan gazın miktarının yeterli olduğu, yangın söndürme tüplerinin uygun yerlerde olduğu, kontrollerinin yapıldığı denetlenir.

Su basmalarına karşı kurulan su sensörlerinin düzenli çalıştığı denetlenir.

Havalandırma sistemi kontrol edilip, sistemde tıkanıklık olup olmadığı denetlenir.

Sunucuların bulunduğu kabinlerin güvenliğinin üst düzeyde olduğu denetlenir.
Sunucuların bulunduğu yerde hava akımının sunucular için optimum düzeyde olması denetlenir.
Sistem odasında bulunan klimanın düzenli çalıştığı ve herhangi bir buzlanma ya da dışarıya su akıtması yapmadığı denetlenir.
Sistem odasından kabloların ortamda güvenli tehdit edecek şekilde olup olmadıkları denetlenir.
Sistem odasının pencerelerinin güvenliği denetlenir.
Sistem odasındaki herhangi bir yerinde, kapıda, pencerelerde, kabinde ya da sunucuda herhangi bir korezyon ya da paslanma olup olmadığı denetlenir.

3.2.2. Donanımsal Denetimler

Sunucuların Hard Disk, Memory, Ekran Kartı, Fan, CPU ihtiyaçlarının olup olmadığı denetlenir.
Sunucu üzerindeki tüm fanların düzenli çalıştığı denetlenir.
Sunucuların içerisindeki parçalarda herhangi bir korezyon ya da paslanma olup olmadığı denetlenir.
Sunucuların iç sıcaklıkları denetlenir.
Sunucudaki kablolama yapısının, sunucunun içerisindeki hava akımını engellemediği denetlenir.
Sunucuların fanları ve iç yapısı, bütün toz ve pisliklerden arındırılacak şekilde temizlenir.
UPS lerin düzgün çalıştıkları kontrol edilip, şebeke elektriği kesilerek UPS testleri yapılır.

3.2.3. Yazılımsal Denetimler

Sunucularda kullanılan tüm yazılımların lisansları denetlenir.
Sunucularda kullanılan tüm yazılımların güncellikleri denetlenir
Sunuculardaki İşletim Sistemlerinin güncellemeleri, yamaları denetlenir.
Özel yazılımlar üzerindeki erişme yetkileri denetlenir.
Güncelliğini yitirmiş ya da kullanılmayan yazılımlar sistemden silinir.

3.2.4. Sunucu Bazlı Denetimler

3.2.4.1. Domain Controller

Group Policy yapısı gözden geçirilir, gerekli görülen değişiklikler varsa yapılır. Fazla yetki verilen kullanıcılar ya da Pc ler varsa yetkileri ellerinde alınır.
DNS yapısı gözden geçirilir, kullanılmayan PC isimleri ya da kullanıcı isimleri varsa silinir. Bir PC ismine birden çok ip bağlanmış olabilir. Kullanılmayan ipler, PC ismi entegrasyonundan çıkarılır.
DHCP yapısı denetlenir. Rezerve olan ip blokları denetlenir. Kullanılmayan ip bloklarının rezervasyonu silinir.
Active Directory'nin, Group Policylerin, DNS ve DHCP yapılarının yedekleri alınır.

3.2.4.2. Mail Server

Mail sistemi olarak Microsoft O365 alt yapısı kullanılmaktadır. Tüm mailler Cloud üzerinde Microsoftun güvencesi altında tutulmaktadır.
Mail Exchanger olarak kullanılan programın güncelliği ve yamaları kontrol edilir.
Mail sunucusundaki veri tabanı kontrol edilir. 6 aydan büyük olan mailler yedeklenip, sistemden silinir.
Bulk olarak adlandırılan ve kullanıcılar tarafından kullanılmayan mailler silinir.
Mail listesindeki kullanıcı isimlerinin güncelliği denetlenir. Kullanılmayan veya Active Directory ile entegre olamamış olan kullanıcılar sistemden silinir.

3.2.4.3. File Server

Dosya sunucusundaki kullanıcılar kotaları kontrol edilir. Kotaları aşan kullanıcılar uyarılarak, gereksiz dosyalarını silmeleri istenir.
Dosya Sunucusunda kullanılmayan paylaşım dosyaları (ör: program kurulumları) silinir.
Dosya sunucusunda silinmek istenen verilerin tamamen silinmesi için özel cleaner programları kullanılır.
Dosya Sunucusundaki tüm dosyaların FULL Back-up'ı alınır.
Dosya Sunucusundaki depolama birimlerinde disk birleştirme işlemi yapılır.

3.2.4.4. Proxy/Firewall Server

Proxy için disk üzerinde ayrılan alan kontrol edilip, gereksiz şekilde tutulan adresler silinir.
Group Policy üzerinde proxy tanımlarının doğru yapıp yapılmadığı kontrol edilir.

Firewall'ın gerekli güncellemeleri yapılmalıdır.

Webfilter'ın gerekli güncellemeleri yapılmalıdır

Anti-Virus'ün gerekli güncellemeleri yapılmalıdır.

Firewallın kuralları gözden geçirilmeli ve görülen açıklıklar kapatılmalıdır.

Firewall üzerinde açık olan portlar kontrol edilmeli ve güvenlik açığı yaratacak olan portlar kapatılmalıdır.

3.2.4.5. IIS Server

IIS Server'da Windows doğrulaması kontrol edilmeli, misafir girişleri yasaklanmalıdır

IIS dosyalarının bulunduğu klasördeki kullanıcı yetkileri gözden geçirilmeli ve gereksiz yetkiler kısıtlandırılmalıdır.

FTP kullanımı açıksa yetkiler kontrol edilmelidir.

Windows'un güvenlik yamaları denetlenmeli, yeni yama varsa yüklenmelidir.

3.2.4.6. Database Server

Veritabanı programının güncelliği denetlenmeli.

Veritabanı sunucusunda bulunan hard diskteki boş alan kontrol edilmeli, gerekirse hard disk takviyesi yapılmalıdır.

Veritabanı programının kullandığı Memory miktarı kontrol edilmeli, kullanılan memory üst düzeydeyse memory takviyesine gidilmeli ya da miktar sınırlandırılmalıdır.

3.2.5. Ağ Güvenliği Denetimleri

Firewallar, Webfilter ve Antivirüs'ün güncellemeleri denetlenmelidir.

Firewall kuralları gözden geçirilmeli, kurallarda güvenliği tehdit edecek açıklar varsa, kurallar düzenlenmelidir.

Firewalldaki açık olan portlar ve uygulamalar denetlenmeli, güvenliği tehdit eden portlar kapatılmalı, uygulamaların ise kullanımı engellenmelidir.

Webfilterların databaseleri güncellenmelidir.

Switch ve Router konfigürasyonları denetlenmelidir. Güvenlik açıkları varsa giderilmelidir.

Kurumdaki DMZ yapısı denetlenmeli, DMZ'deki gereksiz sunucular DMZ'ten çıkartılmalıdır.

VPN erişimleri denetlenmelidir.

3.3. İç Denetim İlkeleri

İç denetim; Bilgi Güvenliği Yönetim Sistemine yapılan yatırımın sürekliliğini sağlamayı, Uygunsuzluklardan doğan açıkların yol açabileceği zararları önlemeyi, Uygunsuzluklardan doğan açıkların yol açabileceği zararları önlemeyi amaçlamalıdır.

İç denetim Bilgi Güvenliği Yönetim Sisteminin kapsamını içermelidir, Kapsam dahilindeki tüm servislerden rastgele seçilmiş en az bir örneklem ile iç denetim yapılmalıdır.

İç denetimi yapan kişi Bilgi Güvenliği Yönetim Sisteminin Planlama ve Uygulama kısmında çalışmayan bir personel olmalıdır.

İç denetimi yapacak kişi Bilgi Güvenliği Yönetim Sistemi, denetleme ve risk yönetimi konusunda bilgili olmalıdır.

Denetçi tarafsız davranabilmelidir.

Önceki denetimlerin çıktıları incelenmelidir.

Kontrol hedeflerinin, kontrollerin, süreçlerin ihtiyaçlara uygunluğunun araştırılmalıdır.

Uygunsuzluklar ve nedenleri belirlenmelidir.

Düzeltilici, önleyici faaliyetleri belirlenmelidir.

Sonuç raporu ve sunumu yapılmalı, iç denetleme sonucunda yüksek risk içeren veya tüm kurumu etkileyen sonuçlar üst yönetimle paylaşılmalıdır.

İç denetim esasları planlanan aralıklar ile gerçekleştirilmelidir.

4. TEDARİKÇİ SEÇME VE DEĞERLENDİRME PROSEDÜRÜ

4.1. Amaç

ÖZEL SALİHLİ GÜVEN SAĞLIK HİZMETLERİ A.Ş. Tedarikçi Seçme ve Değerlendirme işlemlerinin Kalite & Çevre & ISG & MMYS Yönetim Sistemine göre sistematik ve uygun bir şekilde gerçekleşmesinin sağlanmasıdır. Bu prosedürde **ÖZEL SALİHLİ GÜVEN SAĞLIK HİZMETLERİ A.Ş.** 'nin hizmet kalitesine, bilgi güvenliğine ve iş sürekliliğine etki eden tedarikçilerin değerlendirilmesi, seçim kriterlerinin belirlenmesi ve performanslarının takibinde göz önünde tutulacak ölçülerin belirlenmesi amaçlanmaktadır.

4.2. Kapsam

ÖZEL SALİHLİ GÜVEN SAĞLIK HİZMETLERİ A.Ş. Hammadde, Malzeme, Ticari Ürün ve Hizmet Tedarikçi Seçme ve Değerlendirme, Onaylı Tedarikçi listesi oluşturma işlemlerini kapsar.

4.3. Sorumluluklar

- Tedarik Zinciri Yönetimi Direktörü
- Bilgi Teknolojileri Direktörü
- Satın Alma Müdürü
- Ticari Satın Alma Yöneticisi
- Hammadde Satın Alma Yöneticisi
- Lojistik Müdürü
- Teknik Servis Müdürü
- İnsan Değerleri ve Kurumsal İletişim Direktörü
- İş Sağlığı ve Güvenliği Yöneticisi
- Kalite Güvence Müdürü
- Kalite Güvence Yöneticisi
- Kalite Kontrol Yöneticisi
- Kalite Kontrol ve Laboratuvar Teknikeri
- Kalite Kontrol Mühendisi
- Süreç ve Ürün Kontrol Uzmanı
- Dış Proses Kalite Kontrol Teknikeri
- Giriş Kalite Kontrol Teknikeri
- Ar-Ge ve Tasarım Merkezi Müdürü

4.4. Uygulama

4.4.1. Tedarikçi Seçme İşlemi

Tedarikçilerin sağladıkları ürün ve hizmetler **ÖZEL SALİHLİ GÜVEN SAĞLIK HİZMETLERİ A.Ş.** i hizmetinin kalitesine, bilgi güvenliğine ve iş sürekliliğine olan etkisine göre değişik seviyelerde ve kapsamlarda değerlendirmelere tabi tutulurlar. Ürün, hizmet veya süreç satın alınan tüm tedarikçilerin **ÖZEL SALİHLİ GÜVEN SAĞLIK HİZMETLERİ A.Ş.** Torbalı Şubesi ve beklentilerini karşılayabilecek yeterlilikte olmalıdır. Tedarikçilerden sürekli istenen kalitede ürün temin edebilmek için yapılan değerlendirmelerin kayıtları Kalite Güvence Müdürlüğü tarafından tutulur.

Tedarikçiler yılda bir Satın Alma Müdürlüğü & Kalite- Ürün Güvenliği Birimi tarafından değerlendirilir. Değerlendirme sonuçları Kalite Güvence Müdürü tarafından konsolide edilir, Genel Müdür onayına sunulur. Genel Müdür kararı ile tedarikçi ile çalışma kararı verilir.

4.4.1.1. Hammadde, Malzeme ve Ticari ürün Tedarikçisi Seçme Kriterleri ve İşlemi

Alternatif Tedarikçi bulunduğu tedarikçi beş ana kriter açısından değerlendirilir.

- Kalitesel Şartlar
- Üretim Yeterliliği ve Şartları
- Satın Alma
- ISG Durumu ve Şartları
- Sosyal Hizmetler Durumu ve Şartları

Eşitlik İlkesine uygun olarak, çalışanlarımız arasında etik kurallar ve fırsat eşitliğinin istisnasız uygulanmasını sağlamak amacıyla; maaş, yan ödeme/yardımlar, terfi, disiplin, işten çıkarma veya emekliye ayrılma dahil olmak üzere, işe alma ve istihdam uygulamalarında ırk, din, yaş, milliyet, sosyal ve etnik köken, cinsel eğilim, cinsiyet, siyasi görüş veya özürllüklerine dayanarak ayrımcılık yapmayız.

Yukarıdaki kriterlere uyan tedarikçiler belirlenir.

Yukarıdaki kriterlere uyan tedarikçilerden, numune ile birlikte;

- Sistem ve ürün kalite belgeleri
- Kalite kontrol raporları
- Teknik Spesifikasyonlar

- Malzeme/Ürün/ Hizmeti tanımlayıcı ve açıklayıcı katalog, broşür vb. istenir.

Ar-Ge & Tasarım veya Ticari Satın Alma Bölümlerinden gelen yeni ürünler için temin edilen numuneler veya fason üretilmesi ön görülen Ticari Satın Alma tarafından uygun görülen Ticari Ürünler (prototip ürünler/ pilot ürünler/ numune ürünler) için belirlenen süreçler işletilir.

4.4.1.1.1. Ticari Satın Alma Ürün Grubu İçindir

Ticari Ürünler (prototip ürünler/ pilot ürünler/ numune ürünler) Ticari Satın Alma Yöneticisi/ Ticari Satın Alma Uzmanı tarafından Kalite - Ürün Güvenliği Birimine verilir.

Kalite - Ürün Güvenliği Birimi numuneyi şartnameye göre inceler, fonksiyonel olarak değerlendirir.

Kalite Kontrol ve Laboratuvar Teknikeri / Kalite Kontrol Mühendisi tüm kontrol ve görüşleri değerlendirdikten sonra karar verir ve kararını yazar.

Numune talep formu hangi bölümden geliyorsa (Tasarım & Ar-Ge veya Satın Alma Birimine) ilgili birime ürün gönderilir ve ilgili birimlere rapor yayımlanır.

Ticari Satın Alma Birimi, Numune İnceleme Raporunu tedarikçiye gönderir. Numune inceleme raporu teknik şartnameyi ve şartnameye göre numune malzemenin test sonuçlarını içerir. Tedarikçi test sonuçlarını kabul ettiğinin teyidini vererek, raporu Ticari Satın Alma Uzmanına /Ticari Satın Alma Süreç Personeline ulaştırır.

Uygun olan ürünler için Ticari Satın Alma Uzmanı tarafından sipariş açılır ve satın alma işlemi başlatılır.

4.4.1.1.2. Hammadde Satın Alma Grubu İçindir

Numune Ürünler, Satın Alma Uzmanı/ Satın Alma Süreç Personeli tarafından Kalite - Ürün Güvenliği Birimine verilir.

Kalite - Ürün Güvenliği Birimi numuneyi şartnameye göre inceler, fonksiyonel olarak değerlendirir.

Kalite Kontrol ve Laboratuvar Teknikeri / Kalite Kontrol Mühendisi tüm kontrol ve görüşleri değerlendirdikten sonra karar verir ve kararını yazar.

Numune talep formu hangi bölümden geliyorsa (Tasarım & Ar-Ge veya Satın Alma Birimine) ilgili birime ürün gönderilir ve ilgili birimlere rapor yayımlanır.

Satın Alma Birimi, Numune İnceleme Raporunu tedarikçiye gönderir. Numune inceleme raporu teknik şartnameyi ve şartnameye göre numune malzemenin test sonuçlarını içerir. Tedarikçi test sonuçlarını kabul ettiğinin teyidini vererek, raporu Satın Alma Uzmanına /Satın Alma Süreç Personeline ulaştırır.

Uygun olan ürünler için Satın Alma Uzmanı tarafından sipariş açılır ve satın alma işlemi başlatılır.

4.4.1.2. Makine Yedek Parça Tedarikçileri Seçme Kriterleri ve İşlemi

Makine Yedek Parça Seçme Kriterleri aşağıdaki gibidir:

- Yedek Parça Kalitesi
- Fiyatı
- Kullanılabilirliği
- Ömrü
- Termin

Makine Yedek parça alımı esnasında, ihtiyaç olunan parça numunesi veya katalog numarası dikkate alınarak Teknik Satın Alma Birimi ve Bakım ve Onarım Birimi tarafından gerekli araştırma yapılır.

Fiyat teklifleri alınır, fiyat onay baremine göre Tedarik Zinciri, Satın Alma Müdürü en son Genel Müdürlük onayına sunulur. Yukarıda belirtilen kriterlere göre uygun olan tedarikçiden alım gerçekleştirilir.

4.4.1.3. Mamul ve Sevk Depo Hizmet Tedarikçileri Seçme İşlemi

Sevkiyat ve Mamul Depoda Mamul ve Sevk Depo Hizmet Tedarikçileri Değerlendirmesi tablosuna göre, hizmet tedarikçileri seçilir. Burada belirtilen seçme kriterleri aşağıdaki gibidir.

Fiyat uygunluğu

Malı zamanında ve hasarsız teslim etmesi

Tedarikçinin temin ettiği araç özellikleri (aracın bakımlı görünüşü, kasa içerisinde kırık veya hasar olup olmaması, yüklenen yüke zarar verici unsurların olmaması, araçtan yağ, mazot vb kimyasal sızıntı olmaması)

Aracın yüklenen yükü dış etkilere karşı koruyacak olan çadır veya brandası ile gerekirse yükü bağlayacak ip, urgan vs. malzemesinin olup olmaması.

Tedarik edilen aracın kasa ölçülerinin ve iç hacminin yük için uygun olması.

Kanaat

Tedarikçi firmanın KYS / ÇYS sistem sertifikasına sahip olması

Kullanılan yakıtın yasal olması, gerekli yeterlilik belgelerine sahip olması
Uygun tedarikçilerin teklifleri, Lojistik Müdürü tarafından değerlendirilir ve incelenir.
Uygun tedarikçi belirlendikten sonra önce Tedarik Zinciri, Satın Alma Müdürü onayı sonrasında
Genel Müdür onayı ile hizmet alımı başlatılır.

4.4.1.4. Hizmet Tedarikçileri Seçme İşlemi

Seçme İşlemi Aşağıda belirtilen HİZMET TEDARİKÇİLERİ SEÇME KRİTERLERİ tablosuna göre yapılmaktadır.

ALINAN HİZMET	SEÇME KRİTERİ	İLGİLİ BÖLÜM YETKİLİSİ ONAY
Kalibrasyon	TS ISO 17025 standardına göre izlenebilirliğe sahip olmalıdır.	Kalite Güvence Müdürü
	Fiyat	
	Kalibre edilecek %70 kapsayan kısmının kalibre edebilecek kapasitede olması	
Laboratuvar	TS ISO 17025 standardına göre izlenebilirliğe sahip olmalıdır.	
	Fiyat	
Danışmanlık hizmeti	Referansların uygun olması	
	Konusunda uzman olması	
Eğitim hizmeti	Referansların uygun olması	İnsan Değerleri ve Kurumsal İletişim Direktörü
	Konusunda uzman olması	
	Eğitimin içeriği ve süresi uygunluğu	
	Fiyat	
Yangın Söndürme tipleri dolun hizmeti	TSE Yeterlilik belgesi olması	
	ISO 9001 2000 KYS belgesi olması	
	Referansların uygun olması	
Forklift Bakımı ve Onarımı	Servis Yetki belgesi olmalıdır	
	Fiyat	
Yük kaldırıcı ekipmanların testleri	Yetki belgesi olmalıdır	
	Fiyat	
Tank sızdırmazlık testleri	Yetki belgesi olmalıdır	Bakım ve Teknik Hizmetler Müdürü
Elektronik kart onarım hizmeti	Referansların uygun olması	
	Tamir bedeli	
Bakım Servis Hizmeti	Yetki belgesi olmalıdır	
	Referansların uygun olması	
	Servis kapsamı	
	Fiyat	

4.4.2. Tedarikçi Değerlendirme İşlemi

Tedarikçi Değerlendirme işlemi iki ana gruba ayrılır;

- Ticari Ürün, Hammadde ve Malzeme Tedarikçileri değerlendirme (Kimyasal malzemeler dahil)
- Ürün kalitesine etki eden Hizmet Tedarikçileri Değerlendirme

4.4.2.1. Hammadde, Malzeme ve Ticari ürün Tedarikçileri Değerlendirme

Ürün kalitesine etki eden hammadde ve malzeme tedarikçilerine yapılan işlemleri kapsar. (Sarf malzemelerini kapsamaz.)

Değerlendirme her yıl aralık ayında Kalite Güvence Müdürü ve Satın Alma Müdürü tarafından yapılır. Değerlendirme kriterleri aşağıdaki gibidir.

PUAN TÜRÜ	HEDEF PUAN	PUAN TÜRÜ	HEDEF PUAN
TERMİN PUANI	130	KALİTE PUANI	400
FİYAT PUANI	90	İSG VE ÇEVRE PUANI	115
SATINALMA PUANI	120	SATINALMA PUANI	485
ÜRETİM YETERLİLİĞİ VE ŞARTLARI	145		

Değerlendirme faaliyeti sonucunda firmalara performanslarına göre puan verilir. Her yeni yıl başlangıcında hazırlanan Onaylı Tedarikçi Listesinde, bu firmaların performansı, aldıkları puana göre 5 ana grupta gruplandırılır:

GRUP	MİN	MAX	AÇIKLAMA
A GRUBU	81	100	Tedarikçi " <u>Stratejik Firma</u> " kapsamındadır. AR-GE çalışmaları da dahil olmak üzere <i>yoğun çalışılabilir</i> .
B GRUBU	70	80	Tedarikçi " <u>İşbirlikçi Firma</u> " kapsamındadır.
C GRUBU	55	69	Tedarikçi " <u>Geliştirilmesi Gereken Firma</u> " kapsamındadır.
D GRUBU	31	54	Tedarikçi " <u>Zorunlu Hallerde Çalışılacak Firma</u> " kapsamındadır. İlk 6 ay içinde 50 puanı geçmesi şarttır. 50 puanı geçemezse
E GRUBU	0	30	Tedarikçi " <u>Çalışılmayacak Firma</u> " kapsamındadır.

Yapılan performans değerlendirme sonucunda, puan türüne karşılık gelen grubunda yer alan tedarikçilere, Satın Alma Müdürü tarafından performans sonuçları bildirilir.

Yıl içerisinde eklenen yeni tedarikçiler için 5.1 Maddesinde bulunan Tedarikçi Seçme Sistemi uygulanır. Tedarikçi seçme kriterlerine uygun olan tedarikçilere alım yapılmaya başlanır ve performansı ilk 6 ay gözlemlenir. Yukarıdaki kriterler eğer uyuyorsa onaylı tedarikçi listesine alınır.

Onaylı tedarikçi listesinde olmayan C ve D grubundaki tedarikçilerden alım yapılmak zorunda kalındığında, Satın Alma Müdürü tarafından Kalite ve Güvence Müdürüne bilgi verilir. Giriş Kalite Kontrol örneklem/sıklıkları artırılır. (Bkz. Giriş Kalite Kontrol talimatı)

Her yıl aralık ayı sonunda Tedarikçi Değerlendirme sonuçlarına göre Onaylı Tedarikçi Listesi Satın Alma Müdürlüğü tarafından revize edilir. Onaylı Tedarikçi listesinde değişiklik mevcut ise revizyon sayısı bir artırılır. Satın Alma Müdürlüğü tarafından Genel Müdür onayı alındıktan sonra QDMS'de yayınlanır.

4.4.2.2. Makine Yedek Parça Tedarikçileri Değerlendirme

Temin edilen Makine Yedek Parçasının tedarikçileriyle yapılan işlemleri kapsar

Temin edilen Makine Yedek parçasının kullanım ömrü dikkate alınarak yapılır. Bakım ve Teknik Hizmetler Müdürü tarafında uygun olmayan tedarikçiler Satın Alma Birimine bildirilir.

Değerlendirme her yıl aralık ayı sonunda Bakım ve Teknik Hizmetler Müdürü ve Satın Alma Müdürü tarafından yapılır. Değerlendirme kriterleri aşağıdaki gibidir.

4.4.2.3. Mamul ve Sevk Depo Hizmet Tedarikçileri Değerlendirme

Sevkiyat ve Mamul Depoda Mamül Ve Sevk Depo Hizmet Tedarikçileri Değerlendirmesi tablosuna göre, hizmet tedarikçileri değerlendirilir. Burada belirtilen değerlendirme kriterleri aşağıdaki gibidir.

- Fiyat uygunluğu
- Malı zamanında ve hasarsız teslim etmesi

- Tedarikçinin temin ettiği araç özellikleri (aracın bakımlı görünüp, kasa içerisinde kırık veya hasar olup olmaması, yüklenen yüke zarar verici unsurların olmaması, araçtan yağ, mazot vb kimyasal sızıntı olmaması)
- Aracın yüklenen yükü dış etkilere koruyacak olan çadır veya brandası ile gerekirse yükü bağlayacak ip, urgan vs. malzemesinin olup olmaması.
- Tedarik edilen aracın kasa ölçülerinin ve iç hacminin yük için uygun olması.
- Kanaat
- Tedarikçi firmanın KYS / ÇYS sistem sertifikasına sahip olması
- Kullanılan yakıtın yasal olması, gerekli yeterlilik belgelerine sahip olması

4.4.2.4. Hizmet Tedarikçileri Değerlendirme

- Kalibrasyon hizmeti verenler.
- Danışmanlık ve eğitim hizmeti verenler.
- Bakım hizmeti verenler.
- Yangın söndürme tüpleri dolun hizmeti verenler.
- Laboratuvar Hizmeti verenler
- Yemek Hizmeti verenler
- Servis/Taşıma Hizmeti Verenler
- Satış Sonrası Hizmetler (servis) Hizmeti Verenler

Hizmet Tedarikçileri değerlendirme, hizmeti alan ilgili birim müdürleri tarafından yapılır.

Birim müdürleri her yılın aralık ayında hizmet tedarikçilerini aşağıda belirtilen HİZMET TEDARİKÇİLERİ DEĞERLENDİRME KRİTERLERİ tablosuna göre yaparlar.

Tedarikçi değerlendirmelerinde yerinde denetimde yapılabilir.

Yerinde Denetim sonuçları ek bir kriter ve puan olarak eklenir.

ALIN AN HİZMET	DEĞERLENDİRME KRİTERİ	İLGİLİ BÖLÜM YETKİLİSİ ONAY
Kalibrasyon	Cihaz hatalarından kaynaklanan ölçüm hatası olmaması (Uygun Olmayan Ürünün ve Düzeltici Faaliyet formları)	Kalite Güvence Müdürü
	ISO 9001 de kalibrasyon işleminden kaynaklanan uygunsuzluk olmaması	
Laboratuvar	Test sonucundan kaynaklanan hata ve buna bağlı Düzeltici Faaliyet açılmış olmaması	
Danışmanlık hizmeti	Danışman tarafından verilen faaliyet planına uyum	İnsan Değerleri ve Kurumsal İletişim Direktörü
Eğitim hizmeti	Eğitim Genel değerlendirme formunda uygun sonuç alması	
Yangın Söndürme tüpleri dolun hizmeti	Yangın Tüpleri Doluluk oranı Servis hizmeti (Boşalan tüplerin doldurulma süresi)	
Forklift Bakımı ve Onarımı	Yapılan tamirlerden ve bakımından sonra arızanın tekrarlanmaması (parça ömrü periyodu içinde)	Bakım ve Teknik Hizmetler Müdürü
Yük kaldırıcı ekipmanların testleri	Yük kaldırıcı ekipmanda uygun çalışması	
	İş kazası olmaması	

Tank sızdırmazlık testleri	Periyodik olarak kontrol esnasında problem görülmemesi	
Elektronik kart onarım hizmeti	Tamir olarak kartın arızasının tekrarlanmaması	
Bakım Servis Hizmeti	Yapılan bakım sonrasında cihazda arıza oluşmaması	

4.4.2.5. Tedarikçileri Ziyaretleri ve Denetimi

Tedarikçi denetimi aşağıdaki durumlarda yapılabilir:

C ve D grubunda bulunan, kapasite ve fiyat kriterine uygun ana hammadde tedarikçileri

Bir alt gruba düşen ana hammadde tedarikçileri

Ana Hammadde sağlayan yeni tedarikçiler

Denetim esnasında Tedarikçi değerlendirme soru listesi kullanılır.

Soru listesine binaen oluşan puana göre tedarikçilere uygulanması gereken tedarikçi grubu tespiti yapılır ve tedarikçi grubuna karşılık gelen uygulama seçilir.

ISO 9001 Kalite Yönetim Sistemi ve/veya ISO 27001 BGYS Belgelerinin olması tercih sebebidir.

Referans onayı olması gereklidir. (Daha önce çalıştığı firmalardan bilgi istenir)

Sözleşmede gizlilik maddesi içermeyen sözleşme sunan ya da **ÖZEL SALİHLİ GÜVEN SAĞLIK HİZMETLERİ A.Ş.** Torbalı Şubesi'nin Gizlilik sözleşmesini onaylamayan firmalar ile çalışılmaz.

5. VARLIK BELİRLEME, SINIFLANDIRMA VE ETİKETLEME PROSEDÜRÜ

5.1. Tanımlar

- **Varlık:** **ÖZEL SALİHLİ GÜVEN SAĞLIK HİZMETLERİ A.Ş.** i için değerli olan herhangi bir şey.
- **Bilgi Varlıkları:** Veri tabanları ve veri dosyaları, kişisel veri, sistem belgeleri, kullanıcı el kitapları, eğitim malzemeleri materyalleri, işlemsel ve destek uygulamaları, devamlılık (süreklilik) planları, yedek anlaşmaları, arşivlenmiş bilgi;
- **Yazılım Varlıkları:** Uygulama yazılımları, sistem yazılımları, geliştirme araçları ve yazılımları vb.
- **Fiziksel Varlıklar:** Bilgisayar ekipmanları (kasa, ekranlar, diz üstü bilgisayarlar, modemler), iletişim ekipmanları (yönlendirici, telefon, faks), manyetik kayıt ortamları (teyp, kartuş, disket, disk, CD), diğer teknik ekipmanlar (güç kaynakları, adaptör, havalandırma üniteleri), mobilya, yerleşim düzeni;
- **Servisler:** Bilgi teknolojileri (bilgisayar) ve iletişim (haberleşme) hizmetleri, genel hizmetler (ısıtma, aydınlatma, elektrik, havalandırma).

5.2. İlgili Dokümanlar

- Varlık Envanter Listesi

5.3. Sorumluluklar ve Uygulama

5.3.1. Varlık Envanterinin çıkarılması

Varlıkların envanterine etkin varlık korumasının gerçekleştiğini temin etmeye yardımcı olması amacıyla; sağlık ve güvenlik, sigorta, kişisel veri ve mali (varlık yönetimi) nedenler gibi diğer ticari amaçlar

için de gereksinim duyulmaktadır. Varlıkların envanterinin toplanması süreci, risk yönetiminin önemli bir parçasıdır. Varlık envanteri çalışmalarında aşağıdaki hususlar göz önünde bulundurulmalıdır. Bilgi teknolojileri varlıklarının envanteri ve kişisel veri envanteri, her bilgi teknolojileriyle bağlantılı olan önemli bilgi varlıklarını ve kişisel verileri içerecek şekilde, ilgili Yönetim birimlerince hazırlanmalı, korunmalı ve bu envanterler periyodik olarak ve değişiklikler oldukça güncellenmelidir. Bu çalışmada:

- Her bir varlık açıkça tanımlanmalı;
- Varlık sahipleri belirlenmeli;
- Varlıkların güvenlik sınıflandırmaları yapılmalı;
- Varlığın mevcut bulunduğu yer (bu kayıp ve hasarlar giderilmeye çalışıldığında önemlidir) belirtilmelidir.

5.3.1.1. Varlık Sınıflandırması

Bilişim sistemleriyle ilgili varlıklar aşağıdaki şekilde kategorize edilebilir:

Bilgi varlığı; korunma gereksiniminin, önceliklerinin ve derecesinin belirlenmesi için sınıflandırılmalıdır. Varlık sınıflandırmasında aşağıdaki konular göz önünde bulundurulmalıdır:

- Varlık sınıflandırması ihtiyaç, önem ve koruma için ayrılacak kaynak gereksinimini yansıtmalıdır.
- Bilgi varlıkları değişik önem ve hassasiyet derecesine sahip olabilirler.
- Bazı bilgi varlıkları, ilave korunma seviyesine veya özel olarak ele alınmaya gerek duyabilir.
- Bilgi varlıkları sınıflandırma sistemi, uygun koruma seviyesi tanımlanması için kullanılmalıdır.
- Bilgi varlıklarının zaman içerisinde sınıflandırma derecesi değişebilir.
- Bilgiye ait bir ögenin; örneğin bir belgenin, veri kaydının, veri dosyası veya disketinin; sınıflandırılmasının ve bu sınıflandırmanın belirli zamanlarda gözden geçirilmesinin sorumluluğu yaratıcıda veya bilgiye atanmış sahibindedir.

5.3.1.1.1. Yüksek Derece

Bu varlıklar, Kurum için yüksek değer taşımaktadır. Kaybı ya da zarar görmesi Kurumun faaliyetlerinin devamlılığında şiddetli etkiye sebep olabilir.

Bu varlıklar, güvenliği sağlanmış ve sadece yetkili kişilerin girebileceği odalarda bulunan kasa ya da kilitli dolaplarda saklanmalı; kopyalama, iletme, imha, silme ve anonimleştirme için yetkili kişinin onayı alınmalıdır. Bu varlıklar, yakılarak ya da birleştirilmeyecek derecede parçalanarak imha edilmelidir.

5.3.1.1.2. Orta Derece

Bu varlık, değerlidir ve yerine başka varlık kullanılabilir, kaybı ya da zarar görmesi durumunda, Kurum karlılığında ani etkilere sebep olabilir.

Yüksek derece varlıklar gibi, yetkili kişi izni ile kopyalama, iletme ve imha işlemi yapılmalıdır.

5.3.1.1.3. Düşük Derece

Bu varlığın, iş devamlılığında ekonomik bir değeri yoktur ve düşük bir maliyetle yeri doldurulabilir.

Sahibine özel kullanılan varlıklardır. Herhangi bir güvenlik derecesine sahip olmayan, iş ile ilgili ya da iş dışındaki bilgilerdir.

5.3.2. Bilgi Etiketleme ve İşleme

Gerekli olduğu durumda, fiziki ve elektronik ortamda olan bilgi varlıkları; sınıflandırma derecesini gösterecek şekilde etiketlenmelidir. Bilgi etiketleme ve işleme için kullanılacak standartlar ve prosedürler belgelenmeli ve uygulanmalıdır. Bilgi etiketleme ve işlemede aşağıdaki kurallar uygulanmalıdır:

- a. Fiziksel etiketler, mümkün olduğu durumlarda kullanılmalıdır. Bununla beraber, elektronik biçimdeki belgeler gibi bazı bilgi varlıkları, fiziksel olarak etiketlenemezler. Bu nedenle, bu tür belgelerde elektronik anlamda etiketlemenin kullanılması gerekmektedir.
- b. Dokümanlar, içerdiği bilginin en yüksek güvenlik seviyesi göz önüne alınarak sınıflandırılmalı ve bu sınıflandırma derecesi her sayfanın sol üst ve alt köşesinde büyük harflerle ve altı çizili olarak yer almalıdır.
- c. Manyetik kayıt ortamındaki (kartuş, disk, disket, CD, kaset vb.) bilgiler yine en üst güvenlik seviyesi dikkate alınarak etiketlenmeli ve sınıflandırma seviyesi büyük harflerle ve altı çizili olarak medya üzerine yazılmalıdır.
- d. Elektronik ortamdaki belgelerde de (Word, Excel, PowerPoint dosyaları vb.), bilginin güvenlik seviyesini gösteren ibare, dosya içerisinde her sayfada sol üst ve alt köşede büyük harflerle ve altı çizili olarak bulunmalıdır.

- e. Yüksek derece, bilgilerin gerekli güvenlik önlemi alınmadan posta, faks veya elektronik ortamda aktarılması gerekmektedir. Yine bu seviyedeki bilgiler, izinsiz kişilerin eline geçme riski olduğundan, cep telefonu, sesli mesaj, telefon gibi ortamlarda aktarılmamalıdır. Bu varlıklara sahip kişiler, bu varlığın bilmesi gerekenlerden başkasının görmemesini sağlamalıdır.

5.4. Varlık Belirleme ve Sınıflandırma

Varlıkların envanterine etkin varlık korumasının gerçekleştiğini temin etmeye yardımcı olması amacıyla; sağlık ve güvenlik, sigorta, kişisel veri ve mali (varlık yönetimi) nedenler gibi diğer ticari amaçlar için de gereksinim duyulmaktadır. Varlıkların ve kişisel veri envanterinin toplanması süreci, risk yönetiminin önemli bir parçasıdır. Varlık ve kişisel veri envanteri çalışmalarında aşağıdaki hususlar göz önünde bulundurulmalıdır:

Bilgi **teknolojileri** varlıklarının envanteri, her bilgi teknolojileriyle bağlantılı olan önemli bilgi varlıklarını içerecek şekilde, ilgili Yönetim birimlerince hazırlanmalıdır. Bu çalışmada:

1. Her bir varlık için tanımlayıcı bir kod verilmelidir.
2. Her bir varlığın hangi kategoride olduğu belirtilmelidir.
3. Her bir varlık açıkça tanımlanmalıdır.
4. Varlık sahipleri belirlenmelidir.
5. Varlığın mevcut bulunduğu yer (bu kayıp ve hasarlar giderilmeye çalışıldığında önemlidir) belirtilmelidir.

5.4.1. Varlık Sınıflandırması

Bilgi varlığı; korunma gereksiniminin, önceliklerinin ve derecesinin belirlenmesi için sınıflandırılmalıdır. Varlık için iki tip (güvenlik, değer) sınıflandırma yapılmalıdır. Bu sınıflandırmalarda aşağıdaki konular göz önünde bulundurulmalıdır:

- a. Varlık sınıflandırması ihtiyaç, önem ve koruma için ayrılacak kaynak gereksinimini yansıtmalıdır.
- b. Bilgi varlıkları değişik önem ve hassasiyet derecesine sahip olabilirler.
- c. Bazı bilgi varlıkları, ilave korunma seviyesine veya özel olarak ele alınmaya gerek duyabilir.
- d. Bilgi varlıkları sınıflandırma sistemi, uygun koruma seviyesi tanımlanması için kullanılmalıdır.
- e. Bilgi varlıklarının zaman içerisinde sınıflandırma derecesi değişebilir.
- f. Bilgiye ait bir ögenin; örneğin bir belgenin, veri kaydının, veri dosyası veya disketinin; sınıflandırılması sorumluluğu yaratıcısında veya bilgiye atanmış sahibindedir.

5.4.2. Varlık Envanterinde Her Bir Varlık İçin Toplanacak Bilgiler Bilgi Varlıkları

Her birim kullandığı kritik bilgi varlıklarını tespit ederek envantere kaydetmelidir. Envanterde yer alan alanların açıklaması aşağıda belirtilmiştir.

- a. **Varlık kod:** Varlık kod numarası verilmelidir.
- b. **Tanımı:** Varlığın tanımı özet olarak yazılmalıdır.
- c. **Alt kategori:** Aşağıdaki alt kategorilerden uygun olanın harfi belirtilmelidir. Bilgi varlığının bu alt kategorilerde belirtilen gruplar dışında değerlendiriyorsanız (E) harfini kullanabilirsiniz ya da eğer gerekiyorsa bu alt kategorilere kendi alt kategorinizin harfini de ekleyebilir ve kullanabilirsiniz (Bu durumda ilgili açıklama notu yazılmalıdır).
 - A. Veri tabanları
 - B. Veri dosyaları
 - C. Basılı materyal (sistem belgeleri, kullanıcı el kitapları, eğitim malzemeleri materyalleri, işlemsel ve destek uygulamaları, devamlılık (süreklilik) planları, yedek anlaşmaları, sözleşmeler vb.)
 - D. Arşivlenmiş bilgi
 - E. Diğer (Yukarıdaki alt kategoriler dışında bulunan bilgi varlıklarıdır.)
- d. **Varlık sorumlusu 1 (Bilgi İşlem Yöneticisi):** Bilgi varlığının sorumlusu belirtilmelidir. Bu kişi varlığın yaratıcısı olabileceği gibi, varlığa erişmesi gerekenleri yetkilendirme kararını veren ve varlık üzerinde yapılması gereken işlerde onay alınması gerekli kişi de olabilir.
- e. **Varlık sorumlusu 2:** Varlık sorumlusu 1' e ulaşılmadığı durumlarda varlıktan sorumlu olan yedek ikinci kişi adı verilmelidir.
- f. **Güvenlik sınıflandırması:** Varlığın içerdiği bilgi itibarı ile güvenlik seviyesi; bu Varlık Belirleme, Sınıflandırma ve Etiketleme Prosedürü'nün Tanımlar başlığında verilen kategoriler içerisinde uygun olarak belirlenmelidir. Güvenlik sınıflandırmasında bu varlığa kimlerin erişebileceği; kurum

içerisindeki değeri, kullanımı, saklanması, iletimi ve yok edilmesinde gerekli güvenlik önlemleri gibi unsurlar düşünülerek sınıflandırma yapılmalıdır.

- g. Değer Sınıflandırması:** Bilgi varlığının Kurum içerisindeki değeri; bu Varlık Belirleme, Sınıflandırma ve Etiketleme Prosedürü' nün Varlık Sınıflandırması başlığında verilen kategorilere uygun olarak belirlenmelidir. Varlığın değeri tespit edilirken; bu varlık üzerinde değişiklik olursa ya da varlık kaybedilirse yaşanacak sıkıntılar, bunun iş devamlılığına ya da sistemlere etkisi, bu sıkıntıların giderilmesi için gerekli kaynak gibi unsurlar göz önüne alınmalıdır.
- h. Bulunduğu sistem:** Bilgi varlığı elektronik ortamda ise bulunduğu sistem bilgisi (fiziksel varlıklar kodu) verilmelidir.
- i. Bulunduğu yer:** Varlığın lokasyonu bina, kat, oda, (varsa dolap) belirtecek şekilde verilmelidir. Elektronik ortamdaki bilgi varlıklarında sistemin bulunduğu lokasyon bilgisi verilebilir.

5.4.2.1. Yazılım Varlıkları

Her birim kendi sorumluluğunda olan yazılım varlıklarını belirleyerek envantere kaydetmelidir. Yazılım dışarıdan temin edilmiş olabileceği gibi, kurum içerisinde geliştirilmiş olabilir. Envanterde yer alan alanların açıklaması aşağıda belirtilmiştir.

- a. Varlık kod:** Varlık kod numarası verilmelidir.
- b. Tanımı:** Varlığın tanımı özet olarak yazılmalıdır. Yazılım varlığının çalıştırılması için gerekli ortam bilgileri de verilmelidir.
- c. Varlık sorumlusu 1:** Yazılım varlığının sorumlusu belirtilmelidir. Bu kişi varlığın yaratıcısı olabileceği gibi, varlığa erişmesi gerekenleri yetkilendirme kararını veren ve varlık üzerinde yapılması gereken işlerde onay alınması gerekli kişi de olabilir.
- d. Varlık sorumlusu 2:** Varlık sorumlusu 1' e ulaşamadığı durumlarda varlıktan sorumlu olan yedek ikinci kişi adı verilmelidir.
- e. Değer Sınıflandırması:** Yazılım varlığının Kurum içerisindeki değeri; bu Varlık Belirleme, Sınıflandırmaya Etiketleme Prosedürü' nün Varlık Sınıflandırması başlığında verilen kategorilere uygun olarak belirlenmelidir. Varlığın değeri tespit edilirken; bu varlık üzerinde değişiklik olursa ya da varlık kaybedilirse yaşanacak sıkıntılar, bunun iş devamlılığına ya da sistemlere etkisi, bu sıkıntıların giderilmesi için gerekli kaynak gibi unsurlar göz önüne alınmalıdır.
- f. Kullanılan sistem:** Yazılım varlığının kullanıldığı sistemler yazılmalıdır. Geliştirilen (kodlaması devam eden) uygulama yazılımları için kullanılması planlanan sistem adı bilgisi verilmelidir.
- g. Bulunduğu sistem:** Yazılım varlığının kurulmak için bulunduğu sistemin kodu yazılmalıdır. Yine yazılımın kaynak kodu varsa kaynak kodunun bulunduğu sistem bilgisi (fiziksel varlık kodu) eklenmelidir.
- h. Bulunduğu yer:** Yazılımın lisansının, kurulum cdleri, source kodunun korunduğu yer (bina, kat, oda) yazılmalıdır. Elektronik ortamdaki bilgi varlıklarında sistemin bulunduğu lokasyon bilgisi verilebilir.

5.4.2.2. Fiziksel Varlıklar

Her birim kendi sorumluluğunda olan kritik fiziksel varlıkları belirleyerek envantere kaydetmelidir.

Envanter tablosunda yer alan fiziksel varlıklar için aşağıdaki alanlardaki bilgiler girilmelidir. Bu alanlardan bazıları boş bırakılabilir. Örneğin d) diğer teknik ekipmanlar alt kategorisinde ip-makine adı bilgisi boş olacaktır; fakat c) manyetik kayıt ortamları için mümkünse bu ortamda hangi makinenin bilgileri yer alıyorsa onun ip/makine adı bilgisi girilmelidir, Marka model kısmına ise kayıt ortamının marka ve modeli girilmelidir.

- a. Varlık kod:** Varlık kod numarası verilmelidir.
- b. Seri numarası:** Makinenin seri numarası girilmelidir.
- c. IP-makine adı:** Makinenin ip ve ad bilgileri girilmelidir.
- d. Marka:** Makinenin marka bilgisi girilmelidir.
- e. Model:** Makinenin model bilgisi girilmelidir.
- f. Tanımı:** Varlığın tanımı özet olarak yazılmalıdır. Varlığın kullanım amacı, hangi sistemin içinde olduğu, diğer hangi sistemlerle bağlantıda olduğu gibi bilgileri yazılmalıdır.
- g. Alt kategori:** Aşağıdaki alt kategorilerden uygun olanın harfi belirtilmelidir. Fiziksel varlığının bu alt kategorilerde belirtilen gruplar dışında değerlendiriyorsanız (d) harfini kullanabilirsiniz ya da eğer gerekiyorsa bu alt kategorilere kendi alt kategorinizin harfini de ekleyebilir ve kullanabilirsiniz (Bu durumda ilgili açıklama notu yazılmalıdır).

- a. Bilgisayar ekipmanları (pc, server, mainframe, diz üstü bilgisayarlar, modemler vb.);
- b. İletişim ekipmanları (yönlendirici, telefon, faks vb.);
- c. Manyetik kayıt ortamları (teyp, kartuş, disket, disk, cd vb.);
- d. Diğer teknik ekipmanlar (Yukarıdaki alt kategoriler dışında bulunan fiziksel varlıklardır.
- e. Güç kaynakları, adaptör, havalandırma üniteleri gibi);
- h. **Varlık sorumlusu 1:** Varlıkla ilgili yetkili kişi adı. Bu varlığın erişim yetkilendirmesine karar veren ve varlık üzerinde yapılması gereken işlerde onay alınması gerekli kişi de olabilir.
- i. **Varlık sorumlusu 2:** Varlık sorumlusu 1' e ulaşılamadığı durumlarda varlıktan sorumlu olan yedek ikinci kişi adı verilmelidir.
- j. **Değer Sınıflandırması:** Fiziksel varlığın Kurum içerisindeki değeri; bu Varlık Belirleme, Sınıflandırma ve Etiketleme Prosedürü' nün Varlık Sınıflandırması başlığında verilen kategorilere uygun olarak belirlenmelidir. Varlığın değeri tespit edilirken; bu varlık üzerinde değişiklik olursa ya da varlık kaybedilirse yaşanacak sıkıntılar, bunun iş devamlılığına ya da sistemlere etkisi, bu sıkıntıların giderilmesi için gerekli kaynak gibi unsurlar göz önüne alınmalıdır.
- k. **Bulunduğu sistem:** Fiziksel varlığın ait olduğu sistem adı eklenmelidir.
- l. **Bulunduğu yer:** Fiziksel varlığın lokasyonu (bina, kat, oda) yazılmalıdır.

Fiziksel varlıklar olarak (c) ve (d) alt kategori grubu için envanter tablosunda "fiziksel varlık-diğer" çalışma sayfası doldurulmalıdır. Bu çalışma sayfasında bulunduğu sistem kısmı hariç yukarıdaki bilgiler envantere kaydedilecektir.

6. YETKİ PROSEDÜRÜ

6.1. Kapsam ve Uygulama

Bu prosedür kurumun bütün çalışanları, sözleşmelileri ve **ÖZEL SALİHLİ GÜVEN SAĞLIK HİZMETLERİ A.Ş.** adı altında çalışan bütün kişiler için geçerlidir. Aynı zamanda **ÖZEL SALİHLİ GÜVEN SAĞLIK HİZMETLERİ A.Ş.** 'nin sahip olduğu ve kiraladığı bütün cihazlar içinde geçerlidir.

- **ÖZEL SALİHLİ GÜVEN SAĞLIK HİZMETLERİ A.Ş.** sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere ve hangi bilgilere erişeceği görev tanımları çerçevesinde belirlenmiş yetkilere göre ilgili bölüm sorumlusu ve/veya müdürü onayı ile BGYS Yönetim Temsilcisine bildirilir. BGYS Yönetim Temsilcisi bu bilgi ile erişim yetkilerini programlar ve sistem üzerinde tanımlar.
- **ÖZEL SALİHLİ GÜVEN SAĞLIK HİZMETLERİ A.Ş.** i tüm çalışan ve ziyaretçilerin erişebileceği fiziki alanlar Yetki Seviyeleri Alanları belirtilmiştir.
- Program kaynak koduna erişim sadece BGYS Yönetim Temsilcisinin yetkisi ve sorumluluğundadır. BGYS Yönetim temsilcisi kaynak koduna erişim ihlal olaylarını engellemek için gerekli kontrolleri yapmak ve tedbirleri almak konusunda yetkili ve sorumludur.
- **ÖZEL SALİHLİ GÜVEN SAĞLIK HİZMETLERİ A.Ş.** sistemlerine ve **ÖZEL SALİHLİ GÜVEN SAĞLIK HİZMETLERİ A.Ş.** adına kamu kurumlarına veya özel kuruluşların veri tabanına erişecek tüm kullanıcıların erişim yetkileri imza sirküplerinde ya da yetkilendirme yazısında tanımlanmıştır. Kimlik doğrulama yöntemi Parola Oluşturma ve Kullanım Prosedürü'nde tanımlanmıştır.
- Kullanıcılara açılacak mail hesapları, kullanım şartları ve hesabın kapatılması E-Posta Yönetimi prosedüründe belirtilmiştir.
- **ÖZEL SALİHLİ GÜVEN SAĞLIK HİZMETLERİ A.Ş.** bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veri tabanları, işletim sistemleri ve log-on olarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkiler Tüm kurumsal sistemler üzerindeki kullanım hakları (kullanıcıların kendi sistemlerine yönelik olarak birbirlerine verdikleri haklar) programlar üzerinde ve BGYS
- Yönetim tarafından kontrol altında tutulur ve düzenlenir.
- Erişim ve yetki seviyelerinin güncelliği BGYS Yönetim temsilcisi ve Kalite Yönetim Temsilcisi tarafından sistemsel değişiklik, fiziki alan değişikliği ve personel değişiklikleri durumunda gözden geçirilir ve güncellenir.
- Teçhizat, bilgi veya yazılım BGYS Yönetim Temsilcisi ve / veya Genel Müdür onayı olmaksızın kuruluş dışına çıkarılamaz.
- Depo giriş / çıkış kontrollü olarak yapılmaktadır.

Gözetimsiz kullanılacak teçhizatın sorumluluğu, teçhizatın sahibindedir. Teçhizatın sahibi gerekli güvenlik önlemlerini almakla yükümlüdür.

7. ACIL DURUM YÖNETİM PROSEDÜRÜ

Acil durum sorumluları atanmıştır. Yetki ve sorumlulukları belirlenmiş ve dokümente edilmiştir. Acil durumlarda kurum içi işbirliği gereksinimleri tanımlanmıştır.

Acil durumlarda sistem kayıtları incelenmek üzere saklanmakta ve kayıtlar rutin olarak kontrol edilmektedir.

Güvenlik açıkları ve ihlallerinin rapor edilmesi için kurumsal bir mekanizma oluşturulmuştur.

Yaşanan acil durumlar sonrası politikalar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilmektedir.

Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulmakta ve bu bildirim süreçleri tanımlanmış şekildedir.

Acil durum kapsamında değerlendirilen olaylar aşağıda farklı seviyelerde tanımlanmıştır:

- Seviye A: Bilgi kaybı. Kurumsal değerli bilgilerin yetkisiz kişilerin eline geçmesi, bozulması, silinmesi.
- Seviye B: Servis kesintisi. Kurumsal servislerin kesintisi veya kesintisine yol açabilecek durumlar.
- Seviye C: Şüpheli durumlar. Yukarıda tanımlı ilk iki seviyedeki duruma sebebiyet verebileceğinden şüphe duyulan ancak gerçekliği ispatlanmamış durumlar.

Her bir seviyede tanımlı acil durumlarda karşılaşılabilecek riskler, bu riskin kuruma getireceği kayıplar ve bu riskler oluşmadan önce ve oluşuktan sonra hareket planları tanımlanmalı ve dokümente edilmektedir.

Acil durumlarda bilgi güvenliği yöneticisine erişilmeli, ulaşılamadığı durumlarda koordinasyonu sağlamak üzere önceden tanımlanmış ilgili yöneticiye bilgi verilmektedir ve zararın tespit edilerek süratle daha önceden tanımlanmış felaket kurtarma faaliyetleri yürütülmektedir.

Bilgi güvenliği yöneticisi tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmek üzere ilgili makamlara iletilmektedir.

Olayın türü ve boyutuna göre emniyet veya diğer kurumlara başvurmak gerekebilir. Bu özel olaylar (hırsızlık vb.), başvurulacak kurumlar, başvuru şekli (telefon, dilekçe vb), başvuruyu yapacak kurum yetkilisi önceden belirlenmiştir ve dokümente edilmiştir.

8. BİLGİ GÜVENLİĞİ GÖZDEN GEÇİRME PROSEDÜRÜ

Bilgi Güvenliği gözden geçirme prosedürü, yılda bir periyodik gözden geçirilmelidir. Bunun dışında sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra da gözden geçirilmeli ve herhangi bir değişiklik gerekiyorsa Bilgi Güvenliği Yöneticisi eşliğinde ilgili kişilerce düzeltilmelidir.

- Gözden geçirme sonrasında belirlenen sebeplerden dolayı değişiklik gereken durumlarda bu işlem Bilgi Güvenliği Yöneticisi eşliğinde ilgili kişilerce düzeltilmelidir.
- Prosedürün etkinliği, kaydedilmiş güvenlik arızalarının yapısı, sayısı ve etkisi aracılığıyla gözlemlenmelidir.
- Prosedürün güncelliği teknolojik değişimlerin etkisi vasıtasıyla gözlemlenmelidir.
- Prosedürün güncelliği değişen personelle birlikte gözden geçirilmeli, yeni personelin katılımı sağlanmalıdır.
- Prosedürün, sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra gözden geçirilmelidir.
- Yasal değişimler durumunda gözden geçirilmelidir.
- İyileştirme veya risk sebepli haller tespitinde gözden geçirilmelidir.
- Prosedür üzerinde yapılan gözden geçirme sonrası değişik gereken hallerde değişim versiyon değişimi olarak kayıt altına alınmalı ve her versiyon üst yönetim tarafından onaylanmalıdır.

9. VERİ ANALİZİ PROSEDÜRÜ

9.1. Prosedür Detayı

Geçmiş verilerin değerlendirilmesi ve geleceğe yönelik planlamaların ve iyileştirme çalışmalarının yapılmasında yararlanılacak istatistiksel verilerin oluşturulmasını sağlamak için veriler Doküman ve Kayıtların Kontrolü Prosedürüne göre arşivlenir.

Kalite ve Bilgi Güvenliği Politikası ve İş Sürekliliği Politikasının gerçekleştirilmesini ve müşteri ihtiyaç ve beklentilerinin karşılanmasını sağlayacak yıllık hedefler belirlenir.

Analizler sonucu elde edilen bilgilerle sürekli iyileştirme sağlanır ve gerekiyorsa yeni kalite hedefleri belirlenir.

Kalite Yönetim Sistemimizde yapılacak iyileştirme ve yeni kalite hedefleri için;

- Müşteri memnuniyeti anketleri,
- İç tetkik raporları,
- Düzeltici/önleyici faaliyetler,
- Eğitim kayıtları,
- Bireysel öneri kayıtları,
- Gerekli görülen diğer kayıtlar ile ilgili analizler yapılır.

Analizler, aşağıdaki tabloya göre Kalite Yönetim Temsilcisi tarafından hazırlanır. Ayrıca bu tablodaki analizlerin dışında Kalite Yönetim Temsilcisi tarafından veri analizi istenebilir.

Kullanılacak doküman, Doküman ve Kayıtların Kontrolü Prosedürü' dür.

Sıra No	Analizi Yapılan	Kullanılan Doküman	Uygulanan Yöntem	Periyot
3	Müşteri memnuniyetinin anket soruları bazında değerlendirilmesi	Müşteri Memnuniyeti Anketi	Tanımlayıcı Analizler	Yılda bir kez
2	Müşteri şikâyetlerinin sayısının ve giderilme oranlarının aylara göre değerlendirilmesi	Müşteri Şikâyetleri ve Bireysel Öneri Kayıtları	Çubuk Grafik	6 ayda bir
3	Müşteri şikâyetlerinin konularına göre değerlendirilmesi	Müşteri Şikâyetleri ve Bireysel Öneri Kayıtları	Çubuk Grafik	6 ayda bir
4	Çalışan önerilerinin sayısının ve giderilme oranlarının aylara göre değerlendirilmesi	Bireysel Öneri Kayıtları	Çubuk Grafik	Yılda bir
5	Düzeltici ve önleyici faaliyet taleplerinin aylara göre sayısının ve kapatılma oranlarının değerlendirilmesi	Düzeltici Faaliyet, Önleyici Faaliyet, İç Tetkik Düzeltici Faaliyet ve İç Tetkik Önleyici Faaliyet Formları	Çubuk Grafik	6 ayda bir

9.2. Analiz Periyotlarına Göre Performans Kriterleri

- Müşteri memnuniyeti anketleri yılda bir kez yapılır. İlgili birim tarafından hazırlanan anketlerin, Analiz sonuçları Yönetimin Gözden Geçirmesi Toplantısında görüşülür
- Müşteri şikâyetlerine ait veriler, 6 aylık dönemleri kapsayacak şekilde analiz edilir. Kalite Yönetim temsilcisi, Yönetimin Gözden Geçirme Toplantısından 1 hafta önce ilgili birimlerden kendilerine ulaşan Müşteri şikâyetlerine ilişkin bilgileri ister. Birimler, talep edilen periyoda ait verileri Kalite Yönetim Temsilcisine iletir. Analiz sonuçları, dönemleri izleyen Yönetimin Gözden Geçirme Toplantısında görüşülür.
- Çalışan önerilerine ait analizler, Yönetimin Gözden Geçirmesi Toplantısında görüşülmek üzere

yapılır.

- Çalışanların ihtiyaçlarının değerlendirilmesine ilişkin Çalışan Memnuniyeti Anketleri yılda iki kez yapılır. Kalite Yönetim Temsilcisi tarafından hazırlanan anketler, tüm birimlere gönderilir. Elde edilen veriler Kalite Yönetim Temsilcisine iletilir. Analiz sonuçları takip eden ilk Yönetimin Gözden Geçirmesi Toplantısında görüşülür.
- Düzeltici/Önleyici faaliyetlere ait analizler 6 aylık dönemlerini kapsayacak şekilde yapılır. Analiz sonuçları takip eden ilk Yönetimin Gözden Geçirmesi Toplantısında görüşülür.
- Birim hedeflerine ve yönetimin kalite hedeflerine ait analizler yıllık dönemlerini kapsayacak şekilde yapılır. Analiz sonuçları bir performans raporu ile takip eden ilk Yönetimin Gözden Geçirmesi Toplantısında görüşülür.

10. YÖNETİMİN GÖZDEN GEÇİRME PROSEDÜRÜ

10.1. Gözden Geçirme Periyotları

ÖZEL SALİHLİ GÜVEN SAĞLIK HİZMETLERİ A.Ş. en az yılda 2 kez BGYS'nin Sgözden geçirilmesi amacıyla Yönetimi Gözden Geçirme Toplantısı yapılır. Bu toplantı iç tetkiklerin yapılmasından sonraki 1 ay içinde yapılmalıdır. Toplantıya Genel Müdür başkanlık eder. Toplantıya Direktörler ve Bölüm Müdürleri katılır. Toplantının raportörlüğünü Yönetim Temsilcisi yapar.

10.2. Toplantının Gündemi

Yönetimin Gözden Geçirilmesi toplantısında ISO 27001 standardının 7. maddesine göre yer alan konu başlıkları değerlendirilir.

10.3. Toplantının Girdileri

BGYS denetimleri ve gözden geçirmelerinin sonuçları, İlgili taraflardan edinilen geri bildirimler,
Kuruluşta BGYS'nin performansını ve etkinliği artırmak için kullanılabilecek teknikler, ürünler ya da prosedürler,
İyileştirici ve düzeltici faaliyetlerin durumu,
Önceki risk değerlendirmede uygun olarak ifade edilmeyen açıklıklar ya da tehditler,
Etkinlik ölçümlerinin sonuçları,
Önceki yönetim gözden geçirmelerinden izleme eylemleri,
BGYS'yi etkileyebilecek herhangi bir değişiklik İyileştirme için öneriler

10.4. Toplantının Çıktıları BGYS etkinliğini iyileştirme.

Risk değerlendirme ve risk işleme planını güncelleştirme.
Gerektiğinde, BGYS üzerinde etkisi olabilecek iç ya da dış olaylara karşılık vermek için bilgi güvenliğini etkileyen prosedür ve kontrol değişiklikleri, aşağıdakilere değişiklikleri içerir:
İş gereksinimleri, Güvenlik gereksinimleri,
Mevcut iş gereksinimlerini etkileyen iş prosesleri,
Düzenleyici ya da yasal gereksinimler,
Anlaşma yükümlülükleri ve
Risk seviyeleri ve/veya risk kabul kriterleri.
Kaynak ihtiyaçları.
Kontrollerin etkinliğinin nasıl ölçüldüğünü iyileştirme.

10.5. Toplantının Kayıt Altına Alınması

Toplantıda görüşülen konular ve alınan kararlar Yönetim temsilcisi tarafından Tutanak Formu ile kayıt altına alınır. Elde edilen kayıtlar Dokümanların ve Kayıtların Kontrolü Prosedürüne göre muhafaza edilir.

11. RİSK DEĞERLENDİRME PROSEDÜRÜ

11.1. Tanımlar

- **Artık Risk:** Risk işlemeden sonra kalan risk,
- **Riskin Kabulü:** Bir riski kabul etme kararı,
- **Risk Analizi:** Kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımı,

- **Risk Değerlendirme:** Riskin önemini tayin etmek amacıyla tahmin edilen riskin verilen risk kriterleriyle karşılaştırılması prosesi,
- **Risk Yönetimi:** Bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler,
- **Risk İşleme:** Riski değiştirmek için alınması gereken önlemlerin seçilmesi ve uygulanması prosesi,
- **Varlık:** Kuruluş için değerli olan herhangi bir şey.

11.2. Sorumluluklar ve Uygulama

Firmada varlıklara karşı ortaya çıkabilecek riskleri belirlemek ve risklerin elimine edilmesi için gereken çalışmanın yapılması maksadıyla Risk Analiz ekibi kurulur, bu ekibin lideri Bilgi Güvenliği Yönetim Temsilcisidir. Bu ekipte diğer görev alanlar ise ilgili birimlerin sorumlularıdır.

Risk analizi süresince çalışanlar gerekli noktalarda yardımcı olacaklardır. Çalışanlar daha sonra Risk Değerlendirme ekibi ile birlikte geliştirme ve iyileştirme prosesine katkıda bulunacaklardır. Risk değerlendirme ile ilgili tüm sorumluluklar aşağıda detaylı olarak açıklanmaktadır.

Risk yönetimi kapsamında kurumdaki tüm çalışanların bir rolü bulunmaktadır. BT risk yönetimindeki roller de bu genel çerçeve içinde değerlendirilmektedir. Bu bölümde, kurum içinde risk yönetiminde değişik grupların üstlenebilecekleri sorumluluklar ve roller incelenmektedir.

11.2.1. Üst Yönetimin Sorumlulukları

- Risk yönetiminin kurum stratejilerine entegrasyonu
- Risk yönetiminin yakından izlenip gerekli desteğin sağlanması
- Risk yönetim çalışmalarının etkililiğinin sorgulanması
- Risk yönetimi eğitimlerinin sağlanması
- Risk yönetiminin daha sistematik hale getirilmesi için gerekli yatırımların yapılması

11.2.2. Birim Yönetimlerinin Sorumlulukları

- Risk yönetim stratejilerinin kurum içinde uygulanmasının sağlanması
- Risklerin önceliklendirilmesi
- Risk yönetiminin performansının değerlendirilmesi
- Risk yönetimi prensiplerinin karar verme sürecinin bir parçası haline getirilmesi
- Risk yönetiminde yeterli planlama, gerçekleştirme, eğitim, kontrol, izleme ve dokümantasyon çalışmasının yapılması

11.2.3. Risk Yönetimi Uzmanlarının Sorumlulukları

- Risk yönetimi ile ilgili öneri, yönlendirme ve yardımların tüm kurumun risk politikalarıyla ve üst yönetimin hedefleri doğrultusunda yapılması
- Birimlerin riskleri belirlemelerine ve risk değerlendirmesi yapmalarına yardımcı olunması
- Birimlere, daha etkili bir risk yönetimi için yardımcı araçlar sağlanması veya bu tür araçların tasarım ve gerçekleştirimine yardımcı olunması

11.2.4. İç Denetim ve Kontrol Uzmanlarının Sorumlulukları

- Risk Yönetimi kuralları çerçevesinde üst yönetime birimlerin performansı konusunda raporlama yapılması

11.2.5. Tüm Çalışanların Sorumlulukları

- Risk yönetimi konularına karşı ilgili ve bilgili olunması
 - İşlerin risk değerlendirmesi çerçevesinde yürütülmesi
 - Bilgi ve doküman sağlanması
- Firmamızda risk değerlendirme aşağıdaki şekilde yapılacaktır.

11.3. Risk Etki Oranı Hesaplaması

Risklerin önceliklerinin belirlenmesinde; risk etki oranı hesaplaması kullanılmalıdır. Bu hesaplamada aşağıdaki değerlendirmeler yer alacaktır:

ŞİDDET TABLOSU

1	ÇOK HAFİF	İş saati kaybı yok. Fiziksel zarar yok. Data kaybı yok. Yetkisiz erişim yok.
2	HAFİF	İş günü kaybı yok. Fiziksel zarar, kalıcı etkisi yok. Data kaybı önemsiz. Yetkisiz erişim yok.
3	ORTA	İş ve data kaybı orta seviyede olup, müdahale gerektiren. Yetkisiz erişim ihtimali, Erişim kontrolü yapılmalı.
4	CİDDİ	İş sürekliliğini etkileyecek. Fiziksel ve data kaybı müdahale gerektiren. Yetkisiz erişim tespiti. Güvenlik ihlali önemli seviyede
5	ÇOK CİDDİ	Uzun süreli iş kaybı. Fiziki varlık kaybı. Geri dönülemez data kaybı. Yetkisiz erişim tespiti. Güvenlik ihlali geri dönülemez yüksek seviyede.

BİR OLAYIN GERÇEKLEŞME OLASILIĞI

OLASILIK		DERECELENDİRME BASAMAKLARI
1	ÇOK KÜÇÜK	HEMEN HEMEN HİÇ
2	KÜÇÜK	ÇOK AZ (YILDA 1 KEZ), SADECE ANORMAL DURUMLARDA
3	ORTA	AZ (YILDA BİR KAÇ KEZ)
4	YÜKSEK	SIKLIKLA (AYDA BİR)
5	ÇOK YÜKSEK	ÇOK SIKLIKLA (HERGÜN, HAFTADA BİR) NORMAL ÇALIŞMA ŞARTLARINDA

ISO 9001:2015 KALİTE YÖNETİM SİSTEMİ RİSK MATRİKSİ

5x5 MATRİS YÖNTEMİ RİSK ANALİZİ RİSK DERECELERİ

OLASILIK	OLUŞABİLECEK ZARARIN ŞİDDETİ				
	1 ÇOK HAFİF	2 HAFİF	3 ORTA	4 CİDDİ	5 ÇOK CİDDİ
1 ÇOK AZ	1 İHMAL EDİLEBİLİR	2 DÜŞÜK	3 DÜŞÜK	4 DÜŞÜK	5 DÜŞÜK
2 AZ	2 DÜŞÜK	4 DÜŞÜK	6 DÜŞÜK	8 ORTA	10 ORTA
3 ORTA	3 DÜŞÜK	6 DÜŞÜK	9 ORTA	12 ORTA	15 YÜKSEK
4 YÜKSEK	4 DÜŞÜK	8 ORTA	12 ORTA	16 YÜKSEK	20 YÜKSEK
5 ÇOK YÜKSEK	5 DÜŞÜK	10 ORTA	15 YÜKSEK	20 YÜKSEK	25 TOLERE EDİLEMEZ

BİLGİ VARLIK DERECE		
Derece	Puan	Tanım
Yüksek	3	Bu varlıklar, Kurum için yüksek değer taşımaktadır. Kaybı ya da zarar görmesi Kurumun faaliyetlerinin devamlılığında şiddetli etkiye sebep olabilir.
Orta	2	Bu varlık, değerlidir ve yerine başka varlık kullanılabilir, kaybı ya da zarar görmesi durumunda, Kurum karlılığında ani etkilere sebep olabilir.
Düşük	1	Bu varlığın, iş devamlılığında ekonomik bir değeri yoktur ve düşük bir maliyetle yeri doldurulabilir.

SO 27001 ve ISO 22301 RİSK MATRİKSİ					
OLASILIK	ÇOK CİDDİ 5	CİD D İ 4	OR T A 3	HAFİ F 2	ÇOK HAFİ F 1
ÇOK YÜKS EK 5	YÜKS EK 225	YÜKS EK 180	YÜKS EK 135	ORT A 90	DÜŞ ÜK 45
YÜKS EK 4	YÜKS EK 180	YÜKS EK 144	ORT A 108	ORT A 72	DÜŞ ÜK 36
ORT A 3	YÜKS EK 135	ORT A 108	OR T A 81	DÜŞ ÜK 54	DÜŞ ÜK 27
KÜÇ Ü K 2	ORT A 90	ORT A 72	DÜŞ ÜK 54	DÜŞ ÜK 36	DÜŞ ÜK 18
ÇOK	DÜŞ	DÜŞ	DÜŞ	DÜŞ	DÜŞ

KÜÇ ÜK 1	ÜK 45	ÜK 36	ÜK 27	ÜK 18	Ü K 3
-------------	----------	----------	----------	----------	-------------

Risk= Varlık Deęeri * [(Olasılık Deęeri* Gizlilik)+(Olasılık Deęeri* Bütünlük)+(Olasılık Deęeri* Eriřilebilirlik)]

ERİŞEBİLİRLİK	GİZLİLİK	BÜTÜNLÜK
ÇOK YÜK SEK 5	ÇOK YÜK SEK 5	ÇOK YÜK SEK 5
YÜKS EK 4	YÜKS E K 4	YÜKS EK 4
OR TA 3	OR TA 3	OR TA 3
KÜÇ Ü K 2	KÜÇ Ü K 2	KÜÇ Ü K 2
ÇOK KÜÇ ÜK 1	ÇOK KÜÇ ÜK 1	ÇOK KÜÇ ÜK 1

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.

EYLEM MATRİSİ

SONUÇ	EYLEM
135-225	KABUL EDİLEMEZ RİSK Bu risklerle ilgili hemen çalışma yapılmalı.
72-134	DİKKATE DEĞER RİSK Risklere mümkün olduğunca çabuk müdahale edilmeli.
3-71	KABUL EDİLEBİLİR RİSK Acil tedbir gerekmebilir.