


	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS) POLİTİKASI	Doküman Kodu: EY.BG.POL.01
		Versiyon: 1
		Yayın Tarihi: 26.02.2019
		Sınıfı: Kurum İçi




BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS) POLİTİKASI

 ABALIOĞLU <small>SAĞIŞAL ÜRETİM A.Ş.</small>	 Lezita <i>Balık</i>	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS) POLİTİKASI	Doküman Kodu: EY.BG.POL.01
			Versiyon: 1
			Yayın Tarihi: 26.02.2019
			Sınıfı: Kurum İçi

 	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS) POLİTİKASI	Doküman Kodu: EY.BG.POL.01
		Versiyon: 1
		Yayın Tarihi: 26.02.2019
		Sınıfı: Kurum İçi

İçindekiler

DOKÜMAN KONTROLÜ.....	Error! Bookmark not defined.
1. GİRİŞ	4
2. Abalioğlu Tarımsal ve Lezita Balık A.Ş'İN BİLGİ GÜVENLİĞİ YAKLAŞIMI	4
3. BGYS'İN AMAÇ VE HEDEFLERİ	4
4. BGYS POLİTİKASI	5
5. BGYS PERFORMANS GÖSTERGELERİ	6
6. BİLGİ GÜVENLİĞİ ORGANİZASYONU	8
6.1. Bilgi Güvenliği Yönlendirme Kurulu (Güvenlik Kurulu)	8
6.2. Genel Müdür	8
6.3. Bilgi Güvenliği Yöneticisi.....	8
6.4. İş Birimi Sorumluları	8
7. İÇ VE DIŞ TARAFLARIN BEKLENTİLERİ	8
8. EKLER	Error! Bookmark not defined.
9. KISALTMALAR VE TANIMLAR.....	Error! Bookmark not defined.

	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS) POLİTİKASI	Doküman Kodu: EY.BG.POL.01
		Versiyon: 1
		Yayın Tarihi: 26.02.2019
		Sınıfı: Kurum İçi

1. GİRİŞ

Bilgi Güvenliği Yönetim Sistemi (BGYS) Politikası'nın amacı, Abalioğlu Tarımsal ve Lezita Balık A.Ş'in BGYS Kapsam Dokümanı'nda belirtilen kapsamdaki şirketler, lokasyonlar, varlıklar, süreçler ve personel için şirket stratejileri doğrultusunda BGYS'ye yönelik anlayışını aktarmak, BGYS amaç ve hedeflerini kayıt altına almak ve bu anlayışın uygulanması için yapılması gerekenleri aktarmaktır.

Dokümanda önce Abalioğlu Tarımsal ve Lezita Balık A.Ş'in bilgi güvenliği yaklaşımı özetlenmiş, BGYS amaçları listelenmiş ve bunlara ulaşmak amacıyla yürütülen faaliyetlerin performansının takibi için belirlenmiş olan göstergelere yer verilmiştir.

Devamında BGYS politikası özetlenmiş ve bu politikanın uygulanmasını sağlayacak organizasyon yapısı açıklanmıştır.

2. ABALIOĞLU TARIMSAL A.Ş ve LEZİTA BALIK A.Ş'İN BİLGİ GÜVENLİĞİ

YAKLAŞIMI

Değerlerimize bağlılığımız sürecinde özellikle güvenilirlik ve operasyonel mükemmellik ilkelerimizle bağlantılı olarak, kurumumuz bünyesinde bir Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmuş bulunuyoruz.

Müşterilerimizle, iş ortaklarımızla, çalışanlarımızla, kamu kurumları, kanun koyucular ve düzenleyiciler ile karşılıklı güvene dayanan ilişkimizin temelini BGYS ile daha da güçlendiriyoruz. Bu amaçla, bilgi güvenliğinin sağlanması, güvenlik süreçlerinin iyileştirilmesi ile en üst seviyede verimliliğe en güvenli şekilde ulaşmayı hedefliyoruz.

3. BGYS'NİN AMAÇ VE HEDEFLERİ

Abalioğlu Tarımsal ve Lezita Balık A.Ş bünyesinde uygulanmakta olan bilgi güvenliği yaklaşımının temel amaçları, kurumsal bilişim sistemleri ve endüstriyel kontrol sistemlerinin herhangi bir aksama olmadan faaliyet göstermesi ve ihtiyaçlar doğrultusunda;

- Abalioğlu Tarımsal ve Lezita Balık A.Ş bilişim sistemlerinde saklanan ve işlenen bilginin **yetkisiz ifşasının engellenmesi, bir başka deyişle bilgi güvenliğinin GİZLİLİK unsurunun tesis edilmesi,**
- Bilginin kazara ya da yetkisiz kişiler tarafından kasıtlı olarak **değiştirilmeye veya silinmeye karşı korunması, bir başka deyişle bilgi güvenliğinin BÜTÜNLÜK unsurunun tesis edilmesi,**
- Bilginin gerek duyulduğunda yetkili kişiler tarafından **erişilebilir olmasının sağlanması, bir başka deyişle bilgi güvenliğinin ERİŞİLEBİLİRLİK unsurunun tesis edilmesi** olarak ifade edilmiştir.

Bu doğrultuda kurulmuş olan BGYS'nin hedefleri şu şekilde belirlenmiştir:

	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS) POLİTİKASI	Doküman Kodu: EY.BG.POL.01
		Versiyon: 1
		Yayın Tarihi: 26.02.2019
		Sınıfı: Kurum İçi

- Bilgi güvenliğine ilişkin hedefleri iş hedefleri ile uyumlu hale getirerek aynı zamanda iş stratejisinin bir parçası olmalarını sağlamak,
- Başta müşteri bilgileri olmak üzere, tüm kritik şirket bilgilerinin ihtiyaçlara uygun ve yönetilebilir bir şekilde korunmasını sağlamak,
- Kurumun bilgi iletişimde bulunduğu iç ve dış tarafların beklentilerinin anlaşılması ve karşılanması ve bu süreçte doğan bilgi güvenliği ile ilgili risklerin tespit edilerek kabul edilebilir seviyeye indirilmesini sağlamak,
- Tüm şirketi, paydaşları ve iş ortaklarını da içeren bir bilgi güvenliği anlayışını yerleştirmek,
- Sürekli değişen ve gelişen teknolojileri takip ederek, ISO 27001:2013 standardının gereklilikleri ile uyumlu, ölçülebilir, raporlanabilir ve denetlenebilir bir bilgi güvenliği yönetim sistemi kurmak,
- Kritik süreçlerin ve sistemlerin sürekliliğini sağlamak üzere uygun iş sürekliliği planlarını ve sistemlerini geliştirmek ve bu kapsamda bilgi güvenliği unsurlarının sürekliliğini sağlamak,
- Bilgi güvenliği ihlal ve zafiyetlerini etkin bir şekilde yönetmek, tekrarlamalarını engellemek adına gerekli aksiyonları almak,
- Abalioğlu Tarımsal ve Lezita Balık A.Ş'in tabi olduğu tüm kanun, mevzuat, yönetmelik, tebliğ, vb. düzenlemelerden kaynaklanan bilgi güvenliğine dair beklentileri karşılamak, bunların düzenli takibi ve iyileştirilmesi için takip mekanizmalarını kurmak.

4. BGYS POLİTİKASI

Abalioğlu Tarımsal ve Lezita Balık A.Ş yukarıda tanımlanan BGYS hedeflerine ulaşıp ulaşılmadığını izleyebilmek adına aşağıda belirtilen şekilde bir model uygulanmaktadır.



BGYS Yönetim Modeli

Yukarıda belirtilen BGYS hedeflerinin karşılanıp karşılanmadığı bu yönetim modeli gereğince ve aşağıda belirtilen unsurlarla değerlendirmeye tabi tutulur:

- Süreç bazlı hazırlanmış olan ve Ek-1 Bilgi Güvenliği Yönetim Sistemi Performans Ölçüm Listesi içerisinde tanımlanan performans ölçütleri yılda en az bir kere değerlendirilir.
- Yılda en az bir kere yapılan BGYS iç denetimleri ile tespit edilen aksaklıklara ilişkin düzeltici faaliyetlerin tespit edilmesi ve planlanması sağlanır.
- Gerekli durumlarda yapılan güvenlik ve sızma testleri ile kapsam dahilindeki süreçler, varlıklar, organizasyon ve bilgi sistemleri ile ilgili zafiyetlerin tespit edilmesi ve bunlara ilişkin iyileştirme çalışmalarının planlanması sağlanır.

	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS) POLİTİKASI	Doküman Kodu: EY.BG.POL.01
		Versiyon: 1
		Yayın Tarihi: 26.02.2019
		Sınıfı: Kurum İçi

- Tüm bu çalışmaların sonuçları Yönetim Gözden Geçirme Toplantısı'nda üst yönetime sunulur ve üst yönetimin BGYS performansı hakkında durum değerlendirmesi yapması sağlanır.

BGYS Politikası ve buna paralel olarak hazırlanmış olan Bilgi Güvenliği Politikaları, Abalioğlu Tarımsal ve Lezita Balık A.Ş kurumsal bilgi sistemlerinin ve endüstriyel kontrol sistemlerinin yönetimi faaliyetlerinin, bilgi güvenliği ile ilgili olan yasa ve yönetmelikler, kabul edilmiş iyi uygulamalar ve ISO 27001 gibi uluslararası standartlar ile uyumlu olmasını sağlamak için kılavuz niteliğini taşımaktadır.

BGYS ve Bilgi Güvenliği Politikaları kapsamında, bu politikalarda belirtilmiş olan yaklaşımların ve kontrollerin nasıl uygulanması gerektiğini anlatan bir Uygulanabilirlik Beyanı oluşturulmuştur.

Abalioğlu Tarımsal ve Lezita Balık A.Ş, çalışanlarının mahremiyetine saygı göstermeyi amaçlar. Bununla birlikte, çalışanların gerçekleştirdiği işlemleri ve Abalioğlu Tarımsal ve Lezita Balık A.Ş bilişim sistemlerini kullanarak çalışanlar tarafından saklanan, işlenen, iletilen veya üzerinde çalışılan bilgiyi denetleme hakkını saklı tutmaktadır.

Tüm bunların ışığında işletilen BGYS'ye ilişkin detaylı model ve akış genel itibarıyla Ek-2 ISO 27001 Tabanlı BGYS Modeli ve Akış Şeması'nda gösterilmiştir.

5. BGYS PERFORMANS GÖSTERGELERİ

BGYS amaçlarının ve hedeflerinin karşılanması ve karşılanma seviyelerinin ölçülmesi için aşağıdaki performans göstergeleri oluşturulmuş ve bunlar Ek-1 Abalioğlu Tarımsal ve Lezita Balık A.Ş BGYS Performans Ölçütleri Listesi'nde dokümente edilerek değerlendirilmektedir.


BGYS Hedef ve Performans Metrikleri

BGYS Hedefi	Performans Metrikleri
1) Bilgi güvenliğini iş hedefleri ile uyumlu hale getirerek aynı zamanda iş stratejisinin bir parçası olmasını sağlamak	<ul style="list-style-type: none"> Bilgi güvenliği politikalarına ve standartlarına yönelik düzenli aralıklar ile gözden geçirmelerin yapılması. Bilgi güvenliği süreçlerinin, Üst Yönetim seviyesinde görünür durumda olması, anlaşılması ve desteklenmesi.
2) Öncelikle müşteri bilgileri olmak üzere, tüm şirket bilgilerinin ihtiyaçlara uygun ve yönetilebilir bir şekilde korunmasını sağlamak	<ul style="list-style-type: none"> Local Admin yetkisi olan son kullanıcı bilgisayar sayısının istenilen düzeyde tutulması Satın alma öncesinde, tutulan veri tiplerine göre, güvenlik risk değerlendirmesi yapılması. Kurum yüksek değerli ya da gizli bilgilere erişme ihtiyacı olabilecek satıcıların tamamı için risk analizi yapılmasını ve %95'inde güvenlik beklentilerinin karşılanmasını bekler.
3) Kurumun bilgi iletişimde bulunduğu iç ve dış tarafların beklentilerinin anlaşılması ve karşılanması ve bu süreçte doğan bilgi güvenliği ile ilgili risklerin tespit edilerek kabul edilebilir seviyeye indirilmesini sağlamak	<ul style="list-style-type: none"> Kurumun bilgi iletişimde bulunduğu iç ve dış taraflar ve bu tarafların beklentilerinin anlaşılması ile beklentiler ile ilgili bilgi güvenliği risklerinin analiz edilerek kontrol altında tutulması.
3) Tüm şirketi, paydaşları ve iş	<ul style="list-style-type: none"> Bilgi güvenliği farkındalık eğitimlerinin kurum bünyesinde bulunan

 	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS) POLİTİKASI	Doküman Kodu: EY.BG.POL.01
		Versiyon: 1
		Yayın Tarihi: 26.02.2019
		Sınıfı: Kurum İçi

ortaklarını da içeren bir bilgi güvenliği anlayışını yerleştirmek	<p>personelere verilmesi.</p> <ul style="list-style-type: none"> Tüm personel tarafından, geçici personel de dahil olmak üzere gizlilik anlaşması imzalanması. Tedarikçiler ile yapılan sözleşmelerde, bilgi güvenliği ve gizlilik hükümlerine ilişkin değerlendirmelerin yapılması
5) Sürekli değişen ve gelişen teknolojileri takip ederek, ISO 27001:2013 standardının gereklilikleri ile uyumlu, ölçülebilir, raporlanabilir ve denetlenebilir bir bilgi güvenliği yönetim sistemi kurmak	<ul style="list-style-type: none"> Bilgi güvenliği metriklerinin Yönetim Kurulu'na ve Üst Yönetim'e yılda iki defa sunulması Sahibi olmayan uygulamalar için yetkili kullanıcı (jenerik) hesabı oluşturulmaması Açık riskler ile ilgili bir sahiplenme olması. Kurumda kritik risklerin %100'ünün sahibi olmalıdır. Bilgi güvenliğine ilişkin oluşturulmuş aksiyon planlarının takibinin yapılması. Düzeltici faaliyetlerin tümünün belirtilen tarih itibarıyla uygulamaya konması. Kurum çalışanlarının kullanmakta olduğu son kullanıcı sistemlerinde bulunan bilgi güvenliği uygulamalarının etkinliğinin değerlendirilmesi
6) Kritik süreçlerin ve sistemlerin sürekliliğini sağlamak üzere uygun iş sürekliliği planlarını ve sistemlerini geliştirmek ve bu kapsamda bilgi güvenliği unsurlarının sürekliliğini sağlamak	<ul style="list-style-type: none"> SAP ve SCADA sistemleri için erişilebilirlik oranı yıllık %99 olacak şekilde hedeflenmesi. Her yıl en az bir kere kurum çapında felaket kurtarma testi düzenlenmesi. Yedeği alınan sistemler için senede en az bir kere olmak üzere yedekten geri dönme testlerinin düzenlenmesi. Güvenlik zafiyeti kaynaklı sistem kesintilerinin sayısının minimumda tutulmasının hedeflenmesi.
7) Bilgi güvenliği ihlal ve zafiyetlerini etkin bir şekilde yönetmek, tekrarlamalarını engellemek adına gerekli aksiyonları almak	<ul style="list-style-type: none"> İç ya da dış nedenler ile gerçekleşen bilgi güvenliği olaylarının değerlendirilmesi ve süreçte iyileştirme ihtiyaçlarının belirlenmesi. Sistemlerde bulunabilecek olası güvenlik zafiyetlerinin durumlarının belirlenmesi ve süreçlerin iyileştirilmesinin hedeflenmesi. İş akdi sonlandırılan kurum çalışanlarının kullanıcı hesaplarının kapatılmasının değerlendirilmesi.
8) ABALIOĞLU TARIMSAL A.Ş VE LEZİTA BALIK A.Ş'in tabi olduğu tüm kanun, yönetmelik, tebliğ, vb. düzenlemelerden kaynaklanan bilgi güvenliğine dair beklentileri karşılamak, bunların düzenli takibi ve iyileştirilmesi için takip mekanizmalarını kurmak	<ul style="list-style-type: none"> Tüm yazılımların dönemsel lisanslarının ve anlaşmalarının tamamlanması. Yürürlükteki yasa ve yönetmeliklere tam uyumun sağlanması, yasalara ilişkin oluşacak herhangi bir uyumsuzluk durumunda ilgili aksiyonun alınması ve en üst seviyede takibin sağlanması.

Tüm bunların ışığında işletilen BGYS'ye ilişkin model ve akış genel itibarıyla Ek-2 ISO 27001 tabanlı BGYS modeli ve akış şemasında gösterilmiştir.

	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS) POLİTİKASI	Doküman Kodu: EY.BG.POL.01
		Versiyon: 1
		Yayın Tarihi: 26.02.2019
		Sınıfı: Kurum İçi

6. BİLGİ GÜVENLİĞİ ORGANİZASYONU

Abalioğlu Tarımsal ve Lezita Balık A.Ş bünyesinde bir bilgi güvenliği organizasyon yapısı tanımlanmıştır. Bu yapı düzenli olarak gözden geçirilir ve gerekli hallerde güncellenir. Organizasyon yapısındaki rol ve sorumluluklar tanımlanırken, mümkün olan her durum için görevler ayrılığı ilkesi benimsenir. Bu yapı ile birlikte, birbiriyle uyuşmayan roller aynı kişiye atanmaz.

6.1. Bilgi Güvenliği Yönlendirme Komitesi (Güvenlik Kurulu)

Raporlama Yaptığı Merc: Genel Müdür

Rolü: Abalioğlu Tarımsal ve Lezita Balık A.Ş nezdinde tüm birimlerin bilgi güvenliği ile ilişkili konularını tartışan ve çözen merkezi bir birim olarak görev alır. Kuruluş bünyesinde bilgi güvenliği ile ilgili politika ve prosedürlerin uygulanmasından sorumludur. Bilgi güvenliği ile ilişkili konularının tartışılması ve genel bilgi güvenliği stratejisinin kuruluş bazında koordineli ilerlemesinden de yükümlüdür.

Bilgi Teknolojileri, İK, Satın Alma, Hukuk gibi faaliyet gösteren tüm bölümlerin sorumluları ve Bilgi Güvenliği Yöneticisi'nden oluşur. Genel Müdür Yardımcısı bu kurulun doğal üyesidir.

6.2. Genel Müdür

Rolü: İş stratejileri ve güvenlik politikaları doğrultusunda Bilgi Güvenliği Yönetim Sistemi'ne yön verilmesi ve gerekli kaynakların tahsis edilmesinden sorumludur.

6.3. Bilgi Güvenliği Yöneticisi

Raporlama Yaptığı Merc: Genel Müdür ve Bilgi Güvenliği Yönlendirme Kurulu

Destek Veren: İş Birimi (departman)Yöneticileri

Rolü: Bir bütün olarak kuruluşun bilgi güvenliğine uyumunu koordine etmek ve sağlamaktan, güvenlik konularını ve bunların durumunu (uygulanmalarının izlenmesi) Bilgi Güvenliği Yönlendirme Kurulu'na (Güvenlik Kurulu) raporlamaktan sorumludur.

6.4. İş Birimi Yöneticileri

Raporlama Yaptığı Merc: Bilgi Güvenliği Yöneticisi

Rolü: Birim çalışanlarının, bilgi güvenliği politika ve prosedürlerine bağlı kalmalarını sağlamaktan ve ilgili oldukları bölüm içerisinde bilgi güvenliği politika ve prosedürlerinin uygulanmasından sorumludur.

7. İÇ VE DIŞ TARAFLARIN BEKLENTİLERİ

Abalioğlu Tarımsal ve Lezita Balık A.Ş, BGYS ile ilgili olabilecek tüm iç ve dış tarafları ve bu ilgili tarafların bilgi güvenliği ile ilgili, yasal, düzenleyici ve sözleşmesel tüm gereksinimlerinin farkında olup, bu gereksinimleri BGYS doğrultusunda karşılamaktadır.

	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS) POLİTİKASI	Doküman Kodu: EY.BG.POL.01
		Versiyon: 1
		Yayın Tarihi: 26.02.2019
		Sınıfı: Kurum İçi

Abalioğlu Tarımsal ve Lezita Balık A.Ş. aşağıdaki iç ve dış taraflar ile belirtilen konular hakkında iletişim halindedir. Bu konular ile ilgili var olan tüm riskler Risk Değerlendirme Çalışması'nda tanımlanıp, ilgili taraflara bağlanarak değerlendirilmiştir.

İlgili Taraf	Tipi	Beklentiler / Paylaşılan Rapor ve Belgeler
Bankalar	Dış	Borç, mutabakat ve otomatik ödeme bilgileri paylaşılmaktadır.
SMS Uygulaması	Dış	Kantarda ölçümü yapılan kamyonların fabrikadan çıkış zamanı bilgileri bayiler ile paylaşılmaktadır.
Gelir İdaresi Başkanlığı	Dış	Fatura, e-defter ve berat için iletişim kurulmaktadır.
Maliye Bakanlığı	Dis	Mali veriler paylaşılmaktadır.
Avukatlık Bürosu	Dis	Hukuki belgeler ve icra takip bilgileri paylaşılmaktadır.
Belediyeler	Dis	Alt yapı hakkındaki bilgiler paylaşılmaktadır.
İnternet Servis Sağlayıcı	Dis	Tüm bağlantı altyapısı, MPLS yapısı Superonline firması omurgası üzerinden sağlanmaktadır.
Tedarikçiler	Dış	Yapılan işin niteliğine göre gerekli bilgiler paylaşılmaktadır.
Müşteriler	Dış	Kendi abone bilgileri, alt yapı bilgileri ve ilgili duyurular paylaşılmaktadır.
Çalışanlar	İç	Şirket politika ve prosedürleri, şirket uygulamaları, duyurular vb gibi konular açılmaktadır.
Yönetim	İç	Yönetim gözden geçirme toplantı sunumları, politikalar, prosedürler, denetim raporları paylaşılmaktadır.