EKOSinerji
Elektrik San. ve Tic. A.Ş.

EKOS-EK-03

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ EL KİTABI

19.06.2020

	HAZIRLAYAN	ONAYLAYAN
GÖREVİ	**BGYS TEMSİLCİSİ**	**GENEL MÜDÜR YARDIMCISI**
İMZA		

İÇİNDEKİLER

KISALTMALAR TABLOSU

Kısaltma	Tanım
EKOSinerji	EKOSinerji Elektrik Sanayi ve Ticaret A.Ş.
BGYS	Bilgi Güvenliği Yönetim Sistemi
BGYS Sorumlusu	Üst Yönetim tarafından BGYS kurulması ve yönetilmesinden sorumlu kişi
BGYS Yöneticisi	BGYS Sorumlusu tarafından görevlendirilmiş kişi
Üst Yönetim	EKOSineji Üst Yönetimi

KURULUŞ TANITIMI :

EKOSinerji Elektrik Sanayi ve Ticaret A.Ş. yatırım ve hizmet projeleri, üretim, otomasyon ve koruma ve kontrol sanayi için pazarlama sistemleri alanlarında sağlayan bir mühendislik firmasıdır güç. Şirketin amacı, enerji tasarrufu için, kullanıcılara enerji dağıtım yoluyla uygulamaları, üretim, taşıma geniş bir örtü kullanılabilir kaliteli çözümler yapıyor. **EKOSinerji Elektrik Sanayi ve Ticaret A.Ş.** programlarında VAR (katma değerli satıcı) tasarım hizmetleri ve sistem entegrasyonu şirketi General Electric (GE Multilin ve GE Energy NA & S) alanında dünya lideri olan sağlamaktadır. **EKOSinerji Elektrik Sanayi ve Ticaret A.Ş.** kapsamı satış, proje teslim ve mühendislik koruyucu ekipman ve kontrol röle alanlarında içeren, kontrol sistemleri ve otomasyon, SCADA ürünleri ve sistemleri Tedbirler elektrik tesisatları ve endüstriyel tesislerde kullanılır....

Alçak ve orta gerilim için genel amaçlı SF6 gazlı ve vakum kesicili modüler hücreler, modüler RMU'lar ve SF6 gazlı kompakt RMU'ları uluslararası test raporları ve ISO 9001:2008, ISO 14001:2004, OHSAS 18001:2007 ve TSE belgeleri ile üretmektedir. 1995 yılında faaliyette başlayan firma, Türk Elektromekanik Sanayisi'nin prestijli kuruluşları arasında hızla yerini almıştır. Ülkemizin teknolojisine katkılar sağlamak azmi ve kararlılığında olan fima, Tübitak-TTGV Türk Teknoloji Geliştirme Vakfı desteğiyle yürütmüş ve başarıyla gerçekleştirmiş olduğu SCADA'ya hazır projelerle, Orta Gerilim Metal Mahfazalı Modüler Hücreler, Orta Gerilim RMU imalatlarını da tamamlayarak, üretmiş olduğu ürünleri yurt ve Dünya pazarlarına sunmuştur.

EKOSinerji Elektrik Sanayi ve Ticaret A.Ş

GEBZE-MERKEZ

İstasyon Mah. Güney Yanyol Cad.
No:78 Gebze – KOCAELİ

Tel : 0 262 656 47 67
Fax : 0 262 656 47 70
e-mail : ekosinerji@ekosinerji.com
web : www.ekosinerji.com

Balıkesir-FABRİKA

Organize Sanayi Bölgesi 7.Cadde No:17-19 Altıeylül/Balıkesir/Türkiye
Tel : +90 266 281 12 95
Fax : +90 266 281 12 95
e-mail : ekosinerji@ekosinerji.com
web : www.ekosinerji.com

1. Giriş

1.1. Bilgi Güvenliği Nedir?

Bilgi, diğer önemli ticari ve kurumsal varlıklar gibi, bir işletme ve firma için değeri olan ve bu nedenle uygun olarak korunması gereken bir varlıktır. Bilgi güvenliği; bilgiyi, yetkisiz kişilerin görmesinden, değiştirmesinden, bilgilerin silinmesinden korumaktadır. Şüphesiz firmalarda saklanan ve üretilen birçok bilgi yetkisiz kişiler tarafından görülmemesi gereken, silindiğinde ve yetkisiz kişilerin eline geçtiğinde firmayı sıkıntıya sokacak bilgilerdir.

Bilgi güvenliği, firmalarda bilişim sistemlerinin kullanılmasıyla daha önemli hale gelmiştir. Bilgi saklama ortamları olarak çoğunlukla kağıt kullanılmadığı zamanlarda güvenlik önlemleri olarak fiziksel güvenlik önlemlerine ağırlık verilmiş, ancak gelişen teknolojiler kullanılarak bilgilerin dijital ortamlarda, veri tabanlarında, CD, disk gibi saklama ortamlarda kullanıcısının 24 saat erişebileceği şekilde saklanması gündeme geldiğinde fiziksel güvenlik önlemleri yetersiz kalmaya başlamıştır. Gerek bilişim sistemlerinin bağlantı ihtiyaçları sonucunda internet erişimleri nedeniyle dünya üzerindeki birçok saldırganın tehdit oluşturması, gerekse iç kullanıcıların bilinçli veya bilinçsiz olarak bilgi güvenliğinde açıklara neden olması, kurumlarda bilgi duyulan ihtiyaçla birlikte, güvenliğin sağlanması için bilinçli personel barındırmak ve güvenlik sürecinin işletilmesi için yeterli doküman ve prosedürlerin oluşturulması da bir zorunluluk olmuştur.

Bilgi güvenliği, bu politikada aşağıdakilerin korunması olarak tanımlanır.

Gizlilik : Bilginin sadece erişim yetkisi verilmiş kişilerce erişebilir olduğunu garanti etmek,

Bütünlük : Bilginin ve işleme yöntemlerinin doğruluğunu ve yetkisiz değiştirilememesini temin etmek,

Kullanabilirlik : Yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara en hızlı şekilde erişebileceklerini garanti etmek.

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

1.2. Bilgi Güvenliği Amaçları

Bilgi sistemleri henüz yeterli güvenlik seviyesine ulaşmamıştır. Teknik olanaklar aracılığıyla ulaşılabilen güvenlik sınırlıdır ve uygun yönetim ve yöntemlerle desteklenmelidir. EKOSinerji bünyesinde bulunan bilgi güvenliğinin amacı uygun ve etkili prensip ve politikalar kullanarak bilgi sistemlerinin güvenlik seviyesini artırmaktır.

EKOSinerji bilgi güvenliğinin hedefi her seviyede kullanıcıya bilgi sistemlerini kullanımları sırasında ne şekilde hareket etmeleri gerektiği konusunda yol göstermek, kullanıcıların bilinç ve farkındalık seviyelerini artırmak ve bu şekilde bilgi sistemlerinde oluşabilecek riskleri minimuma indirmek, kurumun güvenirliliğini ve temsil ettiği makamın imajını korumak, üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak, firmanın temek ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamaktır.

Firmanın risk yönetim çerçevesi, bilgi güvenliği risklerinin tanımlanmasını, değerlendirilmesini, işlenmesini kapsar. Risk Değerlendirme ve Analiz dokümanı firmanın risk değerlendirme metodolojisini ve bilgi güvenliği risklerinin nasıl kontrol edildiğini tanımlar.

1.3. Bilgi Güvenliği Kapsamı

BGYS kapsamı olarak EKOSinerji bilgi işlem varlıkları, süreçleri, sistem odası, bilgi işlem insan kaynaklarını ve üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ayrıca bilgi sistemleri yapısına hizmet, yazılım veya donanım destek sağlayıcılarını kapsamaktadır. Lokasyon olarak Bilişim Merkezi olan Balıkesir Tesisi bu kapsamda olacaktır.

Bu doğrultuda bilgi sistemleri varlıkları ile etkileşim içerisinde olan süreçler belirlenmiş olan risk yönetimi metodolojisi çerçevesinde incelenecektir.

1.3.1 Kuruluş Bağlamı

Kuruluşun, amaçları ile ilgili olan ve bilgi güvenliği yönetim sisteminin hedeflenen çıktılarını başarma kabiliyetini etkileyebilecek iç ve dış hususları belirlenmiş ve iç ve dış hususlar başlıkları altında aşağıda listelenmiştir.

Dış Hususlar

- Kuruluşu etkilecek bölgesel faktörler
- Siyasi ve politik faktörler
- Hukuksal faktörler
- Teknolojik faktörler
- Ekonomik faktörler (hisseler vs.)
- Paydaşlarınızın yaklaşımları ve değerlerinin etkisi.

İç Hususlar

- Kaynaklar ve faaliyetler için gerekli unsurlar (Sermaye, Zaman, İnsan, süreçler, sistemler ve teknolojiler),
- Bilgi işletim sistemleri, bilgi akışı ve karar süreci (resmi ya da gayri resmi),
- Dahili (kuruluş içi) paydaşlar,
- Tanımlanmış hedeflere ve geçerli stratejilere ulaşmak için yapılacak eylemler,
- Temel prensipler, değerler ve Şirket kültürü,
- Kuruluşun üstlendiği standartlar, kılavuzlar ve referans modeller
- Organizasyon (ör. yönetim, görev ve sorumluluklar)

2. Yönetim Desteği

BGYS kurulurken üst yönetim tarafından BGYS Temsilcisi atanmalıdır. BGYS Temsilcisi değiştiğinde, işten ayrıldığında üst yönetim tarafından atama tekrar yapılmalıdır. BGYS Temsilcisinu belirlemek ve değiştirmek üst yönetimin yetkisindedir.

Yönetim kademeleri bilgi güvenliği konusunda ısrarcı olmalı, alt kademelerde bulunan personele sorumluluk verme ve örnek olma konusunda yardımcı olmalıdır. Üst kademelerden başlayan ve uygulanan bir güvenlik anlayışıyla, firmanın en alt kademe personeline kadar inilmesi zorunludur. Bu yüzden firmadaki yöneticilerin, gerek yazılı gerekse sözlü olarak güvenlik prosedürlerine uymaları,

güvenlik konusundaki çalışmalara katılmaları ve güvenlik ile ilgili çalışmalarda bulunan personele destek olmaları gerekmektedir.

3. Güvenlik Politikası Dokümanı Güncellenmesi ve Gözden Geçirilmesi

Politika dokümanının sürekliliğinin sağlanmasından ve gözden geçirilmesinden BGYS Temsilcisi sorumludur.

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 değişiklikten sonra da gözden geçirilmeli ve herhangi bir değişiklik gerekiyorsa versiyon değişimi olarak kayıt altına alınmalı ve her versiyon Bilgi Teknolojileri sorumlusuna ve 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.
- Politikanın güncelliği değişen personelle birlikte gözden geçirilmeli, yeni personelin katılımı sağlanmalıdır
- Politika, sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra gözden geçirilmelidir.

4. Kurumsal Güvenlik

4.1. Bilgi Güvenliği Altyapısı

Bilgi güvenliği ile ilgili tüm faaliyetlerden BGYS Temsilcisi sorumludur.

BGYS kapsamlı çalışmalar BGYS komitesi ve Beta Servis ile yürütülmektedir. BGYS komitesi Genel Müdür Yardımcısı, Grup liderleri ve Bilgi Teknolojileri sorumlusundan oluşmaktadır.

- Bilgi güvenliği politikalarının ve sorumlulukların gözden geçirilmesi,
- Büyük tehditlere karşı varlıklardaki önemli değişikliklerin değerlendirilmesi,
- Bilgi güvenliği olaylarının ve hatalarının gözden geçirilmesi,
- Bilgi güvenliği için önceliklerin gözden geçirilmesi.

BGYS Temsilcisi, yukarıda belirtilen gündeme konu ekleyebilir, gündemden konu çıkarabilir ve gündem tarihini ortak bir başka tarihe değiştirebilir.

4.2. Üçüncü Şahısların Bilgiye Erişimi

EKOSinerji personeli olmayan üçüncü tarafların, bilgi sistemlerini kullanma ihtiyacı olması durumunda BGYS sorumlusu, 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 bakım personelinin politikaya uyması için süre tahsis edilmelidir. Gizlilik sözleşmesi ve Bilgi Güvenliği sözleşmesi imzalanacak firma ve kişileri BGYS Sorumlusu belirlemelidir.

4.3. Dış Kaynak Sağlanması

Bilgi Teknolojisi Sistemleri, 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.

5. Varlıklar

5.1. Varlıkların Sınıflandırılması ve Denetimi

Varlık : Bir kurum için değeri olan ve bu nedenle uygun olarak korunması gereken tüm unsurlardır.

Firma bünyesinde kullanılmakta olan her bir varlık envanter kayıtlarına geçirilmelidir. Envanter kayıtları sürekli olarak güncel tutulmalı ve yeni varlıklar envanter kayıtlarına hemen girilmelidir.

Belli başlı bilgi, yazılım, donanım ve hizmet varlıkları için sahipler atanmalı ve varlıkların sahipleri envanter kayıtlarında bulunmalıdır. Herhangi bir bilgi teknolojisi varlığının sahibi olarak belirlenmiş personel, bu varlığın korunmasından sorumludur.

Tüm bilgi, veri ve dokümanlar anlaşılır bir biçimde etiketlenmelidir. Bilgi varlıklarının sınıflandırılmasından ve bu sınıflandırmanın belirli zamanlarda gözden geçirilmesinden BGYS Sorumlusu sorumludur. Gerektiğinde BGYS sorumlusu sınıflandırmayı belirleyebilir veya belirlemek üzere birini görevlendirebilir.

Erişim kontrol prosedürü ve risk analizi tedavi planı hazırlanırken varlık envanteri listesi göz önünde bulundurulmalıdır.

6. Personel Güvenliği

- Tüm çalışanlar, firmanın bilgi güvenliği politikalarına uymakla yükümlüdürler. Kullanıcılar, politikalara uygun olmayan davranışları sonucu meydana gelebilecek bilgisayar olaylarından sorumlu olacaklardır.
- Firma çalışanları, firma personeli olduğu sürece ve firmadan ayrılmaları (emeklilik, istifa, vs.) durumlarında firma bilgilerini gizlilik prensibine uygun olarak korumaktan sorumludur.
- İşten ayrılan veya firma içinde görev değişikliği olan personel için kullanıcı hesaplarının silinmesi, erişim yetkilerinin değiştirilmesi gibi gerekli kontroller hemen yapılmalıdır.
- Üçüncü şahıslar da dahil olmak üzere, EKOSinerji bilgi sistemlerini kullanması gereken her personel için Bilgi Sistemleri olanaklarının doğru kullanımı da dahil olmak üzere uygun güvenlik politikaları ve prosedürleri konusunda gerekli taahhütnameler hazırlanmalı ve ilgili personele imzalatılmalıdır.
- Kullanıcı adı açılmış tüm firma personeline farkındalık eğitimi verilmelidir. Bu eğitimler, her yeni personel alımı sonrasında yeni personel için de tekrarlanmalıdır. Toplu olarak verilen eğitimler de öncesi ve sonrası değerlendirme anketleri uygulanmalı, etkinlik gözden geçirilmelidir.

7. Fiziksel Güvenlik

7.1. Güvenlik Korumalı Bölgeler

- Kritik veya hassas iş faaliyetlerini desteklediği belirlenen tüm bilgi teknolojisi araçları, kart kontrollü, parmak izi kontrollü veya benzeri girişlerle korunan, fiziksel erişim kontrolü gerektiren alanlarda bulunmalıdır.
- Giriş yetkisi sahibi tüm personel, ilgili taahhütnameye uygun davranmalıdır. Kendisinin izni olmayan alanlara girmek için başkalarının kartını kullanmamalıdır.
- Güvenli alanlara alınacak ziyaretçilere atanmış firma personeli sürekli eşlik etmeli ve ziyaretleri süresince güvenli bölgelerde yalnız bırakılmamalarına dikkat edilmelidir.
- İzin verilmediği sürece güvenli alanlarda fotoğraf çekmek, görüntü almak ve ses kaydetmek yasaktır.
- Güvenli alanlara erişen yetkili personel dışındaki tüm kişilerin giriş ve çıkış saatleri kaydedilmelidir.
- Kritik alanlar dijital ortamlarda görüntülü kayıt altına alınmalıdır.

7.2. Donanımsal Güvenlik

- Personel, önemli varlıkların bulunduğu güvenli alanlarda sigara içmemeli, yiyecek ve içecekle güvenli alana girmemelidir.
- Bilgi teknolojisi araçlarının, herhangi bir elektrik kesintisinde çalışmalarına devam etmeleri için kullanılan UPS, jeneratör gibi güç kaynakları yılda bir sefer olmak üzere periyodik olarak üreticilerin talimatlarına uygun biçimde kontrol edilmelidir.
- Tüm donanımların, elverişliliği ve güvenirliliği garanti etmek amacıyla üretici firmanın talimatlarına uygun olarak, düzenli periyodlarda bakımları yapılmalıdır.
- Dizüstü bilgisayara, belge, CD ve taşınabilir bellek gibi taşınabilir firma varlıklarının korunması için gerekli önlemlerin alınmasından envanter sisteminde varlık sahibi olarak kaydedilmiş kişi sorumludur. Herhangi bir kaybolma veya çalınma durumunda da hasarı karşılayacak kişi varlık sahibidir.
- Çalışanlar, adlarına kayıtlı taşınabilir cihazların korunmasından ayrıca firma dışına çıkıldığı durumlarda da sorumludurlar.
- Firma dışına çıkarılabilen varlıklar firma dışında çalışırken gizlilik prensipleri ve varlık sınıflandırmaları göz önünde bulundurulmalı ve bilgi varlıklarının dışarı çıkarılabilmesine varlık sınıflandırması sonucuna uygun olduğu takdirde izin verilmelidir.
- Personel, kendisine ait varlıkları (şahsi dizüstü bilgisayar, avuç içi bilgisayar vb…) BGYS Yöneticinden habersiz ve onaysız firma sistemlerine bağlı kullanamaz.
- Hassas bilgiler içeren depolama aygıtları ilgili prosedürüne uygun olarak elden çıkarılmalıdır.

7.3. Genel Güvenlik Denetimleri

- Kullanıcılar, kullanmadıkları zamanda ekranlarının izinsiz kişilerce görülmesini engellemek için işletim sisteminin ekran kilitlenmesi özelliğini etkin hale getirmek gibi önlemleri almalıdırlar. İlkenin tam olarak uygulanması için, merkezi olarak buna uygun kurallar bütün kullanıcı bilgisayarları ve sunuculara dağıtılmalıdır.
- Firma kullanıcıları, kendilerine verilmiş olan kullanıcı adı ve şifrelerinin sadece kendileri tarafından kullanılması ilkesini koruma sorumluluğuna uymalıdırlar. Bu ilkenin ihlali durumunda parola sahibi kullanıcı sorumlu olacaktır.

- Varlık sınıflandırmasında hassas bilgi olduğu için belirlenen dokümanların kağıt baskılarının erişim yetkisi olmayan kişilerce erişimini engellemek amacıyla firma personeli tarafından temiz masa politikası uygulanmalıdır. Temiz masa politikası, önemli dokümanların diğer kişilerce görülmesini engellemek amacıyla, kullanılmadığı zamanlarda masa üstlerinden kaldırılıp gerekli korumaları alınmış çekmecelerde saklanmasıdır. Bu şekilde masa üstlerinde hassas bilgilerin bulunmayacağı garanti altına alınmaktadır.
- Kullanıcılar çalıştıkları ortamdaki masa ve dolap çekmecelerini kilitli tutmaları ve anahtarları sorumlu kişiler haricinde kimseyle paylaşmamaları gerekmektedir.
- Personelin kişisel bilgisayarının sabit diski üzerinde bulunan dokümanlarının kişiye özel kalacağı garanti edilemez. Firma, haber vermeden her türlü bilgiyi izleme, kaydetme ve inceleme hakkına sahiptir.

8. Sistemlerin İşletim Güvenliği

8.1. İşletim Prosedürleri

Firma içi donanım ve uygulamaların işletim prosedürler hazırlanmalı ve aşağıdaki hususlara uyulmalıdır.

- Yazılı prosedürler ihtiyaç duyulduğunda Bilgi Teknolojileri sorumlusu tarafından hazırlanır ve BGYS sorumlusu tarafından onaylanarak güncellenir.
- Onaylı olmayan işletim prosedürleri geçersizdir. Geçerlilik onayı için Genel Müdür Yardımcısının imzalaması gereklidir.
- Firma genelinde tüm işletim prosedürleri yazılı olarak bulunur ve ihtiyaç duyulduğunda sürekli erişilebilen ortamlarda yayınlanır. (web, basılı doküman, vs.)
- Prosedürlerin süreklilikleri atanmış sahipleri tarafından kontrol edilmeli, değişen işletim talimatları prosedürlere yansıtılmalıdır.

8.2. Olay Yönetimi Prosedüleri

- Herhangi bir güvenlik olayı başlangıcında, sırasında ve sonrasında yapılması gereken adımları içeren ilgili prosedürleri uygulanmalıdır.
- Bilgi güvenliği ihlal olayı olarak değerlendirilen her durum için düzeltici ve önleyici faaliyet raporu oluşturulmalı ve kayıt açılmalıdır.
- Belirlenen eksiklikler tamamlanarak olayların tekrar gerçekleşmesinin önüne geçilmelidir.

8.3. Geliştirme, Test ve İşletim Sistemlerinin Ayrılması

Geliştirme, işletim ve test sistemleri birbirinden fiziksel olarak ayrılmalı, her bir sistem için ayrı cihazlar tahsis edilmelidir. Ayrıca her bir sistem için sorumlu personel atanmalıdır.

8.4. Sistem Planlama ve Genişletme

Varlık envanterinde kaydı bulunan her türlü varlık performans ve yeterlilik kapsamında yardımcı programlar vasıtasıyla, sürekli gözden geçirilmelidir. Yetersizlik veya ihtiyaç durumlarında değişim planlaması yapılarak satın alma süreci başlatılmalıdır.

8.5. Kötü Niyetli Yazılımlara Karşı Korunma

	HAZIRLAYAN	ONAYLAYAN
GÖREVİ	BGYS TEMSİLCİSİ	GENEL MÜDÜR YARDIMCISI
İMZA		

Firma genelinde kötü niyetli yazılımlara karşı gerekli korunma önlemleri alınmalı ve altyapı yeni tehditlere karşı sürekli olarak gözden geçirilip güncellenmelidir. Gerekli görülen ek önlemler BGYS toplantısında tartışılıp gerekli testleri yapıldıktan sonra sisteme entegre edilmelidir. Ancak kullanıcılar mevcut önlemlere güvenerek sistemi savunmasız bırakacak biçimde hareket etmemelidir.

8.6. Ağ Yönetimi

Tüm ağ (ana omurga ve aktif cihazlar) yönetimi yapılanması ve kurulumu BGYS Temsilcisi ve Beta Servis tarafından yapılmaktadır.

- Firma ağı içerisinde kullanıcılar sadece yetkileri olan klasörlere erişimleri bulunmaktadır.
- Ağ altyapı cihazlarına fiziksel erişim ile (konsol bağlantısı ile) veya uzaktan erişim (telnet, web, ssl, ssh üzerinden, yönetim yazılımı veya snmp ile) bağlantıları için kimlik kontrolü yapılmalıdır.

8.7. Bilgi Ortamı Yönetimi ve Güvenliği

- Taşınabilir ortamdaki bilgi artık kullanılmayacaksa, silinmelidir.
- Gerekli olmadığı sürece bilgi varlıkları yetkisiz kişilerle paylaşılmamalıdır.
- İşlemlerin, prosedürlerinin, veri yapılarının, yetkilendirme işlemleri gibi hassas bilgilerin bulunduğu sistem dokümantasyonu, yetkisiz kişilerin erişimini engellemek amacıyla güvenli ortamlarda bulundurulmalı, elektronik kopyalarına iç ağ üzerinden ilgili kişilerin erişebileceği şekilde erişim kontrolü prensipleri uygulanmalıdır.
- Dışarıdan yardım alınacak üçüncü şahıs firmaları ve dış kaynaklı çalışma personeline gerektiği takdirde geçici yetkileri bulunan kullanıcı hesapları tanımlanmalıdır. Bu hesaplar çalışma biter bitmez devreden çıkarılmalıdır.

8.8. Bilgi ve Yazılım Değişimi

- Bilgi varlıklarının dağıtımı veya nakli sırasında uygun güvenlik tedbirlerinin alınmasına dikkat edilmelidir. Bu tedbirler, özel güvenlikli paketleme, güvenli kurye kullanma veya elektronik ortamlar için sayısal imzalama ve şifreleme kullanma gibi önlemler olabilir.
- E-posta hizmetlerini kullanan tüm firma personeli, e-postaların güvenliğini sağlamak amacıyla oluşturulmuş olan politikalarda belirtilen kurallara uymakla yükümlüdürler.
- Web sitesi, çevresel bilgi sistemi ve diğer yollarla internet üzerinden bulunan halka açık firma bilgilerinin izinsiz olarak değiştirilmesine, eklenmesine veya silinmesine karşı gerekli koruma önlemleri alınmalı ve yetkilendirmeler yapılmalıdır.
- Ftp sunucusuna yapılan bağlantılar kullanıcı adı ve şifre korumalı olmalı, ftp üzerindeki her türlü hareket kayıt altına alınmalıdır.

9. Erişim Denetimi

9.1. Gereklilikler

- EKOSinerji bilgi sistemleri kaynaklarını kullanan tüm firma personeli, hizmet sağlayıcı firma dışı personel ve diğer üçüncü şahıslar ilgili prosedüre uymakla yükümlüdürler.

9.2. Kullanıcı Erişim Yönetimi

- Her kullanıcı, kendine ait hesabı kullanarak işlemlerini yürütür. Kullanıcılar kendi hesaplarının güvenliğini, şifrelerini saklayarak, başkalarının kendi hesabını kullanmasına izin vermeyerek ve gerektiğinde oturum kilitleme gibi özellikleri kullanarak korumakla yükümlüdürler.
- Her kullanıcıya standart erişim hakları verilmektedir. İhtiyaç olunan ek haklar için ilgili form / taahhütname imzalatılarak erişim hakları verilmelidir.
- İnsan Kaynakları tarafından Bilgi Teknolojileri sorumlusuna bildirilen işten ayrılan personel için gerekli hesap kapatma, birim değiştiren kullanıcıların ise erişim haklarının düzenlemesi işlemleri hemen yapılmalıdır.
- Gereksiz kullanıcı hesaplarının kontrol edilmesi ve kaldırılması işlemi yılda en az 1 defa yapılmalıdır.
- Kullanıcıların erişim hakları her değişiklikten sonra veya belirli aralıklarla gözden geçirilmelidir.
- Kullanıcıların sunuculara olan yetkisiz erişim denemeleri ile hak sahibi personelin erişimleri Bilgi Teknolojileri sorumlusu tarafından kullanılan güvenlik yazılımlarıyla kontrol edilmeli, gerektiği takdirde erişimler ve erişim denemeleri rapor edilmelidir.
- Çeşitli sebeplerle kapatılan kişi ve/veya bilgisayar hesap bilgileri ayrı bir yerde en az 5 yıl süreyle saklanmalıdır.

9.3. Ağ Erişim Denetimi

Ağ hizmetlerini kullanan tüm personel ve üçüncü taraflar, ilgili prosedüre uymalıdır.

9.4. İşletim Sistem, Erişimi Denetimi

- Başarısız oturum girişimleri güvenlik yazılımları tarafından kaydedilip, gerektiğinde incelenmek üzere saklanmaktadır.
- Onaylı olmayan yazılımların kullanıcı bilgisayarlarına yüklenmesi yasaktır. Zaman zaman kullanıcı bilgisayarlarında bu tip yazılımların varlığını denetlemelidir. Denetleme BGYS Temsilcisi tarafından yapılır.

9.5. Uygulama Erişimi Denetimi

- Uygulama sistemlerinin kullanıcıları, erişim isteklerini yardım masası üzerinde ki ilgili kategoriyi seçerek talepte bulunmalıdır.

9.6. Dışarıdan Sisteme Erişim Denetimi

Dış ağlardan firma iç ağına doğru yapılan erişimler sürekli olarak denetlenmelidir. Saldırı tespit ve önleme sistemi, antivirüs ve kötü niyetli kod engelleme sistemleri daima aktif durumda tutulmalıdır.

10. Uygulama Sistemi Geliştirilmesi ve İdamesi

10.1. Sistem Güvenlik Gereklilikleri

Sistem tasarımı/planlamasında güvenlik gerekleri göz önünde bulundurulmalı, gerektiği zaman BGYS komitesi tarafından tartışılmalıdır. Firma tarafından geliştirilen yazılımlar, ilgili prosedürüne uygun

yazılmalıdır. Firmada geliştirilmekte olan yazılımın bütünlüğü, erişim kontrolleri, kısıtlanmış haklar bu prosedürde tanımlanmıştır.

10.2. Sistemlerde Güvenlik

- Geliştirilmekte olan uygulama yazılımlarında hatalı girdi ve çıktı kontrolleri bulunmalıdır. Bu şekilde sıra dışı değerler, geçersiz karakterler, tampon taşması yaratabilecek değerler girilmesi engellenmektedir.

- Geliştirilen sistemler, teknolojiye uygun güvenlik açığı tarama sistemleri tarafından periyodik olarak kontrol edilmeli, bulunan açıklar versiyon değişiklikleri ile kapanmalıdır.

10.3. Sistem Dosyaları Güvenliği

- Geliştirilen yazılımlar test ortamında denendikten ve operasyonel sistemlerde bir problem çıkartmadığına emin olunduktan sonra işletim ortamına aktarılmalıdır.

- Testler için kullanılmakta olan verilerin sahibi atanmalıdır. Test verilerinin sahibi olarak atanan personel, verilerin korunmasından ve kontrolünden sorumludur.

- Test için operasyonel veriler kullanılmaktaysa, bu verilerin gizlilik sınıflandırmalarına uygun olarak korunmaları düşünülmelidir.

- Programların kaynak kütüphaneleri operasyonel sistemlerden ayrı olarak tutulmalı, gerekli erişim kontrol prensipleri sıkı bir şekilde uygulanmalıdır.

11. İş Sürekliliği Yönetimi

İş Sürekliliği Planının amacı EKOSinerji bilişim sistemlerinde, olası felaket ve iş akışını engelleyecek veya aksatacak her türlü senaryonun gerçekleşmesi halinde, firmanın kritik fonksiyonlarının kesintisiz biçimde devam ettirilmesi ve kesintiye uğrayan fonksiyonların ihtiyaç duyulan süre içerisinde geri döndürülmesidir.

İş sürekliliği yönetim sürecinde oluşturulan takımlar, en az yılda bir kez toplantı yapmalı ve sistemi gözden geçirmelidirler.

12. Uyum Süreci

12.1. Yasal Gereksinimlere Uyum

- EKOSinerji bünyesinde uygulanan bilgi güvenliği politikası, yürürlükteki tüm kanunlara uyumlu olmakla zorundadır.
- EKOSinerji bünyesinde kullanılmakta olan tüm yazılımların lisans sözleşmeleri olmak zorundadır. Lisanssız ürünlerin firma varlıklarında kullanılması yasaktır.
- Herhangi bir bilişim suçu işlediği saptanan personel, yasalara uygun olarak cezai işlem görür.
- EKOSinerji bünyesinde ya da ulusal yasalarda bilgi güvenliği politikasını etkileyen bir değişiklik belirtildiğinde, politika güncellenmelidir.

	HAZIRLAYAN	ONAYLAYAN
GÖREVİ	BGYS TEMSİLCİSİ	GENEL MÜDÜR YARDIMCISI
İMZA		

- Bilgi güvenliği olayı için kanıt oluşturabilecek herhangi bir veri, yetkililer gelene kadar değişime uğramayacak ve kanıt özelliğini kaybetmeyecek şekilde saklanmalıdır.

12.2. Sistem Denetleme Gereklilikleri

Sistem denetlemesi süresince, bilgi sistemlerini ve denetleme araçlarını korumak amacıyla gerekli önlemler alınmalıdır. Denetleme araçlarının yanlış/yetkisiz kullanılmasını engellemek amacıyla denetleme aracı sahibi, ilgili prosedürü kullanılarak gerekli önlemlerin alındığını kontrol etmelidir.

13. Teknik Güvenlik İlkeleri

13.1. Kullanıcı Parola İlkeleri

- Tüm kullanıcılar etki alanına dahil olan donanımlarında EKOSinerji tarafından sağlanan hizmetlerden faydalanmak için sisteme logon (giriş yapmalı) olmalıdır. Tüm kullanıcıların kullanıcı-kimliği (user-ID) (varsa e-anahtarı) ve şifre ile kimlik doğrulamasının yapılması zorunludur.
- Kullanıcıların şifreleri en az 6 karakterli olmalıdır, ilk 5 karakter sayı, son karakter küçük harf olacak şekilde şifreler belirlenmelidir.
- Elektronik mesajlarda veya göndermelerde ihtiva edilen kullanıcı adı, elektronik posta adresi, organizasyonel bağlantı ve ilgili bilgi, mesajı yazan kişiyi yansıtmalıdır.
- EKOSinerji tarafından sağlanan internet hizmeti dışında alternatif internet hizmeti kullanılamaz.
- EKOSinerji, elektronik haberleşmenin kişiye özel olacağını garanti edemez. Personel elektronik haberleşmenin, teknolojiye bağlı olarak, başkaları tarafından aktarılabileceğinin, engellenebileceğinin, yazıya dökülebileceğinin ve depolanabileceğinin farkında olmalıdır.
- Elektronik haberleşmenin içeriğinin düzenli olarak izlenmesi, EKOSinerji Bilgi Güvenliği Politikasının bir parçası değildir. Ancak firma şüphelenilen mesajların incelenme hakkına ve yetkisine sahiptir. Bununla birlikte internet üzerinden yapılan elektronik haberleşmenin içeriği ve elektronik haberleşme sistemlerinin kullanımı işlevsel, bakım, teftiş, güvenlik, araştırma faaliyetlerini desteklemek için izlenebilir. Kullanıcılar kendi elektronik haberleşmelerini EKOSinerji'nin elektronik haberleşmenin içeriğini zaman zaman kontrol edeceği gerçeğini kontrol ederek düzenlenmelidirler.
- Genellikle kabul edilen iş uygulamalarına uyumlu olarak, EKOSinerji elektronik haberleşme ile ilgili istatistiksel bilgiler toplamaktadır. Bu bilgileri kullanarak teknik destek personeli bu sistemlerin devam eden güvenirliğini ve kullanabilirliğini emniyet altına almak için izlemektedir. Bu yüzden personel, EKOSinerji tarafından konulan kısıtlamalara bağlı olarak internet'ten kullanılan kaynaklar açısından adını gizleme şansına sahip değildir.
- Personel, üçüncü şahıslarla ilgili elektronik mesajlarda küfürlü, ayıp veya küçültücü ifadeler kullanmamalıdır. Bu tip ifadeler şaka yaparken bile kişisel iftira gibi yasal sorunlar yaratır.
- Firma e-posta sunucusuna gelen mesajlar virüs tarayıcısından geçirildikten sonra kullanıcılara ulaştırılmaktadır, ancak yine de kullanıcılar, e-posta vasıtasıyla bulaşacak virüs gibi zararlı

içerikten korunmak amacıyla, tanımadığı kişilerden gelen ve şüpheli eklentiler içerdiği görülen mesajları gerekmediği sürece açmamalıdır.

- Kullanıcılar her türlü bilgi güvenlik alarmlarını, ikazlarını, şüpheli ihlalleri ve bunun gibi olayları derhal ilgili prrosedüre uygun olarak rapor etmelidir.
- Elektronik posta sistemleri önemli bilgilerin arşiv depolamasına uygun değildir. Depolanmış önemli elektronik posta mesajları sistem yöneticileri tarafından periyodik olarak silinebilir, kullanıcılar tarafından kaza ile silinebilir ve sistem problemleri meydana geldiğinde kaybolabilir. Kullanıcılar önemli e-postalarının yedeklerini almaktan sorumludurlar.
- Kullanıcı şifreleri sürekli geçerli olup kullanıcı şifreleri parolanın güvenlikte olmadığına dair bir gösterge olduğu zaman (ör: saldırılar, çalınma süresi, Truva atı bulunması, vs.) değiştirilmelidir.
- Firma personeli şahsi şifrelerini özel kontrol altında tutmalı, şifrelerini hiç kimseyle paylaşmamalıdır.
- Kullanıcılar, firma servisleri için kullandıkları şifreleri, internet üzerinden başka amaçlar için (örneğin tartışma grupları ve/veya bedava e-posta hesapları için) kullanmamalıdır.
- Şifreler, dosya otomatik komut dosyası (log-in script), yazılım makrosu, erişim kontrolü olmayan bilgisayarlar ve yetkisiz personelin fark edeceği yerlere (kağıt üzerine yazarak bilgisayarın yanına bırakmak gibi) yazılmamalıdır.
- Kullanıcılar veya sistem yöneticileri, bilgisayarlarını veya sunucuları kilitlemeden kullanılır durumda bırakmamalıdırlar.
- Kullanıcılar, kullanmaya kısa süreli ara verdikler, bilgisayarları veya terminalleri parola korumalı ekran koruyucu gibi özellikler kullanarak güvenlik altına almakla yükümlüdürler.

13.2. İnternet ve E-Posta Kullanım İlkeleri

EKOSinerji internet sistemi yalnızca iş faaliyetlerini destekleyecek şekilde kullanılmalıdır. Internet kullanımı;

- Kişisel kullanımda, görev amaçlı kullanılabilecek kaynaklar az miktarda kullanılıyorsa,
- Çalışanların verimliliğini engellemiyorsa,
- Herhangi bir iş faaliyetini aksatmıyorsa,
- Kullanıcıların bazı kişisel işlerini daha hızlı yerine getirmesini sağlıyorsa bu tip kişisel kullanıma izin verilebilir.

  - Kullanıcıların internet kullanım yoğunluğu diğer kullanıcıların internete ulaşımlarını engelleyecek şekilde olmamalıdır. Sistem bakım-idame işlerini yürüten personele ayrıcalıklar tanınabilir.
  - İnternet kullanımı, içerik kontrolcüleri ve virüs tespit sistemleri kullanılarak sınırlandırılmaktadır. Kullanıcılar, bu kontrollerin yapıldığını bilerek interneti kullanmalı, güvenlik amacıyla konulan önlemleri devre dışı bırakmaya çalışmamalıdır.
  - Çalışanlar kendi kullanımlarına kayıtlı olanlardan başka e-posta/iletişim ağı/uygulama hesaplarını kullanamazlar. Eğer bilgi paylaşımı gerekiyorsa, kullanıcı adı/şifresi paylaşımından ziyade mesaj gönderme veya diğer kolaylıklar gibi alternatif yaklaşımlar kullanılmalıdır.

- İş amaçları için gerekli olmayan mesajlar periyodik olarak kullanıcılar tarafından kişisel elektronik mesaj saklama alanlarından silinmelidir. Belirli bir süreçten sonra çok kullanıcılı sistemlerde saklanan elektronik mesajlar otomatik olarak sistem yönetim personeli tarafından silinecektir. Bu, az olan saklama alanını çoğaltmakla kalmayıp, kayıt yöntemini ve ilgili faaliyetleri de kolaylaştıracaktır.
- EKOSinerji bilgisayar ve iletişim sistemleri, personelin her türlü şahsi düşünce, fikir, yorum ve ifade özgürlüğü hakkı için kullanılmamalıdır. Aksi davranışlar resmi soruşturmaya yol açabilir.
- EKOSinerji bilgisayarlarına veya ağlarına gönderilen her türlü bilgiyi filtreleme yetkisini saklı tutar. EKOSinerji suç veya kanunsuz olması muhtemel olarak görülen her türlü malzemeyi kendi sistemlerinden çıkarma hakkını veya bununla ilgili resmi işlem başlatma hakkını saklı tutar.

13.3. Virüs ve Zararlı İçerikten Korunma İlkeleri

- EKOSinerji bilgisayar ağına bağlı olarak çalışan bilgisayarlara BGYS Temsilcisi tarafından onaylanmış anti-virüs programının yüklenmesi zorunludur. Eğer personelin bilgisayarında bu yazılım yok ise bunu Bilgi Teknolojileri sorumlusuna bildirmekle yükümlüdür.
- Virüs tanımlamaları program tarafından güncellenmektedir. Kullanıcı, anti-virüs yazılımın ve imza tablolarının güncelliğini kontrol etmeli, kullandığı bilgisayar üzerinde güncellemenin yapılmadığını fark ederse derhal bilgi teknolojileri sorumlusuna haber vermelidir.
- Bilgisayar virüsleri karmaşık ve gelişmiş olabileceğinden, personelin bunları uzman yardımı olmadan yok etmeye çalışmaması gerekir. Eğer personel virüsten şüphelenirse, hemen ilgili bilgisayarı kullanmayı bırakmalı, tüm iletişim ağlarıyla bağlantıyı kesmeli ve Bilgi Teknolojileri sorumlusuna haber vermelidir. Eğer şüphelenilen virüs, bilgilere ve yazılıma zarar vermeye başlarsa, personel hemen bilgisayarı kapatmalıdır ve Bilgi Teknolojileri sorumlusunun gelmesini beklemelidir.
- Dışarıdan temin edilen CD ve benzeri ortamlar virüs içerebilir, bu yüzden bu tür ortamlar virüs kontrolü yapılmadan ve virüs olmadığı belirlenmeden kullanılmamalıdır. Eğer virüs bulunduysa, olay ihbarında bulunulmalı ve virüsün yok edildiği gösterilene kadar bilgisayarda hiçbir çalışma yapılmamalıdır.
- Bilgi Teknolojileri sorumlusu virüs istilası ve sistem arızaları gibi acil durumları kontrol altına alabilmek için özel kullanıcı dosyalarını inceleme yetkisine sahiptir. Kullanıcı dosyaları bu şekilde incelendiğinde, buna dahil olan kullanıcı(lar) bilgilendirmek zorunda değildir.
- Kullanıcıların, EKOSinerji bilgisayar sistemlerine zarar verebilecek herhangi bir bilgisayar kodunu kasıtlı olarak yazmaları, çoğaltmaları, kopyalamaları, üretmeleri, çalıştırmaları ya da tanıtmaları yasaktır.

13.4. Taşınabilir Cihazlar Kullanım İlkeleri

- Taşınabilir cihazlar; firma bilgisi taşıyan her türlü dizüstü bilgisayar, avuç içi bilgisayar, CD, USB disk, teyp, taşınabilir sabit disk, yazılı raporlar gibi veri saklayabilecek ortamları tanımlamaktadır.

- Taşınabilir cihazlardaki bilgilerin üçüncü taraflarla paylaşımında da gerektiği kadar bilgi verme prensibi göz önünde bulundurulmalıdır. Söz konusu cihaz bilgisayarsa, yetkisiz kişilerin erişimine karşı sistemler ekran kilitleme özelliği gibi özelliklerle korunmalıdır.
- Firma dışına çıkarılabilen varlıklar firma dışında çalışırken gizlilik prensipleri ve varlık sınıflandırmaları göz önünde bulundurulmalı ve bilgi varlıklarının dışarı çıkarılabilmesine varlık sınıflandırması sonucuna uygun olduğu takdirde izin verilmelidir.
- Dizüstü bilgisayar, belge, CD gibi taşınabilir firma varlıklarının korunması için gerekli önlemlerin alınmasından envanter sisteminde varlık sahibi olarak kaydedilmiş kişi sorumludur. Herhangi bir kaybolma veya çalınma durumunda da hasarı karşılayacak kişi varlık sahibidir.
- Taşınabilir bilgi ortamlarının kullanılması, dışarı çıkarılması sırasında varlığın bilgi sınıflandırmasına uygun kontroller uygulanmalıdır.
- Dizüstü bilgisayarlarda virüs taramaları en az iki haftada bir kez yapılmalı, virüs güncellemeleri firma bilgi sistemleri üzerinden gerçekleştirilmelidir.
- Personelin kullanımı için tahsis edilmiş olan dizüstü bilgisayar, sadece yetkilendirilmiş personel tarafından ve veriliş amaçları doğrultusunda kullanılmalıdır.

14. Kullanıcı Bilgi Güvenliği Eğitimi

Aşağıdaki konuları kapsayan eğitimin, tüm firma kullanıcılarına verilmesi gerekmektedir. Böylece güvenlik ilkeleri anlayışının firmaya dağıtılması ve yaşatılması sağlanır.

- Bilgi güvenliği politikası eğitimi
  - Bilgi güvenliğinin tanımı, gerekliliği
  - EKOSinerji bilgi güvenliğinin hedefleri
  - EKOSinerji bilgi güvenliği politikasının tanıtımı ve politikaya uyulmasının önemi
- Kullanıcı güvenlik eğitimleri
  - Virüslerden, zararlı kodlardan korunma yolları
  - Zararlı e-postalardan korunma yolları
  - Güçlü şifreler seçme ve bunları güvenli saklama yolları
  - Temiz ekran ve temiz masa politikalarının önemi
- Firma gizliliğini sağlama bilinci için gerekli bilgiler
- Güvenlik olayı gözlemlenmesi durumunda kullanıcıların izlemesi gereken prosedürler

Yukarıdaki konuları kapsayan eğitimin, tüm firma kullanıcılarına verilmesi gerekmektedir. Böylece güvenlik ilkeleri anlayışının firmaya dağıtılması ve yaşatılması sağlanır.

Bu eğitimlerde;

- Bilgi güvenliği politikasından, kullanıcıların uyması gereken kurallardan, güvenlik olayı ihlallerinde nelerin yapılması gerektiğinden bahsedilmelidir.
- Ayrıca kullanıcıların eğitim düzeyini arttırmak için kullanmakta oldukları programlarla ilgili ve genel sistem yapısı ile ilgili bilgiler verilmelidir.

	HAZIRLAYAN	ONAYLAYAN
GÖREVİ	BGYS TEMSİLCİSİ	GENEL MÜDÜR YARDIMCISI
İMZA		

15. Roller ve Sorumluluklar

Bu kısımda EKOSinerji personeli için bilgi güvenliği rolleri ve sorumlulukları tanımlanmaktadır.

15.1. Genel Müdür Yardımcısının Sorumlulukları

- Güvenlik Politikasını onaylamak,
- BGYS kapsamlı Risk Değerlendirme ve Analiz dokümanını onaylamak,
- BGYS kapsamlı risk analizinde kritik seviyenin üstündeki riskleri onaylamak,
- Bilgi Teknolojileri sorumlusunu atamak,
- Bilgi Teknolojileri sorumlusunun hazırlamış olduğu dokümanları onaylamak,
- Bilgi Teknolojileri sorumlusunun yapmış olduğu faaliyetleri kontrol etmek ve onaylamak.

15.2. Grup Liderlerinin Sorumlulukları

- Kendisine bağlı çalışan personelin özel erişim yetkilerini onaylamak,
- Kendisine bağlı kısımda çalışacak üçüncü taraf bilgi sistemleri kullanıcılarının politikalardan haberdar olmasını sağlamak,
- Kendisine bağlı kısımda çalışan personelin bilgi güvenliği için kullanılan donanım ve yazılım kullanım talimatlarına uymasını sağlamak,
- Fark ettiği veya kendisine çalışanları aracılığıyla iletilen bilgi sistemleri ile ilgili güvenlik problemlerini BGYS Temsilcisina bildirmek,
- Sahibi olduğu bilgi varlığını korumak ve gerektiğinde güncellemelerde bulunmak,
- Bilgi Güvenliği Yönetim Sistemi Politikası'nı uygulamak.

15.3. BGYS Temsilcisinun Sorumlulukları

- Bilgi güvenliği ile ilgili konularda bölümler ve dış servis sağlayıcılar arasında koordinasyonu sağlamak,
- Güvenlik politikasının sahibi olarak, politikaların güncelleştirilmesinden ve uygulanmasından sorumlu olmak,
- Firma genelindeki tüm dokümanların Güvenlik Politikası prensiplerine uygun olarak yazılmasını sağlamak,
- Eğitimleri planlamak ve gerçekleşmelerini sağlamak,
- Sahibi olduğu bilgi varlığını korumak ve gerektiğinde güncellemelerde bulunmak, herhangi bir hata/arıza/olay olduğunda ilgili kişilere haber vermek,
- Güvenlik zaafları ve olaylarının nedenlerini araştırmak; gerektiği zamanlarda delilleri saklamak ve raporlamak, önlemler ve iyileştirme önerilerinde bulunmaktan sorumludur.

15.4. Kullanıcıların Sorumlulukları

- Bilgi Güvenliği politikasına uymak,
- Herhangi bir bilgi güvenliği olayını fark ettiğinde, zaman geçirmeden grup liderine ve/veya bilgi teknolojileri sorumlusuna bilgi vermek,

	HAZIRLAYAN	ONAYLAYAN
GÖREVİ	**BGYS TEMSİLCİSİ**	**GENEL MÜDÜR YARDIMCISI**
İMZA		

- Kendisine ait olan hesapların şifrelerinin güvenliğini sağlamak,
- Taşınabilir cihazların güvenliğini sağlamak, yetkilendirme olmadan dışarı varlık çıkarmamakla sorumludur.
- Bu dokümanda yer alan kurallara ve kullanıcı taahhütnamesinde yer alan tüm kurallara uymak.