


		BİLGİ GÜVENLİĞİ POLİTİKASI		
KOD NO	YAYIN TARİHİ	REVİZYON NO	REVİZYON TARİHİ	SAYFA
Y-BG.AŞ.PT.01-YG	15.08.2016	0	-	1/16

BİLGİ GÜVENLİĞİ POLİTİKALARI

1. GİRİŞ	3
1.1. BİLGİ GÜVENLİĞİ NEDİR?	3
1.2. BİLGİ GÜVENLİĞİ AMAÇLARI	3
1.3. BİLGİ GÜVENLİĞİ KAPSAMI	4
2. YÖNETİMİN DESTEĞİ	4
3. GÜVENLİK POLİTİKASI DOKÜMANI GÜNCELLENMESİ VE GÖZDEN GEÇİRİLMESİ	4
4. KURUMSAL GÜVENLİK	4
4.1. BİLGİ GÜVENLİĞİ ALTYAPISI	4
4.2. ÜÇÜNCÜ ŞAHISLARIN BİLGİYE ERİŞİMİ	5
4.3. DIŞ KAYNAK SAĞLANMASI	5
5. VARLIKLAR	5
5.1. VARLIKLARIN SINIFLANDIRILMASI VE DENETİMİ	5
6. PERSONEL GÜVENLİĞİ	6
7. FİZİKSEL GÜVENLİK	6
7.1. GÜVENLİK KORUMALI BÖLGELER	6
7.2. DONANIMSAL GÜVENLİK	6
7.3. GENEL GÜVENLİK DENETİMLERİ	7
8. SİSTEMLERİN İŞLETİM GÜVENLİĞİ	7
8.1. İŞLETİM PROSEDÜRLERİ	7
8.2. OLAY YÖNETİMİ PROSEDÜRLERİ	7
8.3. GELİŞTİRME, TEST VE İŞLETİM SİSTEMLERİNİN AYRILMASI	8
8.4. SİSTEM PLANLAMA VE GENİŞLETME	8
8.5. KÖTÜ NİYETLİ YAZILIMLARA KARŞI KORUNMA	8
8.6. AĞ YÖNETİMİ	8
8.7. BİLGİ ORTAMI YÖNETİMİ VE GÜVENLİĞİ	8
8.8. BİLGİ VE YAZILIM DEĞİŞİMİ	8
9. ERİŞİM DENETİMİ	9
9.1. GEREKLİLİKLER	9
9.2. KULLANICI ERİŞİMİ YÖNETİMİ	9
9.3. AĞ ERİŞİMİ DENETİMİ	9
9.4. İŞLETİM SİSTEMİ ERİŞİMİ DENETİMİ	9
9.5. UYGULAMA ERİŞİMİ DENETİMİ	9
9.6. DIŞARIDAN SİSTEME ERİŞİM DENETİMİ	10
10. UYGULAMA SİSTEMİ GELİŞTİRİLMESİ VE İDAMESİ	10
10.1. SİSTEM GÜVENLİK GEREKLİLİKLERİ	10
10.2. SİSTEMLERDE GÜVENLİK	10
10.3. SİSTEM DOSYALARI GÜVENLİĞİ	10
11. İŞ SÜREKLİLİĞİ YÖNETİMİ	10
12. UYUM SÜRECİ	10
12.1. YASAL GEREKSİNİMLERE UYUM	10
12.2. SİSTEM DENETLEME GEREKLİLİKLERİ	10
13. TEKNİK GÜVENLİK İLKELERİ	11
13.1. KULLANICI PAROLA POLİTİKASI	11
13.2. İNTERNET VE E-POSTA KULLANIM İLKELERİ	11
13.3. VİRÜS VE ZARARLI İÇERİKTEN KORUNMA İLKELERİ	12

HAZIRLAYAN	ONAYLAYAN
BİLGİ TEKNOLOJİLERİ YÖNETİCİ YARDIMCISI	GENEL MÜDÜR YARDIMCISI

	BİLGİ GÜVENLİĞİ POLİTİKASI			
KOD NO	YAYIN TARİHİ	REVİZYON NO	REVİZYON TARİHİ	SAYFA
Y-BG.AŞ.PT.01-YG	15.08.2016	0	-	2/16

13.4. TAŞINABİLİR CİHAZLAR KULLANIM POLİTİKASI	13
13.5. SOSYAL MEDYA KULLANIM POLİTİKASI	13
13.6. BULUT SİSTEMLERİ KULLANIM POLİTİKASI	14
14. KULLANICI BİLGİ GÜVENLİĞİ EĞİTİMİ	14
15. ROLLER VE SORUMLULUKLAR	14
15.1. KURUM ÜST YÖNETİM SORUMLULUKLARI	14
15.2. BİRİM MÜDÜRLERİNİN SORUMLULUKLARI	14
15.3. BGYS SORUMLUSU SORUMLULUKLARI	15
15.4. BGYS YÖNETİCİSİ SORUMLULUKLARI	15
15.5. KURUM PERSONELİNİN SORUMLULUKLARI	15
16. YÖNETİMİN ONAYI	16
17. ÇALIŞAN ONAYI	16

KISALTMALAR TABLOSU

<u>Kısaltma</u>	<u>Tanım</u>
BGYS	Bilgi Güvenliği Yönetim Sistemi
Envanter	Bilgi işlem tarafından önem arz eden her türlü kurum varlığı
Truva Atı	Bilgisayarlara izinsiz yüklenerek, dışarıdan bağlantıyı mümkün kılan kötü niyetli yazılım
Üst Yönetim	Yönetim kurulu üyeleri, Genel Mdr, İ.K. Md.
BGYS Sorumlusu	Üst Yönetim tarafından BGYS kurulması ve yönetilmesinden sorumlu kişi
BGYS Yöneticisi	BGYS Sorumlusu tarafından görevlendirilmiş kişi
Yardım Masası	Kurum işleyiş, üretim, takip amaçlı hazırlanmış olduğu kayıt yazılımı
VLAN(Sanal yerel ağ)	Birçok farklı ağ bölümüne dağılmış olan ancak birbirleri ile iletişim kurmaları sağlanan bir veya birkaç yerel ağ cihazları grubu.

HAZIRLAYAN	ONAYLAYAN
BİLGİ TEKNOLOJİLERİ YÖNETİCİ YARDIMCISI	GENEL MÜDÜR YARDIMCISI

	BİLGİ GÜVENLİĞİ POLİTİKASI			
KOD NO	YAYIN TARİHİ	REVİZYON NO	REVİZYON TARİHİ	SAYFA
Y-BG.AŞ.PT.01-YG	15.08.2016	0	-	3/16

1. Giriş

1.1. Bilgi Güvenliği Nedir?

Bilgi, diğer önemli ticari ve kurumsal varlıklar gibi, bir işletme ve kurum için değeri olan ve bu nedenle uygun olarak korunması gereken bir varlıktır. Bilgi güvenliği; bilgiyi, yetkisiz kişilerin görmesinden, değiştirmesinden, bilgilerin silinmesinden korumaktadır.

Bilgi güvenliği, kurumlarda bilişim sistemlerinin kullanılmasıyla daha önemli hale gelmiştir. Bilgi saklama ortamları olarak çoğunlukla kâğıt kullanıldığı zamanlarda güvenlik önlemleri olarak fiziksel güvenlik önlemlerine ağırlık verilmiş, ancak, gelişen teknolojiler kullanılarak bilgilerin dijital ortamlarda, veritabanlarında, CD, Çıkarılabilir Disk gibi saklama ortamlarında 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 açıklıklara neden olması, kurumlarda bilgi güvenliğine olan ihtiyacı gün geçtikçe daha fazla artırmaktadır. Bilgi güvenliğine duyulan ihtiyaçla birlikte, güvenliğin sağlanması için bilinçli personel barındırmak ve güvenlik sürecinin işletilmesi için yeterli doküman ve yöntemlerin oluşturulması da bir zorunluluk olmuştur.

Bilgi güvenliği, bu politikada aşağıdakilerin korunması olarak tanımlanır:

- Gizlilik: Bilginin sadece erişim yetkisi verilmiş kişilere erişilebilir olduğunu garanti etmek;
 - Bütünlük: Bilginin ve işleme yöntemlerinin doğruluğunu ve yetkisiz değiştirilememesini temin etmek;
 - Erişilebilirlik: Yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara en hızlı şekilde erişebileceklerini garanti etmek.
- Bilgi güvenliği politikası dokümanı, yukarıdaki korumaları ve gereksinimleri sağlayabilmek için oluşturulmuş denetimlerin uygulanması sırasında kullanılacak en üst seviyedeki prensiplerin belirtildiği dokümandır.

1.2. Bilgi Güvenliği Amaçları


Bilgi sistemleri güvenlik gereksinimleri düşünülerek tasarlanmıştır. Sürekli iyileştirmeler yapılarak çalışmaların devamlılığı sağlanmaktadır. Firmamızda uygulanan Bilgi Güvenliğinin amacı uygun ve etkili prensip ile politikalar kullanarak bilgi sistemlerinin güvenlik seviyesini artırmaktır.

Firmamızın bilgi güvenliğinin hedefi, her seviyede kullanıcıya bilgi sistemleri kullanımları sırasında ne şekilde hareket etmeleri gerektiği konusunda yol göstermek, kullanıcıların bilinç ve farkındalık seviyelerini artırmaktır. Böylece bilgi sistemlerinde oluşabilecek riskleri minimuma indirmek, kurumun güvenilirliğini ve imajını korumak, üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak, kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamaktır.

Bu bağlamda kullanıcılara sürekli eğitimler verilmektedir.

Kurumun risk yönetim çerçevesi, bilgi güvenliği risklerinin tanımlanmasını, değerlendirilmesini, işlenmesini kapsar. Risk değerlendirmesi, uygulanabilirlik bildirgesi ve risk işleme planı, bilgi güvenliği risklerinin nasıl kontrol edildiğini tanımlar.

HAZIRLAYAN	ONAYLAYAN
BİLGİ TEKNOLOJİLERİ YÖNETİCİ YARDIMCISI	GENEL MÜDÜR YARDIMCISI

	BİLGİ GÜVENLİĞİ POLİTİKASI			
KOD NO	YAYIN TARİHİ	REVİZYON NO	REVİZYON TARİHİ	SAYFA
Y-BG.AŞ.PT.01-YG	15.08.2016	0	-	4/16

1.3. Bilgi Güvenliği Kapsamı

BGYS kapsamı olarak, firmamızın bilgi işlem varlıklarını ve süreçlerini, kapsamaktadır.

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

2. Yönetimin Desteği

BGYS kurulurken BGYS komitesi tarafından BGYS Sorumlusu ve BGYS Yöneticisi atanmıştır. BGYS Sorumluluğu ve Yöneticiliği kurum üst yöneticilerinden oluşmaktadır. BGYS Sorumlusu değiştiğinde, işten ayrıldığında üst yönetim tarafından doküman revize edilerek atama tekrar yapılmalıdır. BGYS sorumlusunu belirlemek ve değiştirmek üst yönetimin yetkisindedir. BGYS Yöneticisini belirlemek ve ihtiyaç duyduğunda değiştirmek BGYS Sorumlusunun sorumluluğundadır.

Yönetim kademelerinde bulunan birim müdürlerinin güvenlik konusunda ısrarcı olmaları, alt kademelerde bulunan personele sorumluluk verme ve örnek olma konusunda yardımcı olmalıdır. Üst kademelerden başlayan ve uygulanan bir güvenlik anlayışıyla, kurumun en alt kademe personeline kadar inilmesi zorunludur. Bu yüzden kurumdaki müdürlüklerin, gerek yazılı gerekse sözlü olarak güvenlik yöntemlerine uymaları, güvenlik konusundaki çalışmalara katılmaları ve güvenlik ile ilgili çalışmalara destek olmaları gerekmektedir.

3. Güvenlik Politikası Dokümanı Güncellenmesi ve Gözden Geçirilmesi

Politika dokümanının sürekliliğinin sağlanmasından ve gözden geçirilmesinden BGYS Yöneticisi sorumludur.

Bilgi Güvenliği Politikası Dokümanı, 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 yenilenme (revizyon) değişimi olarak kayıt altına alınmalı ve her versiyon BGYS Sorumlusu ve Üst Yönetimine onaylatılmalıdır. Her sürüm değişikliği tüm kullanıcılara e-mail yolu ile ortak dosya paylaşım sunucusunda ve yardım masası sisteminde 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 Yöneticisi sorumludur.

BGYS Koordinasyon ekibi, BGYS Sorumlusu, BGYS Yöneticisi ve BGYS görevler tablosunda yer alan çalışanlardan oluşmaktadır. Bu koordinasyon toplantılarının amacı, ISO 27001 Bilgi Güvenliğinde alınan kararları birimlerde bulunan diğer personele aktarılmasıdır. Bu toplantılara BGYS Yöneticisi ve BGYS sorumlusu katılmak zorundadır.

HAZIRLAYAN	ONAYLAYAN
BİLGİ TEKNOLOJİLERİ YÖNETİCİ YARDIMCISI	GENEL MÜDÜR YARDIMCISI

	BİLGİ GÜVENLİĞİ POLİTİKASI			
KOD NO	YAYIN TARİHİ	REVİZYON NO	REVİZYON TARİHİ	SAYFA
Y-BG.AŞ.PT.01-YG	15.08.2016	0	-	5/16

Diğer personel gerekli olan durumlarda toplantılara katılmalıdır. BGYS Koordinasyon ekibi en az senede bir kez toplanmalıdır. Önemli bir güvenlik olayı olduğu zamanda da olağanüstü toplanmalıdır. BGYS Yöneticisi, BGYS Koordinasyon Ekibinin toplanmasından sorumludur.

Toplantı gündemi aşağıdaki maddeleri içermelidir.

- 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 yöneticisi, yukarıda belirtilen gündeme konu ekleyebilir, gündemden konu çıkarabilir gündem ve toplantı tarihini bir başka tarihe erteleyebilir. Gerekli görüldüğünde Lezita ve şirketin diğer lokasyonlarında bulunan yetkilileri de toplantıya davet edebilir.

BGYS Komitesi BGYS Sorumlusu ya da BGYS Yönetici başkanlığında ya gerekli gördüğü zamanlarda ya da belirli aralıklarla toplanır

4.2. Üçüncü Şahısların Bilgiye Erişimi

Firmamızın personeli olmayan üçüncü tarafların, bilgi sistemlerini kullanma ihtiyacı olması durumunda (ör: kurum dışı bakım onarım personeli vb.) BGYS Yöneticisi, bu kişilerin kurum 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. Gerekli takdirde bakım personelinin politikaya uyması için süre tahsis edilmelidir. Gizlilik sözleşmesi ve Bilgi Güvenliliği sözleşmesi imzalanacak firma ve kişileri, acil olduğu durumlarda BGYS Yöneticisi normal koşullarda ise BGYS Komitesi belirler.

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.

- Kurum bünyesinde kullanılmakta olan her bir varlık, envanter kayıtlarına geçirilmelidir.
- Envanter kayıtları sürekli olarak güncel tutulmalı ve yeni varlıklar, envanter kayıtlarına hemen girilmelidir.
- Varlık kapsamında değerlendirilen 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. Bu şekilde, kullanıcılar bilgi varlığının sahibinden ve sınıflandırmasından haberdar olacaklardır.

HAZIRLAYAN	ONAYLAYAN
BİLGİ TEKNOLOJİLERİ YÖNETİCİ YARDIMCISI	GENEL MÜDÜR YARDIMCISI

	BİLGİ GÜVENLİĞİ POLİTİKASI			
KOD NO	YAYIN TARİHİ	REVİZYON NO	REVİZYON TARİHİ	SAYFA
Y-BG.AŞ.PT.01-YG	15.08.2016	0	-	6/16

- Bilgi varlıklarının sınıflandırılmasından ve bu sınıflandırmanın belirli zamanlarda gözden geçirilmesinden BGYS Yöneticisi sorumludur. Gerektiğinde BGYS yöneticisi sınıflandırmayı belirleyebilir veya belirlemek üzere BGYS Komitesi'ne aktarabilir.

- Erişim kontrol ve ağ hizmetleri kullanım talimatı (Y-BG.AŞ.T.03-YG) ve risk analizi tedavi planı hazırlanırken varlık envanteri listesi göz önünde bulundurulmalıdır.

6. Personel Bilgi Güvenliği

- Tüm çalışanlar, kurumun bilgi güvenliği politikalarına uymakla yükümlüdürler. Kullanıcılar, politikalara uygun olmayan davranışları sonucu meydana gelebilecek bilgi sistemleri olaylarından sorumlu olacaklardır.

- Kurum çalışanları, kurum personeli olduğu sürece ve kurumdan ayrılmaları (emeklilik, istifa, vs.) durumlarında kurum bilgilerini gizlilik prensibine uygun olarak korumaktan sorumludur.

- İşten ayrılan veya kurum içinde görev değişikliği olan personel için kullanıcı hesaplarının silinmesi, erişim yetkilerinin değiştirilmesi gibi gerekli kontroller hemen yapılmalıdır.

- Üçüncü şahıslar da dâhil olmak üzere, Firmamızın bilgi sistemlerini kullanması gereken her personel için varlık ve kaynakların doğru kullanımı da dâhil olmak üzere uygun güvenlik politikaları ve prosedürleri konusunda gerekli taahhütnameler hazırlanmalı ve ilgili personele imzalatılmalıdır.

- Kullanıcı adı açılmış tüm kurum personeline farkındalık eğitimi verilmelidir. Bu eğitimler, her yeni personel alımı sonrasında yeni personel için de tekrarlanmalıdır.

7. Fiziksel Güvenlik

7.1. Güvenlik Korunmalı Bölgeler

- Kritik veya hassas iş faaliyetlerini desteklediği belirlenen tüm bilgi teknolojisi araçları, fiziksel erişim kontrolü gerektiren alanlarda bulunmalıdır.

- Tüm personel, Sistem Odası Güvenlik Prosedürüne (Y-BG.AŞ.T.05-YG) uygun davranmalıdır. Giriş izni olmayan alanlara girmemeleri gerektiği unutturulmamalıdır.

- Güvenli alanlara alınacak ziyaretçilere atanmış kurum 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 izinli personel dışındaki tüm kişilerin giriş ve çıkış saatleri ziyaret defterine kaydedilmelidir.

7.2. Donanımsal Güvenlik


- Personel, önemli varlıkların bulunduğu güvenli alanlarda sigara içmemeli, yiyecek ve içeceklerle güvenli alana girmemelidir.

- Bilgi teknolojisi araçlarının, herhangi bir elektrik kesintisinde çalışmalarına devam etmeleri için kullanılan UPS, jeneratör gibi güç kaynakları yılda en az iki defa olmak üzere periyodik olarak üreticinin talimatlarına uygun biçimde kontrol edilmelidir.

Güç kaynaklarının sağlıklı şekilde çalışabilmesi için gerekli tedariklerin önceden planlanarak tedarik edilmesi sağlanmalıdır.

- Tüm donanımların, elverişliliği ve güvenilirliği garanti etmek amacıyla üretici firmanın talimatlarına uygun olarak, düzenli periyotlarla bakımları yapılmalıdır.

HAZIRLAYAN	ONAYLAYAN
BİLGİ TEKNOLOJİLERİ YÖNETİCİ YARDIMCISI	GENEL MÜDÜR YARDIMCISI

	BİLGİ GÜVENLİĞİ POLİTİKASI			
KOD NO	YAYIN TARİHİ	REVİZYON NO	REVİZYON TARİHİ	SAYFA
Y-BG.AŞ.PT.01-YG	15.08.2016	0	-	7/16

- Dizüstü bilgisayar, belge, CD ve taşınabilir bellek gibi taşınabilir kurum 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 kurum dışına çıktığı durumlarda da sorumludurlar.

- Kurum dışına çıkarılabilen varlıklar kurum dışında çalışırken gizlilik prensipleri ve varlık sınıflandırmaları göz önünde bulundurulmalıdır.

- Personel, kendisine ait varlıkları (şahsi dizüstü bilgisayar, tablet vb) BGYS Yöneticisinden habersiz kurum sistemlerine sokamaz.

- Hassas bilgiler içeren depolama aygıtları, "Hassas Ortam ve Teçhizat İmha Talimatı"na (Y-BG.AŞ.T.04-YG) uygun olarak işlenmelidir.

7.3. Genel Güvenlik Denetimleri

- Kullanıcılar, kullanmadıkları zamanlarda ekranlarının izinsiz kişilerce görülmesini engellemek için işletim sisteminin ekran kilitlemesi özelliğini etkin hale getirmek gibi gerekli önlemleri almalıdırlar. İlkenin tam olarak uygulanması için, merkezi olarak buna uygun kurallar bütün kullanıcı bilgisayarları ve sunuculara dağıtılmalıdır.

- Kurum kullanıcıları, kendilerine verilmiş olan kullanıcı adı ve şifrelerinin sadece kendileri tarafından kullanılması ilkesini koruma sorumluluğuna uymalıdırlar. Bu ilkenin ihlali durumunda kullanıcı sorumlu olacaktır.

- Varlık sınıflandırmasında hassas bilgi olduğu belirlenen dokümanların kâğıt baskılarının erişim yetkisi olmayan kişilerce erişimini engellemek amacıyla kurum personeli tarafından temiz masa politikası uygulanmadır. 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 alınmalıdır.

- Kullanıcıların çalıştıkları ortamdaki masa ve dolap çekmecelerini kilitli tutmaları ve anahtarları sorumlu kişiler haricinde kimseyle paylaşmamaları gerekmektedir.

-

-Kurum cihazları güvenlik açısından gerekli görüldüğünde merkezi olarak kontrol edilebilecektir.

8. Sistemlerin İşletim Güvenliği

8.1. İşletim Prosedürleri

Kurum içi donanım ve uygulamaların işletim prosedürleri hazırlanmalı ve aşağıdaki hususlara uyulmalıdır:

- Yazılı prosedürler ihtiyaç duyulduğunda BGYS Yöneticisi tarafından hazırlanır ve BGYS sorumlusu tarafından onaylanarak geçerlilik kazanmalıdır.

- Onaylı olmayan işletim prosedürleri geçersizdir.

- Kurum genelinde tüm kritik 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 Prosedürleri

- Herhangi bir güvenlik olayı başlangıcında, sırasında ve sonrasında yapılması gereken adımları içeren Y-BG.AŞ.T.01-YG uygulanmalıdır.

HAZIRLAYAN	ONAYLAYAN
BİLGİ TEKNOLOJİLERİ YÖNETİCİ YARDIMCISI	GENEL MÜDÜR YARDIMCISI

	BİLGİ GÜVENLİĞİ POLİTİKASI			
KOD NO	YAYIN TARİHİ	REVİZYON NO	REVİZYON TARİHİ	SAYFA
Y-BG.AŞ.PT.01-YG	15.08.2016	0	-	8/16

- Bilgi güvenliği ihlal olayı olarak değerlendirilen her durum için düzeltici önleyici faaliyet formu oluşturulmalı ve yardım masası ortamına 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 geçirilmeli. Yetersizlik veya ihtiyaç durumlarında değişim planlaması yapılarak satın alma süreci başlatılmalıdır.

8.5. Kötü Niyetli Yazılımlara Karşı Korunma

Kurum genelinde kötü niyetli yazılımlara karşı gerekli korunma önlemleri alınmakta ve altyapı yeni tehditlere karşı sürekli olarak gözden geçirilip güncellenmektedir. Gerekli görülen ek önlemler BGYS komite toplantısında tartışıldıktan ve gerekli testleri yapıldıktan sonra sisteme entegre edilmelidir. Ancak, kullanıcılar önlemlere güvenerek sistemi savunmasız bırakacak biçimde hareket etmemelidir.

8.6. Ağ Yönetimi

- Tüm ağ (ana omurga ve aktif cihazlar) yönetimi yapılanması ve kurulumu IT ekibi tarafından yapılmaktadır.
- Kurum ağı içerisinde ayrı Vlan yapıları olması zorunludur. Kritik sistemler ve kullanıcı bilgisayarları farklı Vlan üzerinde bulunmalıdır.
- Kurum ağı içerisinde kullanıcılar sadece gerekli olan sunuculara erişimleri bulunmakla birlikte sadece gerekli olan portlara erişimleri olmalıdır.
- Ağ altyapı elemanlarında kimlik doğrulama açık olmalıdır. Anahtarlama cihazında kimlik doğrulama; cihaza yönetimsel veya denetimsel erişim söz konusu olduğu zaman kişinin doğru kişi olup olmadığının kontrolüdür.
- Ağ altyapı cihazlarına fiziksel erişim ile (konsol bağlantısı ile) veya uzaktan erişim (ssl, ssh üzerinden) güvenli kanallar üzerinden bağlantıları için kimlik kontrolü yapılmalıdır.

8.7. Bilgi Ortamı Yönetimi ve Güvenliği

- Taşınabilir ortamdaki bilgi artık kullanılmıyorsa, silinmelidir.
- Gerekli olmadığı sürece bilgi varlıkları yetkisiz kişilerle paylaşılmamalıdır.
- İşlemlerin, prosedürlerin, veri yapılarının, yetkilendirme işlemleri gibi hassas bilgilerin bulunduğu sistem dokümantasyonu, yetkisiz kişilerin erişimini engellemek amacıyla güvenli ortamlarda buldurulmalı, elektronik kopyalarına iç ağ üzerinden ilgili kişilerin erişebileceği şekilde Y-BG.AŞ.T.03-YG 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 güvenli paketleme, güvenli kurye kullanma veya elektronik ortamlar için sayısal imzalama ve şifreleme kullanma gibi önlemler olabilir.

HAZIRLAYAN	ONAYLAYAN
BİLGİ TEKNOLOJİLERİ YÖNETİCİ YARDIMCISI	GENEL MÜDÜR YARDIMCISI

	BİLGİ GÜVENLİĞİ POLİTİKASI			
KOD NO	YAYIN TARİHİ	REVİZYON NO	REVİZYON TARİHİ	SAYFA
Y-BG.AŞ.PT.01-YG	15.08.2016	0	-	9/16

- E-posta hizmetlerini kullanan tüm kurum personeli, e-postaların güvenliğini sağlamak amacıyla oluşturulmuş olan Varlıkların Kabul Edilebilir Kullanımı Talimatı'nda (Y-BG.AŞ.T.02-YG) belirtilen kurallara uymakla yükümlüdürler

- Web sitesi, çevresel bilgi sistemi ve diğer yollarla İnternet üzerinde bulunan halka açık kurum bilgilerinin izinsiz olarak değiştirilmesine, eklenmesine veya silinmesine karşı gerekli koruma önlemleri alınmalı ve yetkilendirmeler yapılmalıdır.

- Özel yazılımlarla paylaşım alanlarına yapılan bağlantılar kullanıcı adı ve şifre korumalı olmalı paylaşım alanı üzerindeki her türlü hareket kayıt altına alınmalıdır. Paylaşım alanına özel erişimler için destek ortamına kayıt açılmalı ve BGYS Yöneticisi onayı alınmalıdır.

9. Erişim Denetimi

9.1. Gereklilikler

- Firmamızın Bilgi Sistemlerini kullanan tüm kurum personeli, hizmet sağlayıcı kurum dışı personel ve diğer üçüncü şahıslar Erişim Kontrol ve Ağ Hizmetleri Kullanım Talimatı'na (Y-BG.AŞ.T.03-YG) uymakla yükümlüdürler.

9.2. Kullanıcı Erişimi 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 bir taahhütname imzalatılarak erişim haklarıyla ilgili bilgi verilmektedir.

- İşten ayrılan personel için gerekli hesap kapatma, birim değiştiren kullanıcıların ise erişim haklarının düzenlenmesi işlemleri hemen yapılmalıdır.

- Gereksiz kullanıcı hesaplarının kontrol edilmesi ve kaldırılması işlemi ayda en az bir defa yapılmalıdır.

- Kullanıcıların erişim hakları her değişiklikten sonra veya belirli aralıklarla gözden geçirilmelidir.

- Kullanıcıların sunuculara olan yetkisiz erişim denemeleri ile hak sahibi personelin erişimleri güvenlik yazılımlarıyla kontrol edilmeli, gerektiği takdirde erişimler ve erişim denemeleri rapor edilmelidir.

9.3. Ağ Erişimi Denetimi

- Ağ hizmetler Ağıni kullanan tüm personel ve üçüncü taraflar, Erişim Kontrol ve Ağ Hizmetleri Kullanım Talimatı'na (Y-BG.AŞ.T.03-YG) uymalıdır.

9.4. İşletim Sistemi Erişimi Denetimi

- Başarısız oturum girişimleri güvenlik yazılımları tarafından kaydedilip, gerektiğinde incelenmek üzere saklanmaktadır.

- BGYS yöneticisi tarafından onaylı olmayan ve lisanssız yazılımların kullanıcı bilgisayarlarına yüklenmesi yasaktır.

9.5. Uygulama Erişimi Denetimi

- Uygulama sistemlerinin kullanıcıları, erişim isteklerini ilgili formu doldurup bağlı buldukları birim müdürünün imzalı onayı ile BGYS yöneticisine ileterek erişim yetkisi talebinde bulunurlar ve sadece onay verilen kısma ulaşabilirler.

- Uygulamalara erişimler, merkezi kayıt izleme yazılımına yönlendirilmeli ve saklanmalıdır.

HAZIRLAYAN	ONAYLAYAN
BİLGİ TEKNOLOJİLERİ YÖNETİCİ YARDIMCISI	GENEL MÜDÜR YARDIMCISI

	BİLGİ GÜVENLİĞİ POLİTİKASI			
KOD NO	YAYIN TARİHİ	REVİZYON NO	REVİZYON TARİHİ	SAYFA
Y-BG.AŞ.PT.01-YG	15.08.2016	0	-	10/16

9.6. Dışarıdan Sisteme Erişim Denetimi

Dış ağlardan kurum 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.

10.2. Sistemlerde Güvenlik

- 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 denedikten ve operasyonel sistemlerde bir problem çıkartmadığına emin olunduktan sonra işletim ortamına aktarılmalıdır.

- Testler için kullanılmakta olan verilerin sahibi atanmıştır. 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 (Y-BG.AŞ.T.03-YG) sıkı bir şekilde uygulanmalıdır.

11. İş Sürekliliği Yönetimi

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

İş sürekliliği yönetim sürecinde oluşturulan takımlar, belirli aralıklarla toplantı yapmalı ve sistemi gözden geçirmelidirler.

12. Uyum Süreci

12.1. Yasal Gereksinimlere Uyum

- Firmamızca uygulanan bilgi güvenliği politikası, yürürlükteki tüm kanunlarla uyumlu olmak zorundadır.

- Firmamızda kullanılmakta olan tüm yazılımların lisans sözleşmeleri olmak zorundadır. Lisanssız ürünlerin kurum varlıklarında kullanılması yasaktır.

- Herhangi bir bilişim suçu işlediği saptanan personel, yasalara uygun olarak cezai işlem görür.


- Bilişim suçları kapsamı yasalar takip edilmeli, yasal düzenlemelerde bilgi güvenliği politikasını etkileyen bir değişiklik belirtildiğinde, politika güncellenmelidir.

- 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

HAZIRLAYAN	ONAYLAYAN
BİLGİ TEKNOLOJİLERİ YÖNETİCİ YARDIMCISI	GENEL MÜDÜR YARDIMCISI

	BİLGİ GÜVENLİĞİ POLİTİKASI			
KOD NO	YAYIN TARİHİ	REVİZYON NO	REVİZYON TARİHİ	SAYFA
Y-BG.AŞ.PT.01-YG	15.08.2016	0	-	11/16

denetleme aracı sahibi, Erişim Kontrol ve Ağ Hizmetleri Kullanım Talimatı (Y-BG.AŞ.T.03-YG) kullanılarak gerekli önlemlerin alındığını kontrol etmelidir.

13. Teknik Güvenlik İlkeleri

13.1. Kullanıcı Parola Politikası

- Tüm kullanıcılar etki alanına dâhil olan donanımlarında Firmamız tarafından sağlanan hizmetlerden faydalanmak için sisteme login (giriş yapmalı) olmalıdır. Tüm kullanıcıların kullanıcı-kimliği (user-ID) (varsa e-anahtarı) ve sadece kullanıcının bildiği şifre ile kimlik doğrulamasının yapılması zorunludur.

- Kullanıcıların şifreleri en az 8 karakterli olmalıdır, büyük harf, küçük harf, noktalama işareti ve rakam özelliklerinden en az üçünü içeren karmaşık şifreler belirlenmelidir.

- Kullanıcı şifreleri 42 gün süreyle geçerli olup geçerlilik süresi dolduğu zaman veya parolanın güvenliğe olmadığına dair bir gösterge olduğu zaman (ör: saldırılar, çalınma şüphesi, Truva atı bulunması, vs.) değiştirilmelidir.

- Kullanıcıya verilen ilk şifre veya şifresini unuttuğu zaman verilen şifreler "geçici şifre" olarak düşünülmeli ve ilk oturum açılışında hemen değiştirilmelidir.

- Kurum personeli şahsi şifrelerini ve var ise e-anahtarını özel kontrol altında tutmalı, şifrelerini sistem yöneticisi de dâhil olmak üzere hiç kimseye paylaşmamalıdır.

- Kullanıcılar, kurum servisleri için kullandıkları şifreleri, İnternet üzerinde başka amaçlar için (örneğin tartışma gruplarına üyelik, gmail gibi bedava e-posta hesapları için) kullanmamalıdır.

- Şifreler, dosya, otomatik komut dosyası (log-in script), yazılım makrosu, erişim kontrolü olmayan bilgisayarlar ve yetkisiz personelin fark edebileceği yerlere (kâğıt üzerine yazarak bilgisayarın yanına bırakmak gibi) yazılmamalıdır.

- Kullanıcılar, bilgisayarlarını veya terminallerini kilitlemeden kullanılır durumda bırakmamalıdır.

- Kullanıcılar, kullanmaya kısa süreli ara verdikleri bilgisayarları veya terminalleri parola korumalı ekran koruyucu gibi özellikler kullanarak güvenlik altına almakla yükümlüdürler. Sistem tarafında da kullanılmayan bilgisayarların 5 dk. sürede ekran kilitlemesine otomatik geçişi sağlanmaktadır.

- Etki alanı denetçileri kullanıcıların belirtilen sürelerde şifrelerini değiştirmeye zorlanmalıdır.

13.2. İnternet ve E-Posta Kullanım İlkeleri

Firmamızın. İnternet Sistemi yalnızca iş faaliyetlerini destekleyecek şekilde kullanılmalıdır.

İnternet kullanımı;

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

- Kullanıcıların İnternet kullanım yoğunluğu diğer kullanıcıların İnternet'e ulaşmalarını engelleyecek şekilde olmamalıdır. Güvenlik yöneticileri, sistem yöneticileri ve bilgisayar operatörleri gibi sistem bakım-idame işlerini yürüten personele ayrıcalıklar tanınabilir.

- İnternet kullanımı, içerik kontrolcülerini ve virüs tespit sistemleri kullanılarak sınırlandırılmaktadır. Kullanıcılar, bu kontrollerin yapıldığını bilerek İnternet'i kullanmalı, güvenlik amacıyla konulan önlemleri devre dışı bırakmaya çalışmamalıdır.

- Çalışanlar kendi kullandıklarına 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.

HAZIRLAYAN	ONAYLAYAN
BİLGİ TEKNOLOJİLERİ YÖNETİCİ YARDIMCISI	GENEL MÜDÜR YARDIMCISI

	BİLGİ GÜVENLİĞİ POLİTİKASI			
KOD NO	YAYIN TARİHİ	REVİZYON NO	REVİZYON TARİHİ	SAYFA
Y-BG.AŞ.PT.01-YG	15.08.2016	0	-	12/16

- Elektronik mesajlarda veya göndermelerde ihtiva edilen kullanıcı adı, elektronik posta adresi, organizasyonel bağlantı ve ilgili bilgi, mesajı yazan kişiyi yansıtmalıdır.
- Firmamızın fiziksel sınırları içerisinde, kurum tarafından verilen internet hizmeti dışında, alternatif internet hizmeti kullanılamaz.
- Kuruma ait 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 Firmamızın politikasının bir parçası değildir. Ancak Firmamız şüphelenilen mesajların incelenme hakkına ve yetkisine sahiptir. Bununla birlikte Internet üzerinden yapılan elektronik haberleşmenin içeriği izlenebilir ve elektronik haberleşme sistemlerinin kullanımı işlevsel, bakım, teftiş, güvenlik, araştırma faaliyetlerini desteklemek için izlenebilir.
- Genellikle kabul edilen iş uygulamalarına uyumlu olarak, firmamızın elektronik haberleşme ile ilgili istatistiksel bilgiler toplama hakkına sahiptir. Bu bilgileri kullanarak teknik bu sistemlerin devam eden güvenilirliğini ve kullanılabilirliğini emniyet altına almak için izlenebilmektedir. Bu yüzden personel, firmamız 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 yaratabilir.
- Kurum e-posta sunucusuna gelen mesajlar spam tarayıcısından geçirildikten sonra kullanıcılara ulaştırılmaktadır, ancak yine de kullanıcılar, e-posta vasıtasıyla bulaşabilecek 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 Bilgi Güvenliği İhlal Olayı Bildirim ve Yönetim Talimatı'na (Y-BG.AŞ.T.01-YG) uygun olarak rapor etmekle sorumludurlar. Kullanıcıların, diğer kullanıcılara ister kurum içinde olsun ister kurum dışında olsun, şirket e-mail adreslerini kullanarak kurum haberleşme bilgileri harici gönderimler için Firmamızın sistemlerinden faydalanmaları yasaklanmıştır.
- 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.
- Uzun süreli saklanması gerekli olmayan mesajlar periyodik olarak kullanıcılar tarafından kişisel elektronik mesaj saklama alanlarından silinmelidir. Belirli bir süreçten sonra çok kullanıcı sistemlerinde saklanan elektronik mesajlar otomatik olarak sistem yönetim personeli tarafından silinecektir. Bu, az olan saklama alanını çoğaltmakla kalmayıp, kayıt yönetimini ve ilgili faaliyetleri de kolaylaştıracaktır.
- Firmamız bilgisayarlarına veya ağlarına gönderilen her türlü bilgiyi sansür etme yetkisini saklı tutar. Firmamız suç veya kanunsuz olması muhtemel olarak görülen her türlü malzemeyi kendi bilgi sistemlerinden çıkarma hakkını ve bununla ilgili resmi işlem başlatma hakkını saklı tutar.

13.3. Virüs ve Zararlı İçerikten Korunma İlkeleri

- Firmamızın bilgisayar ağına bağlı olarak çalışan bilgisayarlara anti-virüs programının yüklenmesi zorunludur. Eğer personelin bilgisayarında bu yazılım yok ise ya da güncelliğini yitirmiş ise bunu IT ekibine bildirmekle yükümlüdür.
- Kullanıcı, anti-virüs yazılımının ve imza tablolarının güncelliğini kontrol etmekten, belirli periyotlarla virüs taramaları yapmaktan IT ekibi sorumludur.
- Anti virüs programı, kullanıcıların kişisel bilgisayarına önceden tanımlanmış standart yapılandırma değiştirilemeyecek şekilde kurulur. Bu yapılandırmanın, bilgisayarı kullanan personel tarafından değiştirilmesi yasaktır. Eğer değişimin yapılması söz konusuysa, değişiklik için IT ekibine bildirilmesi zorunludur.

HAZIRLAYAN	ONAYLAYAN
BİLGİ TEKNOLOJİLERİ YÖNETİCİ YARDIMCISI	GENEL MÜDÜR YARDIMCISI

	BİLGİ GÜVENLİĞİ POLİTİKASI			
KOD NO	YAYIN TARİHİ	REVİZYON NO	REVİZYON TARİHİ	SAYFA
Y-BG.AŞ.PT.01-YG	15.08.2016	0	-	13/16

- 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 IT ekibine haber vermelidir. Eğer şüphelenilen virüs, bilgilere ve yazılıma zarar vermeye başlarsa, personel hemen bilgisayarı kapatmalıdır ve müdahale yapılmasını beklemelidir.

- Dışarıdan temin edilen CD ve benzeri ortamlar virüs, solucan veya Truva Atı 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.

- BGYS yöneticisi virüs istilası ve sistem arızaları gibi acil durumları kontrol altına alabilmek için özel kullanıcı dosyalarını inceleme yetkisine sahiptir. Kullanıcı dosyaları bu şekilde incelendiğinde, buna dâhil olan kullanıcı(lar) bilgilendirilme yapıldıktan sonra incelenecektir.

- Kullanıcıların, Firmamız bilgisayar sistemlerine zarar verebilecek herhangi bir bilgisayar kodunu kasıtlı olarak yazmaları, çoğaltmaları, kopyalamaları, üretmeleri, çalıştırmaları ya da tanıtılmaları yasaktır.

13.4. Taşınabilir Cihazlar Kullanım Politikası

- Taşınabilir cihazlar; kurum bilgisi taşıyan her türlü dizüstü bilgisayar, akıllı telefon, 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.

- Kurum dışına çıkarılabilen varlıklar kurum 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 kurum varlıklarının korunması için gerekli önlemlerin alınmasından envanter sisteminde varlık sahibi olarak kaydedilmiş kişi sorumludur. Herhangi bir kaybolma veya çalınma durumunda da Y-İK.PR.11-YG prosedüründe belirtilen şekilde hareket edilir.

- Dizüstü bilgisayarlarda virüs taramaları en az iki haftada bir kez yapılmalı, virüs güncellemeleri çevrimdışı olarak kurum bilgi sistemleri üzerinden gerçekleştirilmelidir.

- Personelin kullanımı için tahsis edilmiş olan dizüstü bilgisayar, mobil cihazlar, tablet vb. sadece yetkilendirilmiş personel tarafından ve veriliş amaçları doğrultusunda kullanılmalıdır. IT ekibi tarafından kullanılan yazılımlar ile kullanıcıların mobil cihazlarda kısıtlanması sağlanabilir.

- Kurum bilgi sistemleri kapsamında üretilen her türlü bilginin USB Bellek, CD vb. ortamlarda saklanması kesinlikle yasaktır. Böyle bir durum gerekliliğinde BGYS Yöneticisinin onayının alınması zorunludur.

13.5 Sosyal Medya Kullanım Politikası


- Kurum mobil cihazları ve bilgisayarları ile kuruma ait herhangi bir doküman, belge, fotoğraf ve benzeri bir paylaşım yapılması yasaktır.

- Kurum çalışanları kendi mobil cihaz ve bilgisayarları ile kuruma ait herhangi bir doküman, belge, fotoğraf ve benzeri bir paylaşım yapılması yasaktır.

- Firmamızın bilgisayar ve iletişim sistemleri, personelin söz özgürlüğü hakkı için kullanılmamalıdır. Aksi davranışlar resmi soruşturmaya yol açar.

- Personelin elektronik posta sistemine, elektronik ilan tahtasına (mevcut ise) ya da diğer elektronik sistemlere gönderdiği yorumlar her zaman firmamızın ya da firmamızın resmi pozisyonunun resmi ifadeleri olmak durumunda değildir.

HAZIRLAYAN	ONAYLAYAN
BİLGİ TEKNOLOJİLERİ YÖNETİCİ YARDIMCISI	GENEL MÜDÜR YARDIMCISI

	BİLGİ GÜVENLİĞİ POLİTİKASI			
KOD NO	YAYIN TARİHİ	REVİZYON NO	REVİZYON TARİHİ	SAYFA
Y-BG.AŞ.PT.01-YG	15.08.2016	0	-	14/16

13.6 Bulut Sistemleri Kullanım Politikası

- Kurum içerisinde kurum ekipmanları ile iş kapsamı dışında bulut depolama hizmetlerinin (Dropbox, Gdrive, Onedrive, Box, vb.) kullanılması yasaktır. Böyle bir durum gerekliliğinde BGYS Yöneticisinin onayının alınması zorunludur.

- Kurum verilerinin güvensiz bulut hizmetlerinde (Megaupload, WeTransfer vb.) yetkisiz kişiler tarafından saklanması yasaktır. Böyle bir durum gerekliliğinde BGYS Yöneticisinin onayının alınması zorunludur.

14. Kullanıcı Bilgi Güvenliği Eğitimi

Aşağıdaki konuları kapsayan eğitimin, tüm kurum kullanıcılarına verilmesi gerekmektedir. Böylece güvenlik ilkeleri anlayışının kuruma dağıtılması ve yaşatılması sağlanır:

- Bilgi güvenliği politikası eğitimi:
 - Bilgi güvenliğinin tanımı, gerekliliği
 - Firmamızın bilgi güvenliğinin hedefleri
 - Firmamızın Bilgi Güvenliği Politikasının Tanıtımı ve politikaya uyulmasının önemi
- Kullanıcı güvenlik eğitimleri
 - Virüslerden, Truva atlarından korunma yolları
 - Zararlı e-postalardan korunma yolları
 - Güçlü şifreler seçme ve bunları güvenli saklama yolları
 - Temiz ekran ve temiz masa politikalarının önemi
- Kurum gizliliğini sağlama bilinci için gerekli bilgiler
- Güvenlik olayı gözlemlenmesi durumunda kullanıcıların izlemesi gereken prosedürler.

Aşağıdaki konuları kapsayan eğitimin, tüm kurum kullanıcılarına verilmesi gerekmektedir. Böylece güvenlik ilkeleri anlayışının kuruma 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.
- IT personeli BGYS ile ilgili ve mesleki gelişimleri ile ilgili eğitimlere katılmalıdır.

15. Roller ve Sorumluluklar

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

Bilgi Güvenliği Politikasının hazırlanması, gözden geçirilmesi ve güncellenmesinden Bilgi Güvenliği Yöneticisi ve Kalite Yönetim Temsilcisi sorumludur. IT ekibi, Bilgi Güvenliği Politikasını onaylar ve duyurulmasını sağlar.

15.1. Kurum Üst Yönetim Sorumlulukları

- Güvenlik Politikasının kurum içinde uygulanmasına destek vermek.
- BGYS sorumlusunu atamak.
- Risk değerlendirme yaklaşım dokümanını onaylamak.
- Risk analizinde kritik seviyenin üstündeki riskleri onaylamak.

15.2. Birim Müdürlerinin Sorumlulukları

- Kendisine bağlı çalışan personelin erişim yetkilerini onaylamak,

HAZIRLAYAN	ONAYLAYAN
BİLGİ TEKNOLOJİLERİ YÖNETİCİ YARDIMCISI	GENEL MÜDÜR YARDIMCISI

	BİLGİ GÜVENLİĞİ POLİTİKASI			
KOD NO	YAYIN TARİHİ	REVİZYON NO	REVİZYON TARİHİ	SAYFA
Y-BG.AŞ.PT.01-YG	15.08.2016	0	-	15/16

- Kendisine bağlı kısımda çalışacak üçüncü taraf bilgi sistemleri kullanıcıların politikalardan haberdar olmasını sağlamak,
- Fark ettiği veya kendisine çalışanları aracılığıyla iletilen bilgi sistemleri ile ilgili güvenlik problemlerini BGYS Yöneticisine bildirmek,
- Sahibi olduğu bilgi varlığını korumak ve gerektiğinde güncellemelerde bulunmak,
- Bilgi Güvenliği Politikasını uygulamak

15.3. BGYS Sorumlusu Sorumlulukları

- BGYS Yöneticisi tarafından hazırlanan Güvenlik Politikasını gözden geçirerek üst yönetimin onayına sunmak.
- BGYS Yöneticisini atamak.
- Eğitimleri planlamak ve gerçekleştirmelerini sağlamak
- BGYS Yöneticisinin hazırlamış olduğu dokümanları onaylamak ve uygulanmasını sağlamak.
- BGYS Yöneticisinin yapmış olduğu faaliyetleri kontrol etmek ve onaylamak.
- Gereken iyileştirmeler ve geliştirmeler konusunda üst yetkililere brifingler vermek,

15.4. BGYS Yöneticisi Sorumlulukları

- Bilgi güvenliği ile ilgili konularda bölümler ve dış servis sağlayıcıları arasında koordinasyonu sağlamak,
- Güvenlik Politikasının sahibi olarak, politikaların güncelleştirilmesinden ve uygulanmasından sorumlu olmak,
- BGYS Komitesinin gündemini belirlemek, alınan kararların uygulanmasını takip etmek,
- Kurum genelindeki 27001 kapsamındaki dokümanların Güvenlik Politikası prensiplerine uygun olarak yazılmasını sağlamak,
- İş sürekliliği planının işletilmesi, denetlenmesi ve testlerinin yapıldığını kontrol etmek,
- Acil durumlarda komite üyeleriyle yakın olarak çalışmak ve bilgi alışverişinde bulunmak,
- Güvenlik zaafı ve olaylarının nedenlerini araştırmak; gerektiği zamanlarda delilleri saklamak ve raporlar, önlemler ve iyileştirme önerilerinde bulunmaktan sorumludur.

15.5. Kurum Personelinin Sorumlulukları

- Çalışan personel için hazırlanmış roller ve sorumluluklarla ilgili dokümanlarında belirtilen görevleri yerine getirmek,
- İşleri gerçekleştirmek için kendisine verilmiş olan ayrıcalıklı kullanıcı kimlikleri var ise bu kimliği ve hakları sadece bu işi yaparken kullanmak,
- Sahibi olduğu bilgi varlığını korumak ve gerektiğinde güncellemelerde bulunmak, herhangi bir hata/arıza/olay olduğunda ilgili kişilere haber vermek,
- Bilgi Güvenliği Politikalarına uymak,
- Acil durum komite üyeleriyle yakın olarak çalışmak ve bilgi alışverişinde bulunmak,
- Bilgi güvenliği için kullanılan donanım ve yazılım kullanım talimatlarına uymak, alınan eğitimleri uygulamak ve yöntemler geliştirmek.
- Herhangi bir bilgi güvenliği olayını fark ettiğinde, zaman geçirmeden BGYS yöneticisine bilgi vermek ve yardım masası ortamına kayıt girmek.
- Kendisine ait olan hesapların şifrelerinin (varsa e-anahtarının) güvenliğini sağlamak,
- Taşınabilir cihazların güvenliğini sağlamak, yetkilendirme olmadan dışarı varlık çıkarmamakla sorumludur.
- Kuruma ait bilgi varlıklarının korunmasının sağlanması ve sahibi olduğu varlıkların sürekli kontrolünün sağlanması.

HAZIRLAYAN	ONAYLAYAN
BİLGİ TEKNOLOJİLERİ YÖNETİCİ YARDIMCISI	GENEL MÜDÜR YARDIMCISI

	BİLGİ GÜVENLİĞİ POLİTİKASI			
KOD NO	YAYIN TARİHİ	REVİZYON NO	REVİZYON TARİHİ	SAYFA
Y-BG.AŞ.PT.01-YG	15.08.2016	0	-	16/16

16. Yönetimin Onayı

Kurum yönetimi olarak; Güvenlik Politikasının uygulanmasının ve kontrolünün yapılmasının, güvenlik ihlallerinde de gerekli yaptırımın icra edilmesinin yönetim tarafından desteklendiğini beyan ederim.

.....

.....

17. Çalışan Onayı

Üstte yazan maddeleri okudum, anladım ve kabul ediyorum. (Lütfen bu ifadeyi el yazısıyla yazıp imzalayınız.)

HAZIRLAYAN	ONAYLAYAN
BİLGİ TEKNOLOJİLERİ YÖNETİCİ YARDIMCISI	GENEL MÜDÜR YARDIMCISI