

 DİLER DEMİR ÇELİK ENDÜSTRİ VE TİCARET A.Ş.	BGYS POLİTİKASI		Doküman No	P.05.16.01				
			Revizyon No	0				
			Revizyon Tarihi					
			Yayın Tarihi	01/03/2016				
			Sayfa No	1/2				
<input type="checkbox"/> Çok Gizli	<input type="checkbox"/> Gizli	<input checked="" type="checkbox"/> x	<input type="checkbox"/> Hizmete Özel	<input type="checkbox"/> Kişisel Özel	<input type="checkbox"/> Herkese Açık	<input checked="" type="checkbox"/> x	<input type="checkbox"/> Dahili	<input type="checkbox"/> Harici

1. AMAÇ

Bilgi Güvenliği Politikasının amacı, Diler Demir Çelik için temel bilgi güvenliği prensiplerini tanımlamaktır.

2. KAPSAM

Bilgi Güvenliği Politikasının kapsamı; Kapsam ve Sınırlar dokümanında tanımlanmış olan organizasyon ve bilgi varlıklarıdır.

3. SORUMLULUKLAR

3.1. Üst Yönetim

Bilgi Güvenliği Politikasının kurum ihtiyaçlarını karşılar nitelikte bulunmasından, uygulanması için gerekli destek ve gözetimin sağlanmasından, politikanın en az yılda bir kez veya kurum politikasında değişiklik gerektirebilecek durumlarda gözden geçirilmesinden sorumludur. Üst yönetimi temsilen bu görevi BGYS Temsilcisi yerine getirir ve yönetim kurulu üyesine onaylatır.

3.2. BGYS Yönetim Temsilcisi

Bilgi Güvenliği Yönetim sisteminin kurulmasından işletilmesi ve yönetilmesine dek her aşamada üst yönetime karşı sorumluluk üstlenen kişidir.

3.3. BGYS Çalışma Grubu

Üst yönetim tarafından görevlendirilen BGYS koordinasyon ekibi, Bilgi Güvenliği Politikasının kurum ihtiyaçlarını karşılar nitelikte bulunmasından, uygulanması için gerekli destek ve gözetimin sağlanmasından, politikanın en az yılda bir kez veya kurum politikasında değişiklik gerektirebilecek durumlarda gözden geçirilmesinden sorumludur.

3.4. Tüm Personel

Bilgi Güvenliği Politikalarını görev alanlarının gerektirdiği biçimde yerine getirilmesinden sorumludur.

4. TANIMLAR

- BGYS: Bilgi Güvenliği Yönetim Sistemi
- BGYT: Bilgi Güvenliği Yönetim Temsilcisi
- BGYS ÇG: BGYS Çalışma Grubu yönetimi temsil eden, BGYS'nin başarılı biçimde sürdürülebilmesi için sorumluluğu üstlenen ve gözetimini sağlayan organizasyondur.
- BGYS İç Denetçisi: BGYS'nin uygulanmasından ve işletiminden bağımsız, BGYS denetimini yerine getirebilecek deneyim, eğitim ve sertifikasyonlara sahip kişi olup BGYS'nin iç denetimini gerçekleştiren kişidir. İç denetçi kurum personeli olabileceği gibi kurum dışından da sağlanabilir.

5. Uygulama

5.1. Yönetim Desteği

- Üst yönetim, BGYS Çalışma Grubu'nun atanması ve bu grubun çatısı altında gerçekleştirdiği faaliyetler, BGYT ve BGYS İç Denetçi personel atamaları, BGYS yatırım, masraf ve eğitim bütçeleri, yönetim gözden geçirme aktiviteleri ile fiili olarak BGYS'yi destekler.

Hazırlayan	Kontrol Eden	Onay

 DİLER DEMİR ÇELİK ENDÜSTRİ VE TİCARET A.Ş.	BGYS POLİTİKASI		Doküman No	P.05.16.01				
			Revizyon No	0				
			Revizyon Tarihi					
			Yayın Tarihi	01/03/2016				
			Sayfa No	2/2				
<input type="checkbox"/> Çok Gizli	<input type="checkbox"/> Gizli	<input checked="" type="checkbox"/> x	<input type="checkbox"/> Hizmete Özel	<input type="checkbox"/> Kişisel Özel	<input type="checkbox"/> Herkese Açık	<input checked="" type="checkbox"/> x	<input type="checkbox"/> Dahili	<input type="checkbox"/> Harici

- Üst yönetim, BGYS politika ve prosedürlerine uyararak ve uyulmasını teşvik ederek BGYS hedeflerine ulaşmak için liderlik eder.
- Üst yönetim, bilgi güvenliği risklerinin yönetiminin kurumun itibarı ve faaliyetlerin sürekliliği açısından önemini yönetsel faaliyetleri uygulayarak ve kurumsal politikalar aracılığı ile ifade eder.
- Yılda en az bir kez riskleri değerlendirir ve Bilgi Güvenliği Politikasını gözden geçirerek sistemin sürekliliğini, sürdürülebilirliğini temin eder.
- Önemli teknolojik ve sistem değişiklikleri, majör güvenlik olay ve ihlalleri söz konusu olduğunda Bilgi Güvenliği Politikasını gözden geçirerek sistemin sürekliliğini ve sürdürülebilirliğini temin eder.

5.2. Bilgi Güvenliği Politikası

- Bilgi varlıklarını yönetmek, varlıkların güvenlik değerlerini, ihtiyaçlarını ve risklerini belirlemek, güvenlik risklerine yönelik kontrolleri geliştirmek ve uygulamak
- Bilgi varlıkları, değerleri, güvenlik ihtiyaçları, zafiyetleri, varlıklara yönelik tehditlerin, tehditlerin sıklıklarının saptanması için yöntemlerin belirleyeceği çerçeveyi tanımlamak.
- Tehditlerin varlıklar üzerindeki gizlilik, bütünlük, erişilebilirlik etkilerini değerlendirmeye yönelik bir çerçeveyi tanımlamak.
- Risklerin işlenmesi için çalışma esaslarını ortaya koymak.
- Hizmet verilen kapsam bağlamında teknolojik beklentileri gözden geçirerek riskleri sürekli takip etmek
- Tabi olduğu ulusal veya sektörel düzenlemelerden, yasal ve ilgili mevzuat gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülüklerini karşılamaktan, iç ve dış paydaşlara yönelik kurumsal sorumluluklarından kaynaklanan bilgi güvenliği gereksinimlerini sağlamak.
- Hizmet sürekliliğine yönelik bilgi güvenliği tehditlerinin etkisini azaltmak ve sürekliliğe katkıda bulunmak
- Gerçekleşebilecek bilgi güvenliği olaylarına hızla müdahale edebilecek ve olayın etkisini minimize edecek yetkinliğe sahip olmak
- Maliyet etkin bir kontrol altyapısı ile bilgi güvenliği seviyesini zaman içinde korumak ve iyileştirmek.
- Kurum itibarını geliştirmek, bilgi güvenliği temelli olumsuz etkilerden korumak.
- Diler Demir Çelik Yönetimi, bilgi güvenliği ile ilgili uygulamaların gerçekleşmesini, gözden geçirilmesini ve sürekli iyileştirilmesini taahhüt eder.

Hazırlayan	Kontrol Eden	Onay