



**RTSO BİLGİ
GÜVENLİĞİ
POLİTİKASI**

Doküman No	RTSO
Yayın Tarihi	01.07.2011
Revizyon Tarihi	01.01.2017
Revizyon No	01
Sayfa	1/1



**RTSO BİLGİ
GÜVENLİĞİ
POLİTİKASI**

HAZIRLAYAN/KALİTE YÖNETİM TEMSİLCİSİ

ONAYLAYAN/GENEL SEKRETER



RTSO BİLGİ GÜVENLİĞİ POLİTİKASI

Doküman No	RTSO
Yayın Tarihi	01.07.2011
Revizyon Tarihi	01.01.2017
Revizyon No	01
Sayfa	1/2

İÇİNDEKİLER

Konu Başlığı	Sayfa No.
KAPAK	1
İÇİNDEKİLER	2
ÖNSÖZ	3
MİSYON	4
VİZYON	4
KALİTE POLİTİKASI	5
BİLGİ SİSTEMLERİNİN GENEL KULLANIM POLİTİKASI	5
AĞ CİHAZLARI GÜVENLİK POLİTİKASI	6
VERİTABANI GÜVENLİK POLİTİKASI	7
İNTERNET ERİŞİM VE KULLANIM POLİTİKASI	8
AĞ YÖNETİMİ POLİTİKASI	10
ŞİFRE POLİTİKASI	11
E-POSTA POLİTİKASI	12
SUNUCU GÜVENLİK POLİTİKASI	13
ANTI-VİRÜS POLİTİKASI	14
GÜVENLİK AÇIKLARI TESPİT ETME POLİTİKASI	15
UZAKTAN ERİŞİM POLİTİKASI	16
RİSK DEĞERLENDİRME POLİTİKASI	17
KABLOSUZ İLETİŞİM POLİTİKASI	18
KRİZ/ACİL DURUM YÖNETİMİ POLİTİKASI	19
BİLGİ SİSTEMLERİ YEDEKLEME POLİTİKASI	20
PERSONEL GÜVENLİĞİ POLİTİKASI	21
BAKIM POLİTİKASI	22
YAZILIM GELİŞTİRME	23
BİLGİ GÜVENLİĞİ POLİTİKASI ONAYI	24

HAZIRLAYAN/KALİTE YÖNETİM TEMSİLCİSİ	ONAYLAYAN/GENEL SEKRETER



RTSO BİLGİ GÜVENLİĞİ POLİTİKASI

Doküman No	RTSO
Yayın Tarihi	01.07.2011
Revizyon Tarihi	01.01.2017
Revizyon No	01
Sayfa	1/3

ÖNSÖZ

Kurumsal bilgi güvenliğini tehdit eden saldırıların bilinmesi, bilgi güvenliğinin sağlanmasına yönelik kurumsal stratejilerin geliştirilmesinde önemli bir role sahiptir. Bilgi sistemlerine yönelik olarak yapılan saldırılar incelendiğinde; saldırıların çok geniş bir yelpazede yapıldığı, E-posta ve anlık mesajlaşma yoluyla gelen tehditlerin yanı sıra, web’de de ciddi bir tehdit unsuru haline gelmiştir. Günümüzde e-posta ve web tehditlerinin birleşmesiyle çok zararlı ve bulaşıcı virüsler doğmaktadır.

Elektronik ortamın doğasında var olan güvensizlik unsuru, elektronik ortamlardaki uygulamaları tehdit eden en büyük unsurdur. Geçmiş yıllarda saldırılar, yaygın ve hedef gözetmeksizin yapılmaktayken artık nokta hedefi gözeten ve bölgesel olarak düzenlenen saldırılar yapılmaktadır.

Son yıllarda bilgi ve bilgisayar güvenliğini zaafa uğratmaya hatta yıkmaya çalışan, kurumlar üzerinde maddi manevi büyük zararlara yol açan, kişi, kurum ve kuruluşları tehdit ederek zararlara uğramasına yol açan bilgi güvenliği tehditlerinin engellenmesi için kurumsal bilgi güvenliği sağlanmalıdır. Kurumsal Bilgi güvenliği standartlarının yüksek seviyede bir güvenlik sağlanmasında etkili olduğu muhakkaktır. Bunun ötesinde de sistemlerde açıklar olabileceği, özellikle web uygulamalarında daha dikkatli olunması gerektiği, yeni eğilim ve yaklaşımların keşfedildikçe kurumsal güvenliğinin artırılması yönünde hayata geçirilmesi gerektiği de asla unutulmamalıdır.

Elektronik ortamlar Dünyada ve Ülkemizde her geçen gün hızla yaygınlaşmakta, Ticari ve günlük yaşantımızdaki varlığı hissedilir oranda arttırmaktadır. Kurumsal bilgi güvenliğinin sağlanması amacıyla, saldırı türlerinin takip edilmesi, saldırganların kullandığı yöntemlerin saptanması, Ülkemizde ve Dünyada bu konuda yapılan araştırmalar, raporlar ve çalışmalar ile tespit edilen açıkların takip edilmesi ve giderilmesi bilgi güvenliği ihlalinin yaşanmaması için gerekli önlemlerin zamanında alınması, güvenlik ihlallerine anında müdahale edilerek saldırı zararlarından en az şekilde etkilenme, felaket anında uygulanabilecek felaket ve iş sürekliliği planlarının uygulanması gibi stratejiler, kurumlar tarafından bu tür oluşumların önüne geçmeleri için kendi bilgi güvenliği politikalarını oluşturmak, hayata geçirmek zorundadır.

Şaban Aziz KARAMEHMETOĞLU
RTSO Yön. Kur. Bşk.

HAZIRLAYAN/KALİTE YÖNETİM TEMSİLCİSİ	ONAYLAYAN/GENEL SEKRETER

