EGE BİLGİ olarak, bilgisayar, network ve server sistemlerinde önemli dökümanter dosya ve veri transferleri akışına sahip olup, bu transfer ve bilgilerin güvenliği, gizliliği ve kişisel hakların korunması büyük önem taşımaktadır.

Firmamızın Network'üne bağlı olan bir bilgisayar veya notebook daki güvenlik açığı, Ege Bilgi'nin tüm network ağına bağlı olan sistemlerin güvenliğini riske atmasına sebep olabilir. Bu nedenle Kurumsal Bilişim sistemlerinin güvenliğinde herhangi bir aksatmaya mahal verilmemesi için genel sistem seviyesinde alınmış olan güvenlik tedbirleri yanında, çalışan personelin de bu konulara hassasiyetle uyması gereken bir takım kurallar vardır. Bu kurallara tüm Ege Bilgi çalışanları uymak zorundadır.
Uyalması gereken kurallar aşağıda belirtilmiştir:

1. Eposta kullanma kuralları:

a) Ege Bilgi'nin e-posta sistemi, taciz, suistimal, kişisel amaç veya herhangi bir şekilde alıcı kişilerin haklarına zarar vermeye yönelik öğeleri ve içerikleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz.
b) Zincir mesajlar ve masajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başka kullanıcılara iletilmemelidir.
c) Çalışanların kişisel kullanımları için, internetteki sitelere üye olunması veya kayıt yaptırılması durumunda, Ege Bilgi'a ait e-posta adresi kullanılmamalıdır.
d) Spam, sahte e-posta, kurum faaliyetleri dışında gelen herhangi bir e-posta veya önemsiz e-postalar klasörüne düşen bir e-postaya kesinlikle yanıt yazılmamalıdır.
e) Kullanıcılar, e-posta için uygun olmayan içerikleri (pornografik, ırçılık, siyasi propaganda, fikri mülkiyet içeren malzeme, vb.) gönderemez.
f) Kullanıcılar, kullanıcı adresi ve şifresi isteyen e-postaları "firmanın haklanme riskini göze alarak" herhangi bir giriş-işlem yapmadan derhal silmelidir.
g) Kullanıcılar, e-postalarının yetkisi olmayan kişiler tarafından okunması veya kaydedilmesini engellemelidir. Şifre kullanmalı ve e-posta erişimii çin kullanılan donanım/yazılım sistemleri yetkisi olmayan kişilere karşı korunmalıdır.
h) Kullanıcılar, kullanıcı kodu veya şifresini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapmadan hemen silmelidir.
i) Ege Bilgi kullanıcıları, mesajlarını düzenli olarak kontrol etmeli ve mesajları cevaplandırmalıdır.
j) Kullanıcılar, kurumsal e-postaların firma dışındaki şahıslar ve yetkisi olmayan kişiler tarafından görülmesi veya okunmasını engellemekten sorumludurlar
k) Kaynağı bilinmeyen e-postalar ve eklerinde gelen dökümanlar kesinlikle açılmamalı ve hemen silinmelidir. Bu e-postaların viruslü, hack amaçlı veya sisteme zarar veribilecek amaçlı zararlı kodları içerebileceği unutulmamalıdır.
l) Ege Bilgi dışında, güvenliğinden şüphe edilen herhangi bir bilgisayarda e-posta sistemi kullanılmamalıdır.

HAZIRLAYAN KALİTE YÖNETİM TEMSİLCİSİ	**ONAY** GENEL MÜDÜR

m) Kullanıcıların gelebilecek e-postarı sık sık kontrol etmesi, gelen e-postaların ise uzun süre genel posta sunucusunda bırakmaması gerekir. Gelen e-postalar kişisel klasör'e taşınmalıdır.
1n) EGE BİLGİ çalışanlarınca, gönderdikleri, aldıkları veya sakladıkları e-postalarda kişisel menfaat-amaç aranmamalıdır. Yasadışı ve hakaret edici e-posta gönderimi veya alımı yapılması durumunda yetkili kişilerce, önceden haber verilmeksizin kullanıcının e-postaları denetlenebilir ve kullanıcının hakkında yasal ve idari işlemler başlatılabilir.
o) Kullanıcılar, kendilerine ait e-posta adreslerinin şifre güvenliğinden ve gönderdikleri e-postalardan doğacak hukuki işlemlerden sorumludurlar. Şifresinin başkalarınca deşifre edildiğini veya hacklendiğini farkettikleri andan itibaren yetkililerle paylaşmakla ve durumu haber vermekle yükümlüdürler.
p) Bir ay süre ile aktif olmayan e-postalar Ege Bilgi Bilgi İşlem birimi tarafından kaldırılacaktır. Firmadan ayrılan personel, kurumsal e-posta sistemini kullanamaz.

2. Şifre Kullanma Kuralları:

a) Ege Bilgi'deki, mevcut tüm kullanıcı şifreleri (e-posta, web, domain, vb.) en fazla altı ayda bir değiştirilmelidir.
b) Şifreler, e-postalara veya herhangi bir elektronik forma eklenmemeli, not edilmemelidir.
c) Şifreler başka kişilerle paylaşılmamalı, kağıt ya da elektronik ortamlarda saklanmamalı, not tutulmamalıdır.
d) Şifreleme esnasında, küçük ve büyük karakterlere (örnek, m-M, d-D) hem rakam hem noktalama hem de dijit karakterlere (örnek, 0-9, !*)/%$+-?'(/)<+§,.) sahip olmalıdır.
e) Şifreler, en az sekiz adet alfanümerik karaktere sahip olmalıdır.
f) Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmalıdır.
g) Aile, doğum tarihi, telefon numarası kullanılmamalıdır.
h) Herhangi bir kişiye telefonda şifre verilmemelidir.
i) e-posta yoluyla şifreler yazılmamalıdır.
j) Şifreler, aile bireyleriyle veya bir başka kişi ile paylaşılmamalıdır.
k) Şifreler, firmadan uzakta olduğunuz zamanlarda diğer iş arkadaşlarına verilmemelidir.
l) Bir kullanıcı adı ve şifresi birden çok bilgisayarda kullanılmamalıdır.
m) Şifre kırma ve tahmin etme işlemleri belli aralıklarla yapılmalıdır. Güvenlik kontrolleri sonucunda şifreler bulunur veya kırılırsa kullanıcıya ait yeni şifre verilir.

3. Anti-Virus Politikası

a) Ege Bilgi'ye ait tüm bilgisayar ve notebook'larda anti-virus yazılımı yüklü olmalıdır ve otomatik olarak güncellenmelidir.
b) Ege Bilgi'ye ait tüm network ve server ağı için virüs programı kullanılacaktır. Ve yıllık sürümleri update edilip güncellenmelidir.
c) Zararlı programları içeren (virusler, trojanlar ve hack saldırıları) programları ve dökümanları firma bünyesinde oluşturmak, çoğaltmak ve kopyalayarak dağıtmak yasaktır.
d) Kullanıcılar, herhangi bir sebepten dolayı anti-virus programını bilgisayarından veya bağlı olduğu sistemde kaldıramaz.

HAZIRLAYAN KALİTE YÖNETİM TEMSİLCİSİ	**ONAY** GENEL MÜDÜR

4. İnternet Kullanım Politikası

a) Ege Bilgi' deki hiç bir kullanıcı, karşılıklı paylaşıma-bağlantıya yönelik internet sitelerini kullanamayacaklardır. (Örnek, KaZaA, Napster, BearShare, LimeWire, OpenNap, WinMX vb.)
b) Kullanıcılar, karşılıklı ağ üzerinden "resmi görüşmeler haricinde" Messenger, Facebook, Twitter vb. mesajlaşma ve sohpet programları gibi chat programlarını kullanmayacaklardır. Ayrıca bu gibi programların üzerinden dosya alışverişinde bulunmayacaklardır.
c) Hiçbir kullanıcı, internet üzerinden görüntülü görüşme veya yapamayacaktır.
d) Çalışma saatleri içerisinde, aşırı bir şekilde iş ile ilgili olmayan internet sitelerinde gezinmek yasaktır.
e) İş ile ilgili olmayan (müzik, video dosyaları) yüksek hacimli dosyalar göndermek veya bilgisayara indirip kaydetmek yasaktır.
f) İnternet üzerinden Ege Bilgi tarafından onaylanmamış yazılımlar indirilemez ve bulunduğu network sistemine bu yazılımlar kurulamaz.
g) İnternet üzerinden gelen ahlak anlayışına aykırı sitelere girilmesi ve dosya indirimi yasaktır.
h) Network ve Server sistemleri için büyük tehlike oluşturduğu için, internet üzerinden ekran koruyucu, masaüstü resimleri veya yardımcı program niteliğindeki hertürlü dosya ve programın indirilmesi veya kopyalanması yasaktır.
i) Üçüncü şahısların firma içerisinden interneti kullanmaları Yönetim temsilcisi izni ve bu konudaki kurallar dahilinde gerçekleştirilbilecektir.
j) Ege Bilgi, iş kaybının önlenmesi ve çalışanların internet kullanımı hakkında gözlemleme ve istatistik yapabilir.

5. Genel Kullanım Politikası

a) Ege Bilgi networkune bağlı tüm PC ve notebook'lar, 10 dakikalık kullanım dışı zamanlarda otomatik olarak şifreli ekran korumasına geçebilmelidir.
b) Notebook ve PC'ler güvenlik açıklarına karşı daha dikkatle korunmalıdır. İşletim sistemi şifreleri aktif hale getirilmeli, anti-virus programları güncelliğini korumalıdır.
c) Ege Bilgi'de bulunan domain sistemi yapısı login halde tutulmalıdır. PC-notebook sistemleri ayrı switchlerde barındırılmalı, ortak paylaşım klasörü haricinde birbirleri ile bilgi alışverişi yapılmamalıdır.
d) Notebook'ların çalınması veya kaybolması halinde, durum farkedildiğinde en kısa sürede Bilgi İşlem sorumlusuna bilgi verilmelidir.
e) Kullanıcılara ait cep telefonları ve PDA (Personal Digital Assistant)'ları firmanın network ağı ile senkronize olsun veya olması şifreleri aktif halde olmalıdır. Kullanım dışı durumlarda kablosuz erişim (kızılötesi, bluetooth vb.) özellikleri aktif halde olmamalıdır ve mümkünse anti-virus programları ile yeni nesil viruslere karşı korunmalıdır.
f) Tüm kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek firmaya veya kişiye yönelik saldırılardan (örnek, elektronik bankacılık vs.) bilgisayar kullanıcısı sorumludur.
g) Kullanıcı, firmanın bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışmamalıdır.

HAZIRLAYAN KALİTE YÖNETİM TEMSİLCİSİ	**ONAY** GENEL MÜDÜR

h) Network ağı güvenliği tehlikeye sokacak veya haberleşme ağını bozacak eylemlere girişmemelidir (örnek, sunuculara erişerek ip adresi veya dns numaralarının değiştirilmesi).
i) Port veya network ağ taraması, ayrıca pink atılarak server IP taraması yapılmamalıdır.
j) Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DoS saldırısı, DNS ve IP ayar değişiklikleri vb.
k) Firmaya ait bilgileri (DNS, IP, wireless şifreleri vb.) firma dışında üçüncü şahıslara iletilmemelidir.
l) Kullanıcıların kişisel bilgisayarları üzerinde, Bilgi İşlem sorumlusunun onayı alınmaksızın herhangi bir çevre birimi bağlantısı veya program yüklenmesi yasaktır.
m) PC, notebook, yazılım veya veriler izinsiz olarak kurum dışına çıkarılması yasaktır.
n) Ege Bilgi'nin kullanmakta olduğu yazılım harici kaynağı belirsiz programları kurmak ve kullanmak yasaktır.
o) Yetkisi olmayan personelin, firmaya ait gizli ve hassas bilgileri görmesi veya elde etmesi-çalışması kesinlikle yasaktır.
p) Firmaya veya kişisel bilgilerin gizliliğine ve mahremiyetine özel önem göstermekte tüm çalışanlar sorumludur. Bu tür gizli dosyalar üçüncü kişilere elektronik veya kağıt ortamında verilemez.
q) Personel, kullandıkları masaüstü veya dizüstü bilgisayarlarındaki kurumsal bilgilerin düzenli olarak server tarafından yedeklenip yedeklenmediğini takip etmekten sorumludur.
r) Bilgi İşlem sorumlusu veya atadığı yetkili kişiler tarafından, kullanıcılara haber verilmeksizin yerinde veya uzaktan erişimle çalışan bilgisayarına erişip güvenlik, bakım ve onarım işlemleri yapabilir. Bu gibi durumlarda uzaktan bakım ve destek hizmeti veren yetkili personel, kişisel veya kurumsal bilgileri görüntüleyemez, kopyalayamaz ve değişiklik yapamaz.
s) Kullanıcılar bilgisayarlarına oyun ve eğlence amaçlı programları çalıştırmamalı / kopyalamamalıdır.
u) Bilgi İşlemin bilgisi olmadan firma network sistemine başka bilgisayarlar bağlanamaz, sunucu nitelikli bilgisayar bulundurulamaz.
v) Ege Bilgi network ağında hiç bir şekilde ağ ayarları, kullanıcı tanımları, kaynak profilleri vb. düzenlemeler değiştirilmemelidir.
w) Bilgisayarlara herhangi bilgi işlem müdürünün onayı olmayan yazılımlar yüklenmemelidir.
x) Gerekmedikçe bilgisayar kaynaklarını paylaşıma açılmamalıdır, kaynakların paylaşıma açılması bilgi işlem sorumlusunun bilgisi dahilinde olmalı ve mutlaka şifre kullanma kurallarına göre yapılmalıdır.

HAZIRLAYAN KALİTE YÖNETİM TEMSİLCİSİ	**ONAY** GENEL MÜDÜR