1. AMAÇ

Bilgi Güvenliği Politikası'nın amacı, **SP ENERJİ**' nin (Kuruluş) kurumsal bilgi güvenliği ilkelerini ana hatlarıyla belirlemek ve kuruluşta bilginin işlenme yöntemlerinin güvenli olarak gerçekleştirilmesini sağlayacak düzenlemeleri ortaya koymaktır. Bilgi Güvenliği Politikası bilgi güvenliği yönetimi için hazırlanan tüm dokümanların üstünde yer alan kapsayıcı bir dokümandır.

Bilgi Güvenliği Politikası, aşağıdaki alanlarda Kuruluş genelinde sürekli ve en iyi seviyede bulunmak amacıyla oluşturulmuştur:

a) Bilginin güvenli bir ortamında kullanılmasını sağlamak
b) Programları, verileri, iletişim ağını ve ekipmanları (donanım) kayıplara, yanlış kullanıma ve suistimallere karşı koruma altına almak
c) Tüm kullanıcıların Politika beyannamesine, ilgili destekleyici politikalara ve prosedürlere bütünüyle uymalarını ve farkında olmalarını sağlamak
d) Tüm kullanıcıların kendi sorumluluklarını, yönetimlerinde olan ve/veya erişebildikleri verinin bütünlüğü ve gizliliğinin önemini anlamalarını sağlamak
e) Tüm kullanıcıların görevler ayrılığı matrisine uygun olarak sorumlulukları dahilinde çalışmalarının önemini anlamalarını sağlamak
f) Kuruluş'un genel ihtiyacı çerçevesinde bilgi güvenliğine genel bir bakış açısı ve standartlar bütünü tanımlamak
g) Kuruluş'un bilgi güvenliğine olan bakışını vurgulamak ve detaylandırmak
h) Üst Yönetim'in Kuruluş'un bilgi güvenliğine verdiği önemi ve desteği ifade etmek
i) Bilgi güvenliğine yönelik sorumlulukların oluşturulmasını sağlamak
j) Kuruluş bilgi güvenliğini tehdit edebilecek olayların oluşmasını engellemek, yönetim ve çalışanların bu amaçla yeterli seviyede bilgilendirilmesini sağlamak

2. TANIMLAR VE KISALTMALAR

Kuruluş: SP ENERJİ ELEKTRİK ÜRETİM LTD. ŞTİ.

Yönetim: SP ENERJİ Yönetimi

Üst Yönetim: SP ENERJİ Genel Müdürü

İş Bölümleri: Bilgi Sistemleri Birimi dışında kalan tüm grup ve bölümleri ifade etmektedir.

Politika: Bilgi Güvenliği Politikası

Kriptografi: Kriptografi, açık ve anlamlı bilgilerin matematiksel algoritmalar ile korunmasıdır.

SSL (Secure Socket Layer): İnternet üzerinde bilginin gizliliğini ve bütünlüğünü korumak için oluşturulmuş bir protokol katmanıdır. Bu protokol bütün yaygın web sunucuları ve tarayıcıları tarafından desteklenmektedir. Bu protokolle çalışan web siteleri 'http' yerine 'https' ile başlar. SSL, gönderilen bilginin sadece doğru adreste deşifre edilmesini sağlar; bilgi gönderilmeden önce şifrelenir ve sadece doğru alıcı tarafından deşifre edilir. Bilginin bütünlüğü de bu süreçte kontrol edilir.

DMZ (Demilitarized Zone): Kuruluşun dış servislerini içeren, bir iç ağ ile güvenli olmayan (örn. İnternet) bir dış ağ arasında yer alan bilgisayar ya da alt ağdır. Kurumlarda genel olarak merkezi güvenlik duvarının dışında olan ve İnternete açık olan alanları ifade eder.

Şifreleme (Encryption): Bilgisayar güvenliğinde verilerin anlaşılmaz kılınacak bir şekilde dönüştürüldüğü ve ancak şifre çözme algoritmasıyla geri kazanılabildiği yöntemdir.

Sızma testi: Sistemin güvenlik açıklarını istismar edilmeden önce tespit etmek ve düzeltmek amaçlı gerçekleştirilen ataklardır.

SSH: Verilerin güvenli bir kanal üzerinden aktarıldığı bir ağ protokolüdür.

İz Kaydı (Log): Bir veri kaynağı hakkında zaman içindeki durumlarının ya da değişikliklerinin kayıt altına alınması sırasında oluşan sistemsel kayıtlardır.

3. KAPSAM ve SORUMLULUKLAR

3.1.Kapsam

Bilgi Güvenliği Politikası, Kuruluş'un manuel ya da elektronik tüm sistemlerini kapsar. Ayrıca,

a) Tüm Kuruluş çalışanlarını,

b) Hizmet sağlayıcıları ve tedarikçileri,

c) Kuruluş ile çalışan tüm üçüncü şahısları,

Kapsamakta olup, aşağıdaki alanları içerecek şekilde oluşturulmuştur:

1. Kuruluş'a ait tüm bilgi sistemleri varlıkları ve bileşenleri: Bu bileşenler aşağıdakilerle sınırlı olmaksızın ve saklandığı formata bakılmaksınız bütün bilgi ve verileri ihtiva eder:

    - Bilgisayar dosyaları ve veritabanları,
    - Veri saklama ortamları (CD, DVD, USB Disk, vb.),
    - Bilgisayar sistemlerinde üretilen tüm raporlar,

- Bilgisayar uygulama ve yazılımları ile bunlara ait dokümanlar,
- Tüm e-posta mesajları,
- Veri iletim araçları.

2. Kuruluş'a ait iletişim ağları,
3. Personel, çevresel ve fiziksel alanlar,
4. Tüm kurumsal süreçler/işleyiş ve yöntemler (iletişim ve işletim süreçleri, risk yönetim süreçleri, İş/BS devamlılık süreçleri vb.),
5. Dış kurum ve şahıslarla ilişkiler ve sözleşmeler,
6. Kanun ve yönetmeliklere uyum

3.2. Roller Ve Sorumluluklar

3.2.1. Yönetim Kurulu

Yönetim Kurulu, Bilgi Güvenliği Politikasının onaylanması ve Kuruluş dâhilindeki tüm bölüm, birim yöneticileri ile tüm Kuruluş çalışanlarına dağıtımından; kendisine düzenli sunulan bilgi güvenliği raporlarını değerlendirmekten sorumludur.

3.2.2. Üst Yönetim

Kuruluş üst yönetimi, bilgi sistemlerinin ve verilerin gizlilik, bütünlük ve erişilebilirliğini sağlayacak önlemlere ilişkin kontrol altyapısının geliştirilmesi ve düzenli olarak güncellenmesi çalışmalarını gözetim altında tutar ve bu amaçla bilgi güvenliği politikasını oluşturur ve onaylar. Üst yönetim, aşağıdaki faaliyetlerin yerine getirilmesini temin edecek mekanizmaları kurar:

a) Bilgi güvenliği politikasının ve tüm sorumlulukların yılda en az bir defa gözden geçirilmesini, güncellenmesini ve Yönetim Kurulu'na sunulacak şekilde onaylanmasını,

b) Bilgi sistemleri ve bilgi sistemleri üzerinde işlenen, saklanan ve iletilen verilerin güvenlik hassasiyet derecelerine göre sınıflandırılmasını ve her bir sınıf için uygun düzeyde güvenlik kontrollerinin tesis edilmesini,

c) Güvenlik alanındaki güncel gelişmeler, yeni tehditler ve zafiyetlerin takip edilmesini, gerekli yazılım güncellemelerinin ve yamaların uygulanmasını, Bilgi güvenliği hususunda farkındalığı artıracak çalışmaların desteklenmesi,

d) Bilgi güvenliği ihlaline ilişkin olayların izlenmesini ve periyodik olarak değerlendirilmesini,

e) Kuruluşun bilgi sistemleri aracılığıyla sunduğu hizmetlerin tasarımı, geliştirilmesi, uygulanması veya yürütülmesinde görevi bulunmayan bağımsız ekiplere yılda en az bir defa sızma testi yaptırılmasını,

f) Bilgi güvenliği hususunda hem kurum içinde hem de iş ortakları nezdinde farkındalığı artıracak çalışmaların gerçekleştirilmesini,

g) Bilgi güvenliği stratejilerine yön verme; bilgi güvenliğine yönelik politika, prosedür, standart ve talimatları önerme ve gözden geçirme

h) Kendisine düzenli sunulan bilgi güvenliği raporlarını değerlendirme;

i) Bilgi güvenliği bilincinin oluşturulması için hazırlanan güvenlik farkındalık eğitimlerinin içeriğini değerlendirme

j) Bilgi güvenliğine yönelik tüm yasal yükümlülüklerin teknik detaylarının hayata geçirilmesi için yönlendirilme;

k) Güvenlik denetimleri sonucu ortaya çıkan bulgu ve açıklıkların takibini koordine etme.

3.2.3. Bilgi Güvenliği Yönetim Temsilcisi

Bilgi güvenliği yönetim temsilcisi, Politika çerçevesinde ele alınan konuların ve stratejilerin hayata geçirilmesi ve uygulamasından; iş yapış şekillerini Yönetim Kurulu aldığı kararlar ve stratejiler doğrultusunda kuruluşta oluşturulan politika, prosedür, teknik prosedür ve standartlara adapte etmek ve uygulamaktan sorumludur.

Bilgi güvenliği yönetim temsilcisi, bilgi güvenliğine yönelik olarak Yönetim Kurulu'nun aldığı kararları takip etmek; ilgili tüm personele tavsiyelerde bulunmak; Bilgi Güvenliği Politikasının ve destekleyici alt politika ve prosedürlerin uygulanıp uygulanmadığını belirli aralıklarla kontrol etmek; güvenlik olayları ile ilgili olarak soruşturma ve araştırma yapmak; hazırlanan güvenlik farkındalık eğitimlerinin içeriğini ve formatı oluşturmak ve güncellemek ve Kuruluş içindeki güvenlik kontrollerinin durumunu Üst Yönetime ve/veya Yönetim Kurulu'na düzenli olarak raporlamaktan sorumludur.

3.2.4. Personel/Çalışan/Kullanıcı

Tüm **SP ENERJİ** personeli, gerek bu Politikada gerekse destekleyici diğer politika ve prosedürlerde belirtilen bilgi güvenliğine yönelik **SP ENERJİ** yaklaşımına uygun bir şekilde hareket etmek ve çalışmalarında bunları uygulamaktan sorumludur.

4. POLİTİKA

4.1. Süreçler Hakkında Genel Bilgi

4.1.1. Bilgi varlıklarının sınıflandırılması

Güvenlik önlemlerinin tesis edilmesinde, bir güvenlik katmanının aşılması halinde diğer güvenlik katmanının devreye girdiği katmanlı güvenlik mimarisi bulunmaktadır.

Bilgi varlıklarına gerektiği seviyede ve yeterli miktarda güvenlik önlemlerinin tanımlanması ve oluşturulması için bu varlıkların güvenlik seviyelerine göre sınıflandırılması gerekmektedir. Bilgi varlıkları aşağıdaki detayda sınıflandırılır:

a) Genele Açık: Kuruluş dışında serbestçe dağıtılabilen ve bu nedenle özel bir koruma gerektirmeyen tüm varlıkları ifade eder.

b) Hizmete Özel: Kuruluş personelinin günlük operasyonel işlerini yerine getirmek amacıyla kullandığı ve ihtiyaç duyduğu ve bu nedenle de Kuruluş içerisinde dağıtımı mümkün olan bilgilerdir. Ancak bu varlıkların üçüncü kişilerin eline geçmesi, bu şahıslara ticari avantaj sağlayabileceği gibi ticari ilişkileri de zedeleyebilir.

c) Özel: Bu sınıfa giren bilgi varlıkları sadece ilgili ve açıkça tanımlanmış kişilere iletilir. Bu bilgilerin açıklanması Kuruluş işletimine veya önemli bir proje veya görevin tamamlanmasına zarar verebilir.

d) Gizli: Yetkisiz kişilere açıklanması Kuruluş çıkarlarına aykırı olan ve önemli zararlar doğurabilecek bilgiler bu sınıfa girer.

4.1.2. Sistemlere/Uygulamalara erişim ve yetkilendirme

Kuruluş'un bilgi sistemlerine erişimde kullanılan kullanıcı hesaplarının yaratılması, izlenmesi ve silinmesi standartlarını tanımlamak, kullanıcıların erişmeye yetkili olacağı uygulamaları ve sistemleri belirleyerek, diğer sistem ve uygulamaları yetkisiz erişimlere karşı korunmak amacıyla ayrı bir **KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI** oluşturulmuştur**.**

4.1.3. Şifre yönetimi

Kuruluş'un bilgi sistemleri ortamlarına erişirken kullanılan şifrelerin standartlara uygun biçimde oluşturulması, korunması, kullanılması ve değiştirilmesi, kullanıcılara tanımlanan şifreler konusunda çalışanların bilgilendirilmesi ve şifre işlemlerinin Kuruluş'un riskini en aza indirecek en güvenli şekilde yapılmasını sağlamak için ayrı bir **PAROLA GÜVENLİĞİ POLİTİKASI** oluşturulmuştur.

4.1.4. Dizüstü ve kişisel bilgisayar kullanımı

Kuruluş'un personeline sunduğu bilgisayarlar, sadece işe uygun amaçlarla kullanılabilmektedir. Bu bilgisayarların, Kuruluş yönetiminden izin alınmaksızın; iş amacı dışında ya da yetki sınırları haricinde kullanımı, uygun olmayan kullanım olarak değerlendirilir.

4.1.5. E-posta güvenliği

E-posta, Kuruluş'un en önemli iletişim kanallarından biridir ve bu kanalın kullanılması kaçınılmazdır. Bunun yanı sıra e-posta, basitliği ve hızı nedeni ile yanlış veya gereğinden fazla kullanıma açık bir kanaldır. E-posta adresi oluşturma ve tanımlama ile bu e-posta hesaplarının kullanımına yönelik kurallar ile e-posta virüs güvenliğine yönelik kullanıcıların bilmesi gerekenler belirlenmiştir.

4.1.6. İnternet kullanımı

İnternet'in uygun olmayan kullanımı, Kuruluş'un yasal yükümlülükleri, kapasite kullanımı ve profesyonel imajı açısından istenmeyen sonuçlara neden olabilir. Bilerek ya da bilmeden, bu türden olumsuzluklara neden olunmaması amacı ile İnternet'in kurallara, etik ve yasalara uygun kullanımının sağlanması gereklidir.

4.1.8. Ağ güvenliği

Kuruluş'da ağ seviyesi bilgi güvenliği stratejilerini gizlilik, bütünlük ve erişilebilirlik prensiplerini göz önünde bulundurarak ortaya koyan bir süreç **(AĞ CİHAZLARI YÖNETİM VE GÜVENLİK POLİTİKASI)** oluşturulmuştur.

4.1.7. Güvenlik olaylarının bildirimi

Kuruluş'un bilgisayar ağında oluşabilecek güvenlik ihlalleri karşısında nasıl davranılması, güvenlik vakalarının sebeplerini analiz edebilmek için gerekli ve yeterli sayıda verinin toplanması, sistemin en kısa sürede en az zarar ile tekrar çalışır duruma getirilmesi, uygunsuzlukların nasıl raporlanması ve Bilgi Güvenliği Yöneticisine ulaştığı bulgulara karşı nasıl hareket edilmesi gerektiği konusundaki kuralları belirlemek amacıyla süreç **(BİLGİ GÜVENLİĞİ OLAY YÖNETİMİ POLİTİKASI)** oluşturulmuştur**.** Bu çerçevede vakaların tanımlanması ve kategorize edilmesi, vakaların bildirilmesi, değerlendirilmesi ve vaka yönetim sürecinin yönetilmesine yönelik konular ele alınmıştır. İlgili sürece göre tüm Kuruluş çalışanları veya üçüncü taraf kullanıcıları, bir güvenlik açığıyla karşılaştıklarında olası güvenlik olaylarını engellemek amacıyla, durumu mümkün olduğu kadar kısa sürede rapor etmelidir. Tüm personel, kullandığı sistemlerin ve uygulamaların durum bilgilerine sahip olmalı ve tüm yetkisiz kullanım ve şüpheli durumları rapor etmek için hazır olmalıdır.

4.1.9. Zararlı yazılımlara karşı koruma

Kuruluşa ait sistemlerin ve kullanıcı bilgisayarlarının zararlı yazılımlardan ve etkilerinden korunması ve sistem güvenliğinin sağlanması, Kuruluş'a ait yazılımların ve içerdiği bilgilerin bütünlüğünün korunması ve zararlı yazılımlardan doğan güvenlik tehditlerinin zamanında tespit edilmesi amacıyla süreç **(ANTİVİRÜS VE ZARARLI YAZILIMLARA KARŞI KORUMA POLİTİKASI)** oluşturulmuştur. Bu süreç çerçevesinde Kuruluş anti-virüs ve anti-spam yazılımlarının kullanılması ve yönetilmesi ile bu alanlarda kullanıcıların bilgilendirilmesine yönelik konular ele alınmıştır.

4.1.10. Fiziksel ve çevresel güvenlik

Kuruluş'un bilgisayar sistemlerinin ve bunların bulunduğu mekânların zarar görmesi ve bu alanların fiziksel ve çevresel tehditlere yönelik olarak yeterli seviyede korunmaması Kuruluş'un verilerinin sağlaması gereken gizlilik, bütünlük ve erişilebilirlik kriterlerini yerine getirilememesine sebep olabilir. Bu nedenle kritik Bilgi Sistemleri varlıklarının korunması bilgi güvenliği yönetiminin önemli bir parçasıdır. Başta kritik sistemler ve donanımlar olmak üzere Kuruluş bilgi sistemlerinin fiziksel ve çevresel güvenliğinin korunması ve arttırılması amacıyla süreç **(FİZİKSEL VE ÇEVRESEL GÜVENLİK POLİTİKASI)** oluşturulmuştur.

Temiz Masa İlkesi: Fiziksel güvenliğin önemli parçası, veri ve dokümanları yetkisiz kişilerin erişiminden korumaktır. Bu amaçla Kuruluş' da tüm personelin uyması gereken "Temiz Masa İlkesi" benimsenmiştir. Bu ilke çerçevesinde tüm Kuruluş personeli, herkese açık çalışma alanlarında ve masalarında Kuruluş'a ve müşterilerine ait bilgi, belge, doküman ve bunları içeren her türlü elektronik/manyetik verileri bulundurmamalıdır. Varlık sınıflandırması gizli veya özel olan verilerin saklanması için özel koruma imkânları (kilitli dolap, kasa vb.) tercih edilmeli; bu sınıflandırmaya giren tüm verileri ve dokümanları başka

bir çalışanın masasına ya da çalışma alanına bırakırken yetkisiz erişimlere açık olup olmadığı kontrol edilmelidir.

4.1.11. Sistem/Uygulama denetim ve iz kayıtlarının yönetimi

Kuruluş'un tüm kritik sistem ve uygulamalarının iz kayıtları saklanmakta, izlenmekte ve analiz edilmektedir. Bu analizler neticesinde yatırım ya da çalışma planları oluşturulabildiği gibi bu sistemleri ve uygulamaları kullanan kullanıcılar hakkında da bilgi toplanabilmektedir. İz kayıtlarının düzenli kontrolü ve takibi için süreç **(İZ KAYDI YÖNETİM POLİTİKASI)** oluşturulmuştur.

4.2. Güvenlik Farkındalık Eğitimleri

Kuruluş çalışanlarının bilgi güvenliğine yönelik farkındalıklarını arttırabilmek bu politikanın temel amaçlarından biridir. Bu nedenle İnsan Kaynakları eğitim programlarına entegre bir şekilde, Kuruluş çalışanlarına yönelik işe girişte ve çeşitli dönemlerde bilgi güvenliği farkındalığı arttırma ve bilinçlendirme eğitimleri düzenlenir. Bu eğitimler çerçevesinde Kuruluş bilgi güvenliği çerçevesinin ve standartlarının çalışanlara aktarılması, güvenlik politika ve standartlarının farkında olunması ve politikalardaki rol ve tanımların bilinmesini ve sahiplenilmesini amaçlar. Bilgi güvenliği bilincinin oluşturulması için hazırlanan güvenlik farkındalık eğitimlerinin içeriğinin değerlendirilmesi Üst Yönetim tarafından gerçekleştirilir.

4.3. Politika'nın Gözden Geçirilmesi ve Güncellenmesi

Bilgi Güvenliği Politikası en az yılda 1 (bir) kere gözden geçirilir ve Yönetim Kurulu onayı ile yeniden yayınlanır. İş bölümleri; Bilgi Güvenliği Politikası ve bu politikada belirtilen standartların uygulanması konusunda, değişiklik, ek ya da çıkartma taleplerini detaylı gerekçeleri ile Bilgi Güvenliği personeline bildirebilirler.

Bilgi Güvenliği Politikası'nın güncellenmesi için yeter şartlar aşağıda sıralanmıştır:

a) Sistem bileşenlerinde büyük değişiklik olması,

b) Yeni tipte güvenlik ihlallerinin çıkması,

c) Mevzuatta, kurumsal süreçlerde ya da işletim talimatlarda değişiklik yapılması,

d) Güvenlik gereksinimlerinde değişiklik olması,

e) Güvenlik ihlalleri,

f) Bilgi Sistemleri Birimi ve Üst Yönetim'in ihtiyaç duyduğu diğer tüm haller

Bilgi Güvenliği Politikası gözden geçirilirken aşağıda listelenen hususlar özellikle göz önünde bulundurulur:

a) Mevcut politikanın etkinliği ve yeterliliği,

b) Tercih edilen güvenlik önlemlerinin ve korunan varlıkların değerleri,

c) Teknolojideki değişiklikler

4.4. Güvenlik Denetimi ve Uyum

Kuruluş, gerek bağlı bulunduğu sektörel düzenlemeler sebebiyle gerekse bilgi güvenliğine yönelik kontrollerin arttırılması amacıyla denetim faaliyetleri gerçekleştirir. Bu amaçla hem Kuruluş içindeki denetimden sorumlu yetkili birimlerce hem de bağımsız denetçilerce düzenli olarak denetimler yapılır. Ayrıca dışarıya açık ve kritik sistemler için yılda en az 1 (bir) kere olmak üzere bağımsız firmalara sızma testi ve teknik güvenlik denetimleri yaptırılır. Bu denetim ve çalışmalar sonucunda bilgi güvenliğine yönelik ortaya çıkan bulgu ve konuların takibini Üst Yönetim koordinasyonunda Bilgi Sistemi Personelleri yapar; önerilen çözüm ve yöntemlerin hayata geçirilmesinden Bilgi Güvenliği personeli sorumludur.

4.6. Personeli İlgilendiren Konular

Kuruluş'da yeni işe başlayan tüm personelin bu Politika dokümanını okuması sağlanır. Bu amaçla bu Politika İnsan Kaynakları oryantasyon eğitiminin bir parçası olabileceği gibi Kuruluş'un tüm personeline açık olarak yayınlanır. Ayrıca tüm **SP ENERJİ** çalışanları Bilgi Güvenliği Politikası'nı okuduğunu ve kabul ettiğine dair taahhütname imzalar ve bu taahhütnameler İnsan Kaynakları tarafından saklanır.

Bilgi Güvenliği Politikası güncellemeleri yayınlanır ve tüm **SP ENERJİ** çalışanlarının e-posta ile bilgilendirilmesi sağlanır.

Aşağıdaki durumlardan en az birinin gerçekleşmesi durumunda Bilgi Güvenliği Politikası'nın ihlal edildiği sonucuna varılır:

a) Kasten ya da ihmal sonucu Bilgi Güvenliği Politikası'nda ve/veya ilgili alt politikalar, prosedürler, teknik prosedürler ve standartlarda açıkça belirtilmiş maddelere karşı hareket etmek,

b) Kuruluş' un itibarını riske atmak,

c) Kuruluş bilgilerini ve bilgi güvenlik sistemini tehlikeye atarak Kuruluş'u fiili ve olası iş kaybına maruz bırakmak,

d) Kuruluş bilgilerini yetkisiz bir şekilde kullanmak, ifşa etmek, değiştirmek, tahrip etmek ve/veya bu bilgileri izinsiz bir şekilde üçüncü kişilerle yazılı/elektronik olarak herhangi ortamda paylaşmak,

e) Kuruluş bilgi varlıklarını yasal olmayan bir amaç için kasten ya da ihmale sonucu kullanmak

Bilgi Güvenliği Politikası'nın ihlali durumunda bu ihlalin ciddiyetine göre hareket etme hakkını saklı tutar; ancak Politika'ya uymama veya kasıtlı Politika ihlalleri, disiplin cezası, yazılı kınama, işten çıkarma, hukuk muameleleri ve/veya cezai kovuşturmalar dâhil olmak üzere bunlarla sınırlı olmayan eylemlerle sonuçlanabilir. Kuruluş, ihlalin ciddiyetine göre, çalışanın sistemlere erişim haklarını ve ilgili sorumluluklarını askıya alabilir.