ÖZET

Bilgi Güvenliği Yönetim Sistemi Politikalarının amacı Bursa Temiz Enerji Elektrik Üretim San. ve Tic.A.Ş. . personelinin, sistemlerinin, bilgi ve varlıklarının; gizlilik, bütünlük ve erişilebilirlik bakımından yapılması, uyulması gereken iş kurallarını hedeflemek ve bu hedefler kapsamında iş sürekliliğini sağlamaktır.

Kurumun amacı herhangi kimse üzerinde kısıtlayıcı politikalar üretmek değil aksine açıklık, güven ve bütünlüğe yönelik kültürü yerleştirmektir. Kurum bilerek veya bilmeyerek yapılan yasadışı veya zararlı eylemlerine karşı personelin ve kurumun haklarını korumaya adamıştır. Bilişim ile alakalı sistemler kurumun sahip olduğu değerlerdir. Güçlü bir güvenlik bütün personelin içerisine dâhil olduğu takım çalışmasıyla oluşturulabilir. Bütün bilgisayar kullanıcıları günlük aktivitelerini yerine getirebilmesi için bu kuralları iyi bilmeli ve uygulamanın sorumluluğunu taşımalıdır.

BGYS politikalarının, gözden geçirilmesi ve güncellenmesinden BGYS Yönetim Temsilcisi ve BGYS Ekibi sorumludur. Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş. yönetimi Bilgi Güvenliği Politikasını onaylar ve duyurulmasını sağlar. Bu politikalara uyulmasından iç ve dış tüm ilgililer sorumludur.

Yaptırım

Bu politikalara uygun olarak hareket etmeyen tüm personel hakkında Disiplin Prosedürü uygulanır.

POLİTİKA LİSTESİ

- ✓ P.01 BİLGİ GÜVENLİĞİ GENEL POLİTİKASI
- ✓ P.02 İNTERNET ERİŞİM POLİTİKASI
- ✓ P.03 E-POSTA POLİTİKASI
- ✓ P.04 ANTİ-VİRÜS POLİTİKASI
- ✓ P.05 PAROLA POLİTİKASI
- ✓ P.06 FİZİKSEL GÜVENLİK POLİTİKASI
- ✓ P.07 SUNUCU GÜVENLİK POLİTİKASI
- ✓ P.08 AĞ YÖNETİMİ POLİTİKASI
- ✓ P.09 UZAK BAĞLANTI VPN POLİTİKASI
- ✓ P.10 TEDARİKÇİ VE ÜÇÜNCÜ TARAF GÜVENLİK POLİTİKASI
- ✓ P.11 KABUL EDİLEBİLİR KULLANIM POLİTİKASI
- ✓ P.12 TEMİZ MASA TEMİZ EKRAN POLİTİKASI
- ✓ P.13 MOBİL VE TAŞINABİLİR CİHAZ POLİTİKASI
- ✓ P.14 VERİTABANI GÜVENLİK POLİTİKASI
- ✓ P.15 DEĞİŞİM YÖNETİMİ POLİTİKASI
- ✓ P.16 KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI
- ✓ P.17 KRİPTOGRAFİK KONTROLLER POLİTİKASI
- ✓ P.18 ZİYARETÇİ KABUL POLİTİKASI
- ✓ P.19 OLAY İHLAL BİLDİRİM VE YÖNETİM POLİTİKASI
- ✓ P.20 GÜVENLİ YAZILIM GELİŞTİRME POLİTİKASI
- ✓ P.21 ERİŞİM KONTROL POLİTİKASI

P.01 BİLGİ GÜVENLİĞİ GENEL POLİTİKASI

Bursa Temiz Enerji Elektrik Üretim San. ve Tic.A.Ş., ISO 27001:2013 Bilgi Güvenliği Yönetim Sistem Standardı doğrultusunda;

a) Kendisi ve paydaşlarının bilgi varlıklarına güvenli bir şekilde erişim sağlamayı,

b) Bilginin kullanılabilirliğini, bütünlüğünü ve gizliliğini korumayı,

c) Kendisinin ve paydaşlarının bilgi varlıkları üzerinde oluşabilecek riskleri değerlendirmeyi ve yönetmeyi,

d) Kurumun güvenilirliğini ve marka imajını korumayı,

e) Bilgi güvenliği ihlali durumunda gerekli görülen yaptırımları uygulamayı,

f) Tabi olduğu ulusal, uluslararası veya sektörel düzenlemelerden, ilgili mevzuat ve standart gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülüklerini karşılamaktan, iç ve dış paydaşlara yönelik kurumsal sorumluluklardan kaynaklanan bilgi güvenliği gereksinimleri sağlamayı,

g) İş/Hizmet sürekliliğine bilgi güvenliği tehditlerinin etkisini azaltmayı ve işin sürekliliği ve sürdürülebilirliğini sağlamayı,

h) Kurulan kontrol altyapısı ile bilgi güvenliği seviyesini korumayı ve iyileştirmeyi,

i) Bilgi güvenliği farkındalığını arttırmak amacıyla yetkinlikleri geliştirecek eğitimleri sağlamayı

Taahhüt eder.

P.02 İNTERNET ERİŞİM POLİTİKASI

Amaç

Bu politika; kurum içinde güvenli internet erişimi için sahip olması gereken standartları belirlemeyi amaçlamaktadır. İnternetin uygun olmayan kullanımı, kurumun yasal yükümlülükleri, kapasite kullanımı ve kurumsal imajı açısından istenmeyen sonuçlara neden olabilir. Bilerek ya da bilmeyerek bu türden olumsuzluklara neden olunmaması ve internetin kurallarına, etiğe ve yasalara uygun kullanımının sağlanmasını amaçlamaktadır.

Kapsam

Bu politika kurum internetini kullanan tüm personeli kapsamaktadır.

Sorumluluk

Bu dokümanın hazırlanmasından, güncellenmesinden BGYS Yönetim Temsilcisi ve BGYS Ekibi, gözden geçirilmesi ve onaylanmasından sorumludur. Dokümanda belirtilen hususları bilmek, uygulamak ve korunmasını sağlamaktan bölüm yöneticileri ve tüm personel sorumludur.

Politika

a) Kurum bilgisayarları içerik denetimi yapan bir uygulama üzerinden internete çıkacaktır. Kurum kültürüne ve yasalara uygun olmayan siteler yasaklıdır. Ancak üst yönetimin yazılı izni ile yetkilendirilmiş kurum personeline internete çıkarken gerekli servisleri kullanma hakkı tanımlanmıştır. (FTP, sosyal medya)

b) 5651 sayılı kanun (İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun) gereği kurum internet erişim kayıtları en az iki yıl arşivlenmektedir.

c) Bilgisayarlar üzerinden yasalara aykırı internet sitelerine girmek ve dosya (film, müzik, program vb.) indirmek yasaktır.

d) Tunnel platformları (VPN), proxy ve DNS değişiklikleri yapılarak internete bağlanılması yasaktır.

e) Sistemler Let's Encrypt ile korunmaktadır. Firma verileri AB bölgesinde güvenli bir sağlayıcıda tutulur. Serverlarımıza sadece SSH üzerinden bağlanılmaktadır. Aktif güvenlik duvarı kullanılmaktadır ve sadece dışarıya 80 ve 443 portları açık durumdadır.

f) Başkalarının fikri haklarını ihlal edici (copyright) materyalin (yazı, makale, kitap, film, müzik eserleri vb.) dağıtımı yasaktır.

g) Sistem ve ağ güvenliğinin ihlal edilmesi yasaktır, cezai ve hukuki mesuliyetle sonuçlanabilir. Kurum bu tür ihlallerin söz konusu olduğu durumları inceler ve eğer bir suç oluştuğundan şüphe duyulursa disiplin yönetmeliğini uygulayabilir veya yasa uygulayıcısı ile işbirliği yapabilir.

h) İnternet üzerinden kullanım amaçlarına uygunsuz, müstehcen, rahatsız edici materyaller ve başkalarına iftira, karalama mahiyetinde mesajlar yayınlamak ve paylaşmak yasaktır.

i) Kullanıcıların internet üzerinden görevleri ile ilgisi bulunmayan, internet trafiğini kısıtlayabilecek veya zarar verebilecek online olarak yayın yapan televizyon, radyo, film, oyun vb. içerikli yayınların kullanılması yasaktır.

j) Kurum e-posta adresi ile internet üzerinde forum, alışveriş vb. sitelere üye olunması yasaktır.

k) Kurum hesaplarına ait kullanıcı adı ve şifrenizin internet üzerinden paylaşılması yasaktır.

l) Kurum içerisinde kullanılan kullanıcı adı ve şifreleri ile sosyal hayatta kullanılan kullanıcı adı ve şifreleri aynı olmamalıdır.

m) İnternet üzerinden yaptığınız kişisel işlemlerinizde (banka, alışveriş, mail vb.) oluşacak olumsuzluklardan kurumumuz sorumlu değildir. Ayrıca, kurum veya kişisel hesabınızı ele geçiren kişi veya kişiler sizin adınıza suç işleyebilir, bu işlemden sorumlu olabilirsiniz.

n) İnternette gezinirken reklam veya bilgi çalmak amaçlı (tebrikler, ödül kazandınız, ödülünüzü almak için tıklayın vb.) aldatıcı resim ve yazılara karşı dikkatli olunmalı ve tıklanmamalıdır.

o) Kurum network ağına kurum dışı cihazların takılması yasaktır.

P.03 E-POSTA POLİTİKASI

Amaç

Bu politika; Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş. e-posta altyapısına yönelik kuralları ortaya koymaktır.

Kapsam

Bu politika; kurum e-postasını kullanan tüm personeli kapsamaktadır.

Politika

a) Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş. personelinin kurum e-postalarından gönderdikleri, aldıkları veya sakladıkları e-postalar Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş. bilgi varlığıdır. Bu yüzden yetkili kişiler gerekli durumlarda önceden haber vermeksizin e-posta mesajlarını denetleyebilir, yasal merciler ile paylaşabilir.

b) Personel e-posta adresi "isimsoyisim" olacak şeklinde açılmaktadır. Örnek: **isim@bursatemizenerji.com** olacak şekilde mail hesabı açılır.

c) Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş. kurumsal e-posta hesapları kişisel amaçlar için kullanılmamalıdır.

d) Kurumun e-posta sistemi, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz. Bu tür özelliklere sahip bir mesaj alındığında hemen ilgili birim yöneticisine veya Bilgi Güvenliği Ekibine haber verilmesi ve daha sonra bu mesajın tamamen silinmesi gerekmektedir.

e) E-posta ile paylaşılamayacak gizlilik seviyesindeki bilgiler gizlilik anlaşması imzalanmamış üçüncü taraflar ile e-posta üzerinden paylaşılmamalıdır.

f) Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.

g) Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen Bilgi Güvenliği Ekibine haber verilmelidir.

h) Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.

i) Kullanıcıların kullanıcı kodu / şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal Bilgi Güvenliği Ekibine haber verilmelidir.

j) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir.

k) Kurum personeli kurumsal e-postaların herhangi bir kişi tarafından okunmamasını sağlamakla yükümlüdür.

P.04 ANTİ-VİRÜS POLİTİKASI

Amaç

Bu politika; Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş.'deki bilgisayar ve sunucuların zararlı yazılımlardan korunmasını amaçlamaktadır.

Kapsam

Bu politika Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş.'deki bilgisayarları ve sunucuları kapsamaktadır.

Politika

a) Kurumun bütün bilgisayarları ve sunucuları anti-virüs yazılımına sahip olmalıdır.

b) Düzenli aralıklarla anti-virüs yazılımı otomatik veya manuel olarak güncellenecektir.

c) Virüs bulaşan makineler tam olarak temizleninceye kadar ağa bağlanmamalıdır.

d) Hiç bir kullanıcı bilgi güvenlik ekibi onayı olmadan (sadece acil durumlarda) herhangi bir sebepten dolayı anti-virüs programını sistemden kaldıramaz veya durduramaz.

e) Bilinmeyen ve şüpheli bir kaynaktan gelen e-posta ve ekleri virüs içerebilir. Kesinlikle açılmamalıdır. Bu tür özelliklere sahip bir mesaj alındığında hemen Bilgi Güvenliği Ekibine haber verilmesi ve yetkili kişiler müdahale edene kadar mesajın silinmemesi, yanıtlanmaması, iletilmemesi ve içeriğine tıklanmaması gerekmektedir.

f) Bilinmeyen ve şüpheli kaynaklardan indirilen dosyaların içerisinde virüs olabilir. Bu tür kaynaklardan dosya indirilmesi yasaktır.

g) Bilgisayarlarda kullanılan CD, USB gibi depolama aygıtları virüs taraması yapılmadan kullanılmamalıdır.

h) Çalışanlar antivirüs programlarını devre dışı bırakmamalı, silmemeli, başka bir antivirüs uygulaması kurmamalı ya da bu işlemlere ilişkin teşebbüslerde bulunmamalıdır.

i) Kurum dışı CD, USB vb. materyaller kurum bilgisayarlarına takılmamalıdır. Oluşabilecek her türlü olumsuzluklardan personel sorumludur.

j) Kurum ağına anti-virüs programı güncel olmayan bilgisayarlar dâhil edilmemelidir.

P.05 PAROLA POLİTİKASI

Amaç

Bu politika; güçlü bir şifreleme oluşturulması ve şifrelerin güvenliğinin sağlanmasını amaçlamaktadır.

Kapsam

Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş.'deki bilgisayarları ve sunucuları kullanan bütün kullanıcı hesaplarını kapsamaktadır.

Politika

a) Kurum içerisinde kullanılan genel kullanıcı bilgisayar şifreleri bilgi güvenliği ekibi dahilinde değiştirilmesi zorunlu kılınmıştır.

b) Parolalar bilgi sistemleri çalışanları, bağlı olunan yönetici ve iş arkadaşları dâhil olmak üzere hiç kimse ile paylaşılmamalı ve periyodik olarak değiştirilmelidir. 90 günde bir şifre değiştirme zorunluluğu vardır.

c) Oluşturulacak şifre içerisinde Türkçe karakter ve son 3 şifre ile aynı nitelikte bulunmamalıdır.

d) Bilgisayar kullanıcı hesaplarının şifreleri en az 8 karakter olmalıdır. Şifre; Büyük harf, Küçük harf, Rakam ve Özel Karakterden en az 3'ünü karşılamalıdır.

e) Şifreleme bilgisayar güvenliği için önemli bir özelliktir. Şifreler kompleks olmalıdır. Kolay tahmin edilen (memleket, çocuk ismi, doğum tarihi, ardışık rakam ve harfler, İstanbul, Ankara, 1qaz2wsx, qwerty vb.) şifreler kullanılmamalıdır.

f) Kullanıcılar bilgisayar başından kalktığı zaman mutlaka oturumlarını kilitlemelidirler Genel kullanıcı bilgisayarları kullanılmadığı zaman otomatik olarak 10 dakika içerisinde şifreli ekran korumasına girecektir.

g) Kurumsal hesaplarınıza ait şifrelerinizin e-posta iletilerine, herhangi bir elektronik forma ve herhangi bir yere not alınması yasaktır.

h) Şifre aile bireyleri dâhil kimseyle paylaşılmamalıdır.

i) Bilgi İşlem Departmanı tarafından size oluşturulan yeni şifreleri hemen değiştirmeniz gerekmektedir.

j) Bir kullanıcı hesabı birden çok kişi tarafından kullanılmamalıdır.

k) Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de kolayca kırılamayacak güçlü bir şifreye sahip olmalıdır.

l) Kişisel Verilerin Korunması Kanunu'na istinaden aktif kurum personelinin bizzat kendi talebi olmaksızın şifresi sıfırlanamaz veya değiştirilemez.

P.06 FİZİKSEL GÜVENLİK POLİTİKASI

Amaç

Bu politika; kurum personeli ve kritik kurumsal bilgilerin korunması amacıyla sistem odasına, kurumsal bilgilerin bulundurulduğu sistemlerin yer aldığı tüm çalışma alanlarına ve kurum binalarına yetkisiz girişlerin önlenmesini amaçlamaktadır.

Kapsam

Kurum binalarında yer alan bilgi varlıklarına erişim sağlayan tüm fiziksel güvenlik konularını kapsamaktadır.

Politika

a) Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binada ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanmalı ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilmelidir.

b) Kurum dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili görevliler gözetiminde gerçekleştirilmelidir.

c) Tanımlanan farklı güvenlik bölgelerine erişim yetkileri düzenli aralıklar ile kontrol edilmelidir.

d) Ofis girişleri ve koridorlar güvenlik açısından kamera ile kayıt altına alınmalıdır.

e) Kritik sistemler özel sistem odalarında ve kilitli dolap kasalarda muhafazası gerekmektedir.

f) Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmalı, yangın ve benzer felaketlere karşı koruma altına alınmalıdır.

g) Açık ofislerde bulunan gizli bilgi varlıklarının olduğu dolaplar ve çekmeceler kilitli ve kontrol altında tutulmalıdır.

h) Bireysel kargo şirketin girişinden fiziksel kontrol sonrasında kurum personeli tarafından alınmaktadır. Kurumsal kargolar güvenlik birimine teslim edilir.

i) Toplantı odalarını kullanan personel, kullanılan yazı tahtasını toplantı sonunda temizlemelidir. Toplantı odasındaki bilgisayar kullanılmış ise toplantı sonunda bilgisayar oturumu kapatılmalıdır. Toplantıda yapılan çalışmaların, alınan kararların ve toplantı notların tutulduğu evrak ve belgeler toplantı masasında ya da çöp kovasında bırakılmamalıdır.

j) Güvenlik kameralarının yerleştirildiği alanlarda kameraların görüntü almasını engelleyecek her hangi bir fiziksel engel bulundurulmamalı, kameralar kapatılmamalı ve fiziksel hasar verilmemelidir.

k) Hasar / hırsızlık gibi oluşabilecek risklere karşı güvenlik sağlanmalıdır.

l) Ekipmanların kullanımı zimmetlenen kişiye aittir, bu ekipmanların güvenliğini sağlanması kişinin sorumluluğundadır.

m) Personeller, çalışma alanları için tahsis edilmiş politika, prosedür ve talimatlara uygun hareket etmelidir.

P.07 SUNUCU GÜVENLİK POLİTİKASI

Amaç

Bu politika; kurumun sahip olduğu sunucuların temel güvenlik kurallarını oluşturmayı amaçlamaktadır.

Kapsam

Bu politika kurumun sahip olduğu bütün sunucuları kapsamaktadır.

Politika

a) Kurum bünyesindeki bütün sunucuların yönetiminden sadece yetkilendirilmiş sistem yöneticileri sorumludur.

b) Bütün sunucular (kurumun sahip olduğu) ilgili envanter yönetim sistemine kayıtlı olmalıdır.

c) Sunucu işletim sistemleri üzerindeki kullanılmayan servisler ve uygulamalar kapatılmalıdır.

d) Çalışanlar görev tanımı dışında kalan sunuculara erişmeye çalışmamalı, müdahale etmemeli, çalışmasını engellemeye ya da performansı azaltmaya yönelik uygulama kurmamalıdır. Personeller kritik sistem ve sunucu saatleri saatlerini değiştirmeye teşebbüs etmemelidir.

e) Sunucular üzerinde yapılan işlemlerin log kayıtları en az 1 ay saklanacak şekilde ayarlanmalıdır.

f) İşletim sistemleri, uygulamalar, veri tabanları, ağ donanımları yetkili erişim logları tutulmalıdır. Böylece güvenlik için gerekli başarılı, başarısız girişler vb. durumlar incelenebilmekte ve ilgili aksiyonlar alınabilmektedir. Her yıl erişim ve yetki kontrolleri gerçekleştirilir.

g) Sunucuların yönetimi için her sunucunun kendi hesabı ile bağlantı yapılmalıdır. Sunuculara dışarıdan yapılan bağlantılar uzak bağlantı politikasının belirlediği kurallara göre yapılmalıdır.

h) Elektrik ve data kabloları sunucu odaları dahil kurum içerisinde kanallardan geçmelidir.

i) Donanımsal ekipmanların bakımları düzenli olarak yapılmalı ve bakım kayıtları tutulmalıdır.

P.08 AĞ YÖNETİMİ POLİTİKASI

Amaç

Kurumun bilgisayar ağında yer alan bilgilerin, ağ alt yapısının ve ekipmanların güvenliğini ve sürekliliğini sağlamayı amaçlamaktadır.

Kapsam

Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş. bünyesindeki ağ altyapısı, ekipman ve kullanıcıları kapsamaktadır.

Politika

a) Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için yedekli ekipman bulundurulmalı veya bakım anlaşmaları yapılmalıdır.

b) Ağ ekipmanları sadece yetkilendirilmiş kişiler tarafından erişilebilir ve yönetilebilir olmalıdır. Yetkisiz erişime karşı korunmalıdır.

c) Ağ hizmetlerinden faydalanan her kullanıcı, erişiminin iş amaçları için verildiğini hatırlayarak iş amaçları dışında kullanımı asgari düzeyde tutarak ağ kaynaklarının etkin kullanımına katkı sağlar.

d) Kurum ağına sadece kurum bilgisayarları bağlanmalıdır. Kurum dışında bir bilgisayar bağlanacak ise yetkili kişinin izni ve gözetiminde bağlanmalıdır.

e) Çalışanlar şirketin faaliyet göstermiş olduğu alanlardaki ağları dinlemeye yönelik herhangi bir uygulamayı, programı bilgisayarına kurmamalı ve bulundurmamalıdır.

f) Kurum internet ağına misafirler alınmamalıdır.

g) Kamera, Kablosuz ağ, misafir ağı ve kullanıcı ağları birbirinden ayrı olmalıdır.

h) Uzaktan bağlantı için kullanılacak portların güvenliği sağlanmalıdır.

i) Ağ cihazları yılda en az 1 defa açıklık tarama testlerinden geçirilerek güvenli hale getirilmelidir.

j) Ağ cihazlarının konfigürasyonları her değişiklikten sonra yedeği alınarak saklanmalıdır.

P.09 UZAK BAĞLANTI VPN POLİTİKASI

Amaç

Bu politika; kuruma dışarıdan yapılacak uzak bağlantının güvenliğini sağlamayı amaçlamaktadır.

Kapsam

Bu politika dışarıdan bağlantı yapacak tüm kurum personelini ve tedarikçileri kapsamaktadır.

Politika

a) Uzaktan bağlantı sadece Team Viewer ile yapılmaktadır.

b) Yetkili personel ilgili sistemlere, yalnızca ofis IP'leri üzerinden VPN ile bağlanabilmektedir.

c) VPN kullanım hakkı verilen kişiler Erişim yetki prosedüründe belirtildiği liste üzerinde düzenli olarak kontrol edilmelidir.

d) Uzak bağlantı yapan kurum dışı bilgisayarlar, Anti-virüs Politikasına uygun bir şekilde cihazların anti-virüs yazılımları kurulu ve güncel olmalıdır.

e) Sadece kurumun onay verdiği kullanıcılar VPN 'i kullanabilir.

f) Kurum personeli dışında üçüncü taraflara verilecek erişimler için gizlilik anlaşması yapılmış olmalıdır.

P.10 TEDARİKÇİ VE ÜÇÜNCÜ TARAF GÜVENLİK POLİTİKASI

Amaç

Bu politika; Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş.'ni bilgi sistemlerine ve bilgi varlıklarına üçüncü taraflar tarafından ulaşılması durumunda güvenliğinin sağlanması amaçlanmaktadır.

Kapsam

Bu politikanın uygulanmasından tüm departmanlar sorumludur.

Politika

a) Tedarikçiler, bakım firmaları veya üçüncü taraflar (müşteriler) bilgi sistemlerimize veya bilgi varlıklarımıza bakım vb. amaç ile geldiklerinde Gizlilik Anlaşması yapılması gerekmektedir.

b) Üçüncü taraflar kurum içerisinde bulundukları sürece kurum politikalarına uygun hareket etmekle yükümlüdürler.

c) Tedarikçilere iletilecek ve aktarılacak kişisel veri sözleşme kapsamına göre belirlenmeli ona göre aktarımı yapılmalıdır.

d) Tedarikçiler, bakım firmaları veya üçüncü taraflar bilgi sistemlerinde veya bilgi varlıkları üzerinde yapacakları çalışmaları Bilgi Güvenliği Yönetim Temsilcisine bildirilmelidir.

e) Tedarikçiler, bakım firmaları veya üçüncü taraflar kurumun bilgi sistemlerine kendilerine verilen yetki kapsamında erişim sağlayabilirler.

f) Tedarikçiler, bakım firmaları veya üçüncü taraflara verilen erişim yetkileri, erişim amaçlarına uygun olarak sadece çalışma alanlarında olacak şekilde kısıtlı verilmeli, logları saklı tutulmalı ve çalışma bittikten sonra verilen yetkiler hemen geri alınmalıdır.

g) Tedarikçiler, bakım firmaları veya üçüncü taraflar bilgi sistemlerine ve bilgi varlıklarına eriştikleri süre boyunca refakatçisiz bırakılmamalıdır.

h) Üçüncü taraflara kurumun ağına erişim izni verilecek bilgisayarlar için Uzak Bağlantı VPN Politikası uygulanacaktır. Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş., tedarikçi, bakım firmaları veya üçüncü taraflara herhangi bir uyarıda bulunmadan ağa olan erişimlerini kesebilir.

P.11 KABUL EDİLEBİLİR KULLANIM POLİTİKASI

Amaç

Bu politika; personelin sistem, bilgi ve varlıkların gizlilik, bütünlük ve erişilebilirlik sınıfları açısından yapılması ve uyulması gereken iş kurallarını bildirmeyi amaçlamaktadır.

Kapsam

Bu politika Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş. bünyesindeki tüm personeli kapsamaktadır.

Politika

a) Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş.'ni gizli olarak belirlediği tüm bilgilerin gizliliğine sıkı bir şekilde uyulacaktır. Kurumun iş gereksinimi dışında bu bilgilerin kopyalanması ve iletilmesi yasaktır.

b) Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş. personeli, kendilerine tahsis edilmiş tüm bilgisayar erişim bilgilerini ve kendisine verilmiş cihazların güvenliğini sağlamakla sorumludur. Erişim bilgileri herhangi birine söylenemez ve bu bilgiler başkaları ile paylaşılamaz.

c) Hiçbir personel, bilgisayarlarından anti virüs koruma yazılımını devre dışı bırakamaz.

d) Kaynağı belli olmayan ve üretici firması tarafından kopya edilmesi yasaklanmış bir bilgisayar yazılımını kopyalamak yasaktır.

e) Bilgisayarlara hiçbir surette lisanssız program yüklenmemelidir.

f) Kullanıcı herhangi bir bilginin çok kritik olduğunu düşünüyorsa o bilgi şifrelenmeli veya yetkili kişiler dışında erişilemeyecek alanlarda saklanmalıdır.

g) Bilgisayarlar üzerinden resmi belgeler, programlar ve eğitim belgeleri haricinde (müzik, film vb.) dosya alışverişinde bulunulmamalıdır.

h) Bilgisayarlarda oyun, eğlence vb. uygulamaların çalıştırılması ve kopyalanması yasaktır.

i) Kritik raporların dökümünü alan kullanıcı, rapor içeriğindeki bilginin uygun bir şekilde korunmasından sorumludur.

j) Herhangi bir kişi kendine ait olmayan kritik bir rapor bulur ise bu durumu Bilgi Güvenliği Yönetim Temsilcisine bildirmelidir.

k) "Gizli" kâğıt belgeleri kilitli dolaplarda muhafaza edilecektir.

l) Sunucu ve bilgisayarların saatleri kullanıcılar tarafından değiştirilemez, saatler sistem tarafından otomatik olarak yönetilmektedir.

m) Laptop bilgisayarlar güvenlik açıklarına karşı korunmalıdır. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmalıdır. Cihazların çalınması veya kaybolması durumunda hemen Bilgi İşlem Departmanı ile iletişime geçilmelidir.

n) Herhangi bir kişi veya kurumun izinsiz kopyalama, ticari sır, patent veya diğer kurum bilgileri, yazılım lisansları vb. hakları kesinlikle ihlal edilmemelidir.

o) Kurum bilgileri kurum dışından üçüncü şahıslara iletilmemelidir.

p) Tüm personel, kendi alanlarına ait Güvenlik Politikalarına uymak zorundadır.

q) Kurum politika ve prosedürleri, bilgi güvenliği ekibi ve ilgili yöneticiler tarafından Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş. personeline, yeni işe başlayanlara ve 3.taraflara duyurulacaktır. İlgili Güvenlik Politikalarına uyulacağı personel iş sözleşmesinde yer almalı ve personele imzalatılmalıdır.

r) Kurum bilgisayarlarında kişisel verilerin barındırılması yasaktır. Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş. kurum ortamında tutulan ve iletilen tüm bilgiler kurumun malıdır ve

Bursa Temiz Enerji Elektrik Üretim San. ve Tic.A.Ş. . bu bilgileri izleme ve denetleme hakkına sahiptir.

s) Kaynağı belli olmayan ve üretici firması tarafından kopya edilmesi yasaklanmış bir bilgisayar yazılımını kopyalamak yasaktır.

t) Hiçbir personel izin almadan kendi bilgisayarından veya başka bir kaynak kullanarak, Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş.'nin bilişim ağını tarayamaz, izleyemez veya dinleyemez.

u) Hiçbir personel, kurum içinde kendilerine tahsis edilen bilgisayar yetkilerinin dışına çıkamaz ve bu konuda yetki aşma işlemine girişemez.

v) Sosyal medya erişimi verilen kullanıcılar görevlerinin dışında bu haklarını kullanmaları yasaktır.

w) Sosyal medya üzerinden kurumu rencide edici, karalayıcı paylaşımlar yapılmamalıdır. Kurumun hassas bilgileri sosyal medya üzerinden paylaşılmamalıdır.

P.12 TEMİZ MASA TEMİZ EKRAN POLİTİKASI

Amaç

Bu politika; Personelin mesai saatleri içi veya dışında kendilerine görevleri gereği paylaşılmış olan bilgilerin yetkisiz erişimler veya uygunsuz kullanımı sonucunda başına gelebilecek riskleri en aza indirmeyi amaçlar.

Kapsam

Çalışma masaları, ekranlar, basılı dokümanlar, belgeler ve kayıtlar.

Politika

a) Çalışma sonunda kâğıt ortamında ya da elektronik cihazlar üzerinde tutulan "gizli ya da çok gizli" bilgiler güvenli ortamlarda (çelik kasa, kilitli dolap ve çekmeceler vb.) saklanacaktır.

b) Her türlü haberleşmede kullanılan cihazlar (telefon, faks, fotokopi makineleri) yetkisiz erişimlere bırakılmayacaktır. Cihazlar üzerinde belge, doküman bırakılmayacaktır.

c) Sistemlerde kullanılan şifre, telefon numarası ve T.C kimlik numarası vb. hassas bilgiler ekran üstlerinde veya masa üstünde bulunmamalıdır.

d) Her türlü bilgi, şifreler, anahtarlar ve bilginin sunulduğu sistemler, ana makineler (sunucu), bilgisayarlar vb. cihazlar yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde başıboş bırakılmamalıdır.

e) Faks ve fotokopi makinelerinde gelen giden yazılar sürekli kontrol edilmeli ve makinede evrak bırakılmamalıdır.

f) Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler kâğıt öğütücü, disk/disket kıyıcı, yakma vb. metotlarla imha edilmeli, bilginin geri dönüşümü ya da yeniden kullanılabilir hale gelmesinin önüne geçilmelidir.

g) Personelin kullandığı masaüstü veya dizüstü bilgisayarlar iş sonunda ya da masa terkedilecekse ekran kilitlenmelidir.

h) Bilgisayarların masaüstlerindeki klasör ve dosyalar düzenli tutulmalıdır.

i) Bilgisayar ekranları yetkisiz kişilerin ekranları izlemesine izin vermeyecek şekilde konumlandırılmalıdır. Bilgisayarların masaüstlerindeki klasör ve dosyalar iş sürekliliği açısından düzenli tutulmalıdır.

P.13 MOBİL VE TAŞINABİLİR CİHAZ POLİTİKASI

Amaç

Bu politika; Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş.'ne ait bilgi içeren mobil ve taşınabilir cihazların kullanımı ile ilgili kuralları belirlemeyi amaçlar.

Kapsam

Bu politikanın uygulanmasından mobil ve taşınabilir cihaz kullanan tüm personel sorumludur.

Politika

a) Kuruluşa ait bilgi içeren taşınabilir cihazlar ilgili kişiye zimmetlenerek teslim edilmelidir.

b) Her çalışan kendisine zimmetlenen cihazın güvenliğinden ve amacına uygun kullanımından sorumludur.

c) Etki alanı dâhilindeki bilgisayarlar admin yetkisi sınırlandırılarak yalnızca User yetkilendirmesi ile ilgili kişiye teslim edilmelidir. Etki alanından bağımsız olan bilgisayarların sorumluluğu personele aittir.

d) Mobil cihaz kullanımı gereksinimi ortadan kalktığında haklar / erişimler iptal edilir.

e) Kullanıcılar mobil cihazları üzerinden eriştikleri bilgilerin güvenliğini sağlamaktan sorumludurlar. Çalışanlar sorumlu olduğu bilgilerin erişim bilgilerini başkaları ile paylaşmamalıdır.

f) Taşınabilir cihazlara (tablet, laptop) yetkisiz erişime karşı şifre tanımlanmalıdır.

g) Etki alanı dâhilindeki bilgisayarlar üzerinde yapılan çalışmalar ve oluşturulan dosyalar departmanlara ait ilgili ortak alana kaydedilmelidir.

h) Taşınabilir cihazlar aile bireyleri dâhil yetki dışı hiç kimse tarafından kullandırılmamalıdır.

i) Taşınabilir cihazlarda hassas ve gizli bilgiler mümkün olduğunca bulundurulmamalıdır.

j) Çalışanlar, şirketin tahsis ettiği bilgisayarlarda kişisel verilerini barındırmamalıdır.

k) Kaybolması ve çalınması kolay olduğundan mobil cihazlar başıboş bırakılmamalıdır.

l) Kullanıcı hatası sebebiyle kurumsal cihaza hasar vermişse verilen hasarı tazminle ödemeye hükümlüdür.

P.14 VERİTABANI GÜVENLİK POLİTİKASI

Amaç

Bu Politika; kurumun veri tabanı sistemlerinin, kesintisiz ve güvenli şekilde işletilmesine yönelik standartları belirtmeyi amaçlamaktadır.

Kapsam

Tüm veri tabanı sistemleri, bu politikaların kapsamı dahilinde yer alır.

Politika

a) Veri tabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilmelidir. Log kayıtlarına, yetkilinin izni olmadan kesinlikle hiçbir şekilde erişim yapılamaz.

b) Veri tabanı sunucusuna, sadece yetki hakkına sahip olanlar bağlanır.

c) Veri tabanı bulunan sistemlere erişim yetkileri kayıt altına alınmalı ve bu yetkiler kontrol edilmelidir.

d) Veri tabanı sistemlerinde tutulan bilgiler sınıflandırılır ve uygun yedekleme politikaları oluşturulur. Yedeklemeden sorumlu sistem yöneticileri belirlenir ve yedeklerin düzenli alınması sağlanır.

e) Bilgilerin saklandığı sistemler, Güvenliği sağlanmış AB alanındaki sanal sunucularda tutulur.

f) Veri tabanı sistemlerinde yapılacak bakım onarım, yama ve güncelleme çalışmalarından önce, ilgili birimlere duyuru yapılmalıdır.

g) Veri tabanına acil erişim gerekmesi durumunda aksiyon öncesinde ve sonrasında ilgili birimlere veya personellere bilgilendirme yapılır.

h) Veri tabanı aksiyonlarında Erişim yetkisi sadece Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş. yazılım sorumlusuna aittir.

i) Veri tabanları yedekleme listesine göre düzenli olarak yedeklenmelidir.

j) Veri tabanı bulunan medyalar kurum dışına çıkarılmamalıdır.

k) Veri tabanlarının bulunduğu medyaların doluluk oranları düzenli olarak kontrol edilmelidir.

l) Veritabanı raporları düzenli olarak ilgili firma tarafından verilmelidir.

P.15 DEĞİŞİM YÖNETİMİ POLİTİKASI

Amaç

Bu Politika; kurumun bilgi sistemlerinde yapılması gereken yazılımsal ve donanımsal değişikliklerinin güvenlik ve sistem sürekliliğini aksatmayacak şekilde yürütülmesini sağlamayı amaçlamaktadır.

Kapsam

Tüm bilgi sistemleri ve bu sistemlerin işletilmesinden sorumlu personel bu politikanın kapsamında yer almaktadır.

Politika

a) Yazılımsal ve donanımsal değişikliklerin talepleri kayıt altında tutulmalıdır.

b) Bilgi sistemlerinde değişiklik yetkilendirilmiş kişiler tarafından yapılır.

c) Herhangi bir sistemde uzun süreli veya önemli değişiklik yapmadan önce, bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenmeli ve ilgili kişilere bilgi verilmeli.

d) Değişiklikler gerçekleştirilmeden önce kurumun ilgili birime / kişiye bilgi verilmelidir.

e) Yapılacak değişiklikten önce değişikliğin yapılacağı sistemlerin yedekleri alınmalıdır.

f) Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanmalı ve ilgili yöneticilere bilgi verilmelidir.

g) Ticari programlarda yapılacak değişiklikler, ilgili üretici tarafından onaylanmış kurallar çerçevesinde gerçekleştirilmelidir.

h) Yapılacak değişiklikler mümkün olduğunca test sunucuları üzerinde gerçekleştirilmelidir, yapılan testlerin başarılı geçmesi halinde canlı sistemde değişiklik gerçekleştirilmelidir. Test sunucusu ve canlı sunucu tüm sistemleri birbirinden tamamen bağımsızdır

i) Değişikliğin varlık kritikliğine göre yapılacağı zaman ve yöntemler, işlemi yapacak bilgi işlem personeli tarafından yönetime bildirmelidir.

j) Farklı bir sağlayıcıya geçiş işlemi risk planında değerlendirilir. Firma acil bir durum veya farklı bir gelişmeden dolayı sağlayıcısını değiştirmesi gerektiğinde bunu kendi iç ekipleri ile bir plan halinde tasarlar ve en az 2 ay önceden firmanın verilerini ve çalınmasını etkilemeyecek şekilde uygulamaya geçirir. Bilgilendirme yazılı olarak e-mail ile yapılır. Geçiş planı ve aksiyonları, oluşabilecek riskler hakkında paydaşlarına bilgi verir

P.16 KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI

Amaç

Bu politika; kurumun bilgi sistemlerine erişimde kimlik doğrulaması ve yetkilendirme politikalarını tanımlamaktır.

Kapsam

Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş. bilgi sistemlerine erişen kurum personeli ile kurum dışı kullanıcılar bu politika kapsamı altındadır.

Politika

a) Kurum sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenecektir.

b) Kurum sistemlerine erişmesi gereken firma kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanacaktır.

c) Kurum bünyesinde kullanılan ve merkezi olarak erişilen uygulama yazılımları, paket programlar, veri tabanları, işletim sistemleri ve log-on olarak erişilen sistemler üzerindeki kullanıcı rolleri ve yetkiler belirlenmeli ve denetim altında tutulmalıdır.

d) Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilmelidir.

e) Kullanıcılar da kurum tarafından kullanımlarına tahsis edilen sistemlerin güvenliğinden sorumludur.

f) Sistemlerin başarılı ve başarısız erişim logları düzenli olarak tutulmalıdır.

g) Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.

h) Sistemlere log-on olan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve kayıt alınmalıdır.

i) Kullanıcı hatalarını kaydetmek ve takip etmek amacıyla olay ihlal formu açılmaktadır.

P.17 KRİPTOGRAFİK KONTROLLER POLİTİKASI

Amaç

Bu politikanın amacı; bilginin gizliliği, aslına uygunluğu ya da bütünlüğünün korunmasıdır.

Kapsam

Bu politika bilgi varlıklarının saklandığı sistemler ve o sistemlere erişimin yapıldığı ağların şifre politikasını kapsamaktadır.

Politika

a) Kurum içerisinde tanımlanan gizli bilgi varlıkları kriptografik şifreleme yöntemleri ile saklanmalıdır. Her personel kendi barındırdığı bilgi varlıklarından güvenliğinden sorumludur.

b) Çalışanlar, kendilerine verilen e-imza, e-fatura, kep vb. kritik bilgi içeren yetki ve kriptografik anahtarların uygun şekilde korumakla sorumludur.

c) Risk değerlendirmelerine göre yüksek düzeyde koruma gerektiren bilgi varlıklarının korunmasında güçlü şifreleme algoritması kullanılmalıdır.

d) Mobil cihazlardaki verilerin korunmasında güçlü şifre kullanılmalıdır.

e) Mail hesabı kurulu akıllı telefonlarda telefon kilidi kullanılması zorunludur.

f) Tanımlanan şifreler belirli aralıklarla değiştirilmelidir.

P.18 ZİYARETÇİ KABUL POLİTİKASI

Amaç

Bu politikanın amacı; dışarıdan gelen misafirlerin kabulü, kuruluş içinde dolaşmaları ve kuruluştan uğurlanmaları ile ilgili kuralları belirlemektir.

Kapsam

Bu politikanın uygulanmasından Bursa Temiz Enerji Elektrik Üretim San. ve Tic.A.Ş. . deki tüm yöneticiler ve personel sorumludur.

Politika

a) Dışarıdan ziyaret amaçlı gelen kişiler kuruluş girişinde güvenlik tarafından karşılanır ve kimlik kontrolü sağlanıp kurum içine girişine izin verilir.

b) Kurum içine gelen ziyaretçiler kamera sistemi ile takip edilmektedir.

c) Kritik birimlere yetkisiz ziyaret girişlerini kısıtlamak için fiziksel güvenlik önlemleri alınmıştır.

d) 5651 İnternet Ortamında Yapılan Yayınlar Kapsamında loglar tutulmakta ve saklanmaktadır.

e) Bu politikaya uygun olarak çalışmayan tüm personel hakkında Disiplin Prosedüründe belirtilen Disiplin Yönetmeliği Maddeleri uygulanır.

P.19 OLAY İHLAL BİLDİRİM VE YÖNETİM POLİTİKASI

Amaç

Bu politikanın amacı; Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş.'nin bilgi güvenliği olay ihlal süreçlerinin belirlenmesidir.

Kapsam

Bu politikanın uygulanmasından tüm personel sorumludur.

Politika

a) Bilginin gizlilik, bütünlük ve erişilebilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumlarında mutlaka kayıt altına alınmalıdır.

b) Bilgi güvenliği olay raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci oluşturulmalıdır.

c) Bilgi güvenliği ihlâli oluşması durumunda, kişilerin tüm gerekli faaliyetleri değerlendirmesi Bilgi Güvenliği Ekibi ile birlikte yapılmalıdır.

d) İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.

e) Tüm personel, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği ihlallerini önlemek maksadıyla güvenlik zayıflıklarını doğrudan kendi yönetimlerine ve Bilgi Güvenliği Ekibine mümkün olan en kısa sürede rapor verilmelidir.

f) Normal olasılık planlarına ilave olarak olayın tanımı ve sebebinin analizi, önleme, tekrarı önlemek maksadıyla düzeltici tedbirlerin planlanması ve uygulanması, olaylardan etkilenen veya olaylardan kurtulanlarla iletişim, eylemin ilgili otoritelere raporlanması konuları göz önüne alınır.

g) İç problem analizi, adli incelemeler veya üretici firmadan zararın telafi edilmesi için aynı türdeki olayların izleme kayıtları (log) toplanır ve korunur.

h) Güvenlik ihlallerinden kurtulmak için gereken eylemler, sistem hatalarının düzeltilmesi hususları dikkate alınır.

i) Bilgi güvenliği olaylarının değerlendirilmesi sonucunda edinilen bilgi ile edinilen tecrübe, yeni kontrollerin oluşturulması, olayların kök nedenine inilmesi ve yazılı hale getirilmesi gerekmektedir.

j) Kanıt toplama faaliyetinde aşağıdaki süreçler takip edilmelidir;

- Kanıtın niteliği ve tamlığını gösteren içerik.
- İhlale neden olan olayların kanıtları için kamera kayıtları, giriş çıkış kayıtları, sunucu/program ve bilgisayar logları, firewall logları ve internet loglarından faydalanılır.
- Olay kanıtlarının korunması yetkili kişilerin dışında erişimi kapatarak veya yedekleme yaparak sağlanır.

k) Bu politikaya uygun olarak çalışmayan tüm personel hakkında Disiplin Prosedüründe belirtilen Disiplin Yönetmeliği Maddeleri uygulanır.

P.20 GÜVENLİ YAZILIM GELİŞTİRME POLİTİKASI

Amaç

Bu politika; Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş.'ni bilgi güvenliği güvenli yazılım geliştirme süreçlerinin güvenlik ve sistem sürekliliğini aksatmayacak şekilde yürütülmesini amaçlamaktadır.

Kapsam

Bu politikanın uygulanmasından ilgili personel sorumludur.

Politika

a) Yönetim sadece uygun yazılım projelerinin başlatıldığından ve proje altyapısının uygun olduğundan emin olmalıdır.

b) Uygulama yazılımlarının kurum içerisinde mi hazırlanacağı yoksa satın mı alınacağının belirlenmesi, uygun bir şekilde tanımlanmalıdır.

c) Sistem geliştirmede, ihtiyaç analizi, fizibilite çalışması, tasarım, geliştirme, deneme ve onaylama safhalarını içeren sağlıklı bir iş planı kullanılmalıdır.

d) Kurum içinde geliştirilmiş yazılımlar ve seçilen paket sistemler, ihtiyaçları karşılamalıdır.

e) Yazılım geliştirme politikalarına uygun olmayan, ulusal ve uluslararası yazılım geliştirme standartları çerçevesinde geliştirilmemiş ve kurum talebi olmaksızın üretilmiş olan yazılımların kurumsal sistemler üzerine entegre edilmesine izin verilmemelidir.

f) Hazırlanan sistemler mevcut prosedürler dâhilinde, işin gerekliliklerini yerine getirdiklerinden ve iç kontrol yapıldığından emin olunması açısından test edilmeli, yapılan testler ve test sonuçları ilgili personele e-posta ile bilgilendirmesi yapılmalıdır.

g) Yeni alınmış veya revize edilmiş bütün yazılımlar test ortamında kontrol edilmelidir. Herhangi bir sorun görülmesi durumunda üretici firma ile iletişime geçilip çözüm arayışına girilir.

h) Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.

i) Yazılımlar sınıflandırılmalı ve envanterleri çıkarılarak varlık envanterinde güncellenmelidir.

j) Kurumda kişisel olarak geliştirilmiş yazılımların kullanılması engellenmelidir.

k) Eski sistemlerdeki veriler tamamen, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılmalıdır.

P.21 ERİŞİM KONTROL POLİTİKASI:

Amaç

Bu politika; yetkili kullanıcı erişimini sağlamak ve yetkisiz erişimi önlemek amacıyla oluşturulmuştur.

Kapsam

Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş.'ni müşterilere, personeline ve tedarikçilerine sunduğu yazılım ve donanım sistemlerinde, yetkili ve yetkisiz kullanıcı erişimleri, yeni kullanıcıların kayıt başlangıçlarından, bilgi sistemlerine ve hizmetlerine erişim gereksinimi artık kalmamış kullanıcıların son kayıttan çıkışlarına kadar olan basamakları içermelidir.

Politika

a) Kurum içerisinde giriş çıkışlar kamera sistemi ile kayıt altına alınmalıdır.

b) Kullanıcılar taşınabilir medyaları (CD, USB, vb.) sadece iş amaçlı kullanmalı ve bu medyalar takıldığı zaman antivirüs yazılımı ile taranmalıdır.

c) Aktif dizine bağlanan kullanıcı parolaları Şifre Politikasına uygun tanımlanmalıdır.

d) Ağ üzerinde aktif departmanlar için ortak alanlar oluşturulmalıdır. Bu ortak alanlar üzerindeki birimler ve kullanıcılara göre yetkilendirme yapılmalıdır.

e) Çalışanlar şirketin vermiş olduğu erişim yetkileri ile sadece kendilerine tanımlanmış alanlara bağlanmalıdır.

f) Yönetim tarafından yetkilendirilen personel haricinde hiçbir personelin dosya silme yetkisi bulunmamalıdır. Silme işlemi sadece ilgili departmanlar tarafından tanımlanan kişiler tarafından yapılmalıdır.

g) Yazılım departmanı üzerine verilen erişimler kontrol edilmelidir.

h) Kurumda mümkün olduğunca SSL ya da benzeri güvenlik protokollerinin kullanılması benimsenmiştir.

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKALARI KABUL ONAYI

Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş. Yönetim Sistemi Politikalarında ifade edilen tüm kurallara uymayı, iş bu güvenlik politikalarının ve revizyonlarının Bilgi Güvenliği Yönetim Sistemi'nde yayınlandığını bildiğinizi ve güncellemeleri takip ederek iş bu değişikliklere uygun davranacağınızı aksi takdirde hakkınızda disiplin ve yasal her türlü işlemin başlatılacağını bildiğinizi kabul ve taahhüt etmektesiniz.

İzlenecek Prosedür

1. Bilgi Güvenliği Politikasını okuyunuz.
2. Aşağıdaki belirtilen bölümlere bilgileri doldurup imzalayınız.
3. Bu sayfayı Yönetim Temsilcisi'ne teslim ediniz.

Anlaşma

Bu forma imza atarak aşağıda yazılanları kabul etmiş oluyorum.
Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş. Bilgi Güvenliği Politikası kabul onayının bir kopyasını teslim aldım, okudum ve anladım.

Personelin;
İmzası :

Adı ve Soyadı :

Unvanı :

Bölümü :

Tarih :

Bu form Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş. Bilgi Güvenliği Politikasının okunduğu, anlaşıldığı ve kabul edildiğinin onaylandığı bir dokümandır. Bursa Temiz Enerji Elektrik Üretim San. ve Tic. A.Ş. kurumunun yönetim temsilcisi ve en üst düzey yöneticisi bu politikanın uygulanabilirliğinden sorumludur.
Bilgi Güvenliği Politikasının onaylayıp yürürlüğe girmesinde Yönetim Temsilcisi sorumludur. Personellere duyuru sadece fiziksel olarak değil, e-mail yoluyla da gerçekleştirip onay alma hakkına sahiptir.