BİLGİ GÜVENLİĞİ BELGESİ

2018

İÇİNDEKİLER

GİRİŞ …….. 3
TERİMLER ……. 4
1. E-POSTA POLİTİKASI …… 6
2. ŞİFRE POLİTİKASI ……. 7
3. ANTİ-VİRÜS POLİTİKASI …… 9
4. İNTERNET ERİŞİM VE KULLANIM POLİTİKASI ……. 9
5. SUNUCU GÜVENLİK POLİTİKASI …….. 10
6. VERİTABANI GÜVENLİK POLİTİKASI ……. 11
7. BİLGİ SİSTEMLERİ YEDEKLEME POLİTİKASI …… 13
8. GÜVENLİK AÇIKLARI TESPİT ETME POLİTİKASI ……..... 14
9. AĞ CİHAZLARI GÜVENLİK POLİTİKASI ……... 14
10. AĞ YÖNETİMİ POLİTİKASI ……. 15
11. UZAKTAN ERİŞİM POLİTİKASI ……. 16
12. SANAL ÖZEL AĞ POLİTİKASI ……. 17
13. RİSK DEĞERLENDİRME POLİTİKASI …… 17
14. KABLOSUZ İLETİŞİM POLİTİKASI …… 18
15. BİLGİ SİSTEMLERİNİN KULLANIM POLİTİKASI ……..... 18
16. DONANIM VE YAZILIM ENVANTERİ OLUŞTURULMA POLİTİKASI 21
17. KRİZ / ACİL DURUM YÖNETİMİ POLİTİKASI …….. 21
18. FİZİKSEL GÜVENLİK POLİTİKASI …… 22
19. KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI …… 22
20. DEĞİŞİM YÖNETİMİ POLİTİKASI …… 23
21. PERSONEL GÜVENLİĞİ POLİTİKASI …….. 24
22. BAKIM POLİTİKASI …… 25
23. UZAKTAN ERİŞİM POLİTİKASI …… 25
24. YAZILIM GELİŞTİRME …… 26
25. PERSONEL VE EĞİTİM …… 26
26. BELGELENDİRME …… 27

GİRİŞ

Günümüzde bilişim sistemleri ve teknolojileri hızla gelişmekte ve değişmektedir. Bunun sonucunda çeşitli ağ yapıları, işletim sistemleri ve iş uygulamaları ortaya çıkmaktadır. Bu çeşitlilik içerisinde kurumlar bilişim sistemlerini organize ederken bilginin gizliliği, bütünlüğü ve erişebilirliği konularında dikkat sarf etmelidirler. Bilginin elektronik ortamda tutulması ile birlikte bunun kullanımı, paylaşımı ve iletimi bilgi güvenliği açısından kritik öneme sahiptir. Bilginin kurumlar arasında iletişimi ve ayrıca İnternete açık olması bilgi güvenliği riskini daha fazla arttırmaktadır. Bu belge, Türk Dil Kurumu Başkanlığının bütün birimlerinde bilgi sistemlerinin güvenliğinin sağlanması için uyulması gereken standartları belirtmektedir. Ekteki politika ve talimatlar aşağıda belirtilen amaçları taşımaktadır.

· Bilgi sistemlerinde paylaşılmakta olan idari, mali ve bilimsel verilerin güvenliğini sağlamak,
· İş devamlılığını sağlamak ve güvenlik ihlalinden kaynaklanabilecek riskleri en aza indirmek.
· Yatırımları korumak.
· Kurumun itibarını korumak.

Bilgi Güvenliği Politikası; Türk Dil Kurumu Başkanlığının bütün birimlerinde, bilişim sistemlerini tasarlarken ve işletirken bilgi güvenliği konusunda uyulması gereken kuralları açıklamaktadır. Bu doküman en üst düzey yöneticiden en alt düzey çalışana kadar bütün kurum çalışanlarını ilgilendirmektedir. Hangi politikadan kimlerin sorumlu olacağı ilgili kısımlarda belirtilmiştir. Bütün çalışanların bu doküman içerisinde kendisi ile ilgili bölümleri okumaları ve tatbik etmeleri gerekmektedir. Dokümanın en son sayfasındaki "Bilgi Güvenliği Politikası Onayı" formunu ilgili çalışanların imzalaması gerekmektedir. Bu doküman içerisinde belirtilen güvenlik politikalarını ihlal eden kurum çalışanları hakkında mevcut yasalar çerçevesinde idari soruşturma açılabilecektir.

TERİMLER

Zincir e-posta: E-postaların art arda gönderilmesidir. Örnek; bir kullanıcıya gelen bir e-postada başka e-posta kullanıcılarına da iletme isteği vardır. Bunlar, şans ve para kazanma yöntemleri gibi bir içeriğe sahiptir.

Spam e-posta: Yetkisiz ve/veya istenmeyen mesajların toplu olarak e-posta ile gönderilmesidir.

DMZ (De-militarized Zone): Kuruluşun dışında, İnternet tarafında olan bir ağ bölümüdür.

Kablo Modem: Kablo üzerinden geniş İnternet erişimidir.
Dial-up Modem: Telefon hatları vasıtası ile bilgisayarlar arasında veri alışverişini sağlayan arabirim cihazıdır.

Dual Homing: Bir bilgisayardan aynı anda birden fazla bağlantı yapılması. Örnek; Kullanıcı yerel alan ağına bağlı olduğu halde İnternete bağlanmasıdır.

Uzaktan Erişim (RDP): İnternet, telefon hatları veya kiralık hatlar vasıtası ile kurumun ağına erişilmesidir.

Split-tunneling: Kurumun ağına VPN ile bağlı olduğu halde aynı anda kurum dışı ağa (örnek, İnternet) bağlanılması, VPN uzak ağa İnternet vasıtası ile erişimin güvenli bir yöntemidir.

Risk: Kurumun bilgi sistemlerin gizliliğini, mevcudiyetini ve bütünlüğünü etkileyen faktörlerdir.

Kullanıcı Denetimi: Sisteme erişmek isteyen kullanıcının yetkili olup olmadığını denetleme metodudur.

Güvenli Kanal: Güçlü bir şifrelemeden oluşan iletişim kanalıdır.

Uygulama Sunucusu: Bir ağda bulunan bir bilgisayarda çalıştırılan uygulamaların çalıştığı sunucudur. Üç katmanlı uygulamaların bir parçasıdır. Bu üç katman: Kullanıcı arayüzü (GUI), uygulama sunucusu ve veritabanı sunucusudur.

Yetkilendirme (authorization): Sisteme giriş izni vermek. Çok kullanıcılı sistemlerde sistem yöneticisi, sisteme girebilecek kişilere giriş izni ve kişilere bağlı olarak da sistemde yapabileceği işlemler için belirli izinler verir.

Yedekleme: Ekipmanın bozulması durumu düşünülerek dosyaların veya veritabanının başka bir yere kopyalanması işlemidir.

Veritabanı (database): Kolayca erişilebilecek, yönetilebilecek ve güncellenebilecek şekilde düzenlenmiş olan bir veri topluluğudur.

Varsayılan (default): Kullanıcı bir ayar parametresi veya herhangi bir değeri belirlemediği zaman, uygulamanın kullandığı daha önceden belirlenmiş sabit bir değer veya ayar parametresidir.

Şifreleme (encryption): Veriyi, istenmeyen kişilerin anlamayacakları bir biçime sokan özel bir algoritma uygulamasıdır.

Hacker: Aslen akıllı programcı anlamına gelen bir terim, ancak günümüzde İnternet üzerinden bilgisayar sistemlerini çökertmeye çalışan kötü niyetli programcılar için kullanılmaktadır.

SSL (Secure Sockets Layer): Ağ üzerindeki mesaj iletişiminin güvenliğinin yönetimi için Netscape tarafından oluşturulmuş bir program katmanıdır.

VPN (Virtual Private Network): Sanal özel ağ. Herkese açık olan iletişim altyapısını kullanan özel bir veri ağıdır. Tünel protokolü ve çeşitli güvenlik prosedürleri ile izinsiz girişlere karşı korunur.

VLAN (Virtual LAN): Sanal yerel ağ. Birçok farklı ağ bölümüne dağılmış olan, ancak aynı kabloya bağlıymışlar gibi birbiri ile iletişim kurmaları sağlanan, bir veya birkaç yerel ağ üzerindeki cihazlar grubudur.

Passphrase: Uzun Şifredir.

1. E-POSTA POLİTİKASI

1.1 Amaç

Bu politikanın amacı Türk Dil Kurumu Başkanlığının e-posta altyapısına yönelik kuralları ortaya koymaktır. Kurumda oluşturulan e-postalar resmi bir kimlik taşımaktadırlar. E-posta, Türk Dil Kurumu Başkanlığının en önemli iletişim kanallarından biridir ve bu kanalın kullanılması kaçınılmazdır. Bunun yanı sıra e-posta, basitliği ve hızı nedeni ile yanlış kullanıma veya gereğinden fazla kullanıma açık bir kanaldır.

1.2 Kapsam Bu politika kurumda oluşturulan e-postaların doğru kullanımını içermektedir ve bütün çalışanları kapsamaktadır.

1.3. Politika

1.3.1 Yasaklanmış Kullanım

a) 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 haber verilmesi ve daha sonra bu mesajın tamamen silinmesi gerekmektedir.

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

c) Kurum ile ilgili olan hiçbir gizli bilgi, gönderilen mesajlarda yer alamaz. Buna, kapsamı içerisine iliştirilen öğeler de dâhildir.

ç) Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.

d) Kişisel kullanım için İnternet'teki listelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.

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

f) Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.

g) Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme, vb.) gönderemez.

1.3.2 Kişisel Kullanım

a) Türk Dil Kurumu Başkanlığında kişisel amaçlar için e-posta kullanımı mümkün olduğunca makul seviyede olmalıdır. Ayrıca iş dışındaki e-postalar farklı bir klasör içerisinde saklanmalıdır.

b) Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu yüzden şifre kullanılmalı ve e-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.

c) Gizli ve hassas bilgi içeren elektronik postalar kriptolanarak (şifrelenerek) iletilmelidir.

ç) Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.

d) Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplandırmalıdır.

e) Kurum çalışanları, kurumsal e-postaların kurum dışındaki yetkisiz şahıslar tarafından görülmesini ve okunmasını engellemek zorundadırlar.

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

g) Elektronik postaların sık sık gözden geçirilmesi, gelen mesajların uzun süreli olarak genel elektronik posta sunucusunda bırakılmaması ve bilgisayardaki kişisel klasöre çekilmesi gerekmektedir.

ğ) 6 ay süreyle hiç kullanılmamış e-posta adresleri kullanıcıya haber vermeden kapatılabilir.

h) E-posta adresine sahip kullanıcı herhangi bir sebepten birim değiştirme, emekli olma işten ayrılma sebepleriyle kurumdaki değişikliğinin yetkililer tarafından Bilgi İşlem birimine bu değişikliğin en geç 15 gün içinde bildirilmesi gerekmektedir.

1.3.3 Gözlemleme Bilgi Güvenliği Politikası

Türk Dil Kurumu Başkanlığı çalışanları gönderdikleri, aldıkları veya sakladıkları epostalarda kişisellik aramamalıdır. Bu yüzden yetkili kişiler önceden haber vermeksizin epostaları denetleyebilirler.

1.3.4 E-Posta Yönetimi

Türk Dil Kurumu Başkanlığı e-postaların kurum bünyesinde güvenli ve başarılı bir şekilde iletilmesi için gerekli yönetim ve alt yapıyı sağlamakla sorumludur

1.3.5 E-Posta Virüs Koruma

Virüs, solucan, truva atı veya diğer zararlı kodlar bulaşmış olan bir e-posta kullanıcıya zarar verebilir. Bu tür virüsler bulaşmış e-postalar, Anti-virüs sistemleri tarafından analiz edilip temizlenmelidir. Ağ güvenlik yöneticileri bu sistemden sorumludur.

2. ŞİFRE POLİTİKASI

2.1. Genel Bakış

Şifreleme bilgisayar güvenliği için önemli bir özelliktir. Kullanıcı hesapları için ilk güvenlik katmanıdır. Zayıf seçilmiş bir şifre ağ güvenliğini tümüyle riske atabilir. Türk Dil Kurumu Başkanlığı çalışanları ve uzak noktalardan erişenler aşağıda belirtilen kurallar dâhilinde şifreleme yapmakla sorumludurlar.

2.2 Amaç

Bu politikanın amacı güçlü bir şifreleme oluşturulması, oluşturulan şifrenin korunması ve bu şifrenin değiştirilme sıklığı hakkında standart oluşturmaktır.

2.3 Kapsam

Bu politika, kullanıcı hesabı olan (bilgisayar ağına erişen ve şifre gerektiren kişiler) bütün kullanıcıları kapsamaktadır.

2.4 Politika

2.4.1 Genel

a) Bütün sistem seviyeli şifreler (örnek: root, administrator, enable, vs.) en az üç ayda bir değiştirilmelidir.

b) Bütün kullanıcı seviyeli şifreler (örnek, e-posta, web, masaüstü bilgisayar vs.) en az altı ayda bir değiştirilmelidir. Tavsiye edilen değiştirme süresi her dört ayda birdir.

c) Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.

ç) Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.

d) Kullanıcı, şifresini başkası ile paylaşmaması, herhangi bir kağıda ya da elektronik ortama yazmaması konusunda eğitilmelidir.

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

f) Şifrelerin ilgili kişiye gönderilmesi "kişiye özel" olarak yapılmalıdır.

g) Bir kullanıcı adı ve şifresi birden çok bilgisayarda kullanılmamalıdır. Bütün kullanıcı ve sistem seviyeli şifrelemeler aşağıdaki ana noktalara uymalıdır.

2.4.2 Ana Noktalar

A. Genel Şifre Oluşturma Kuralları

Şifreler değişik amaçlar için kullanılmaktadır. Bunlardan bazıları: Kullanıcı şifreleri, web erişim şifreleri, e-posta erişim şifreleri, ekran koruma şifreleri, yönlendirici erişim şifreleri vs. Bütün kullanıcılar güçlü bir şifre seçimi hakkında özen göstermelidir. Zayıf şifreler aşağıda belirtilen karakteristiklere sahiptir:

a) Şifreler sekizden daha az karaktere sahiptirler.

b) Şifreler sözlükte bulunan bir kelimeye sahiptir.

c) Şifreler aşağıdaki gibi ortak değere sahiptir.

-Ailesinin, arkadaşının, sahip olduğu bir hayvanın veya bir sanatçının ismine sahiptir

-Bilgisayar terminolojisi ve isimleri, komutlar siteler, donanım veya yazılım gibi.

-"kurum adı", "başkanlık", gibi isimler.

-Doğum tarihi veya adres telefon numaraları gibi kişisel bilgiler

-Aaabbb, qwerytzyxwuts,

123321 vs. gibi sıralı harf ve rakamlar

-Yukardaki herhangi bir kelime geri yazılış şekli

-Yukardaki herhangi bir kelimenin rakamla takip edilmesi (örnek: gizli1, gizli2).

Güçlü şifreler aşağıdaki karakteristiklere sahiptir:

a) Küçük ve büyük karakterlere sahiptir (örnek, a-z, A-Z)

b) Hem dijit hem de noktalama karakterleri ve ayrıca harflere sahiptir. (0-9,!@#$^&*()_+|~-=/,{}[]:";<>?,./)

c) En az sekiz adet alfa nümerik karaktere sahiptir.

ç) Her hangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.

d) Aile isimleri gibi kişisel bilgiler olmamalıdır.

e) Şifreler her hangi bir yere yazılmamalıdır veya elektronik ortamda tutulmamalıdır. Kolayca hatırlanabilen şifreler oluşturulmalıdır. Örnek olarak ; "olmaya devlet cihan bir nefes sıhhat gibi" cümlesi "Odc1nSg!" veya türevleri şeklinde olabilir.

B. Şifre Koruma Standartları

Türk Dil Kurumu Başkanlığı bünyesinde kullanılan şifreleri kurum dışında herhangi bir şekilde kullanmayınız (örnek, İnternet erişim şifreleri, bankacılık işlemlerinde veya diğer yerlerde) Değişik sistemler için farklı şifreleme kullanın. Örnek, Unix sistemler için farklı şifre, Windows sistemler için farklı şifre kullanınız.

Türk Dil Kurumu Başkanlığı bünyesinde kullanılan şifreleri herhangi bir kimse ile paylaşmayınız bütün şifreler Türk Dil Kurumu Başkanlığına ait gizli bilgiler olarak düşünülmelidir. Aşağıdakiler yapılmayacakların listesidir:

Herhangi bir kişiye telefonda şifre vermek,
E-posta mesajlarında şifre belirtmek,
Başkaları önünde şifreler hakkında konuşmak,
Aile isimleri şifre olarak kullanmak,
Herhangi form üzerinde şifre belirtmek,
Şifreleri aile bireyleri ile paylaşmak,
Şifreleri işten uzakta olduğunuz zamanlarda iş arkadaşlarınıza belirtmek.

a) Herhangi bir kimse şifre isteğinde bulunursa bu dokümanı referans göstererek Bilgi İşlem Birimi yetkilisini aramasını söyleyiniz.

b) Uygulamalarındaki "şifre hatırlama "özelliklerini seçmeyiniz. (Örnek; Outlook, İnternet Explorer, vs.)

c) Tekrar etmek gerekirse, şifreleri herhangi bir yere yazmayınız ve herhangi bir ortamda elektronik olarak saklamayınız.

ç) Şifreler en az 6 ayda bir değiştirilmelidir (Sistemlerin şifreleri ise en az 3 ayda bir değiştirilmelidir) Tavsiye edilen aralık ise 3 ayda birdir.

d) Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcı şifresini değiştirilmesi talep edilir.

C. Uygulama Geliştirme Standartları

Uygulama geliştiricileri programlarında aşağıdaki güvenlik özelliklerinin sağlandığından emin olmalıdırlar.

a) Bireylerin (grupların değil) kimlik doğrulaması (authentication) işlemini destekleyemeyebilir.

b) Şifreleri text veya kolay anlaşılabilir forumda saklanmamalıdır.

c) Kural yönetim sistemini desteklemelidir. (Örnek: Bir kullanıcı diğer bir kimsenin şifresini bilmeden de fonksiyonlarına devam edilmesi.)

D. Uzaktan Erişim Kullanıcılar Şifre Kullanımı

Kurumun bilgisayar ağına uzaktan erişim tek yönlü şifreleme algoritması veya güçlü bir "passphrase" ile yapılacaktır.

E. Uzun Şifre (Passphrase)

a) Bir passphrase standart şifrelerinden daha uzun karakter dizisine sahiptir (genellikle 4'ten 16'ya kadar karaktere sahiptir.) Dijital imzaların (bir mesajı gönderen kişinin gerçekten o kişi olduğunu kanıtlayan kodlanmış bir imza), mesajların kodlanması veya çözülmesinde kullanılır.

b) Passphrase şifreler gibi değildir passphrase şifrelerden daha uzundur, dolayısıyla saldırılara karşı daha güvenlidir.

c) Passphraseler tipik olarak birçok kelimeden ibarettir. Bundan dolayı passphrase "sözlük" saldırılara karşı daha güvenlidir

ç) Büyük ve küçük rakamlardan oluşan kombinasyona sahiptir. (örnek bir passphrase: "*?#>*1012incicaddekiTrafik*&#!#BuSabah")

d) Şifreleme için geçerli olan bütün kurallar passphraseler için daha gereklidir

3. ANTİ-VİRÜS POLİTİKASI

3.1 Amaç

Türk Dil Kurumu Başkanlığındaki bütün bilgisayarların virüs algılama ve engelleme standardına sahip olması için gereklilikleri belirlemektir.

3.2 Kapsam

Bu politika Başkanlığın PC-tabanlı bütün bilgisayarlarını kapsamaktadır. Bunlar masaüstü bilgisayarlar, file/ftp/tftp/proxy vs. sunuculardır.

3.3 Politika

Kurumun bütün PC tabanlı bilgisayarları anti-virüs yazılımına sahip olmalıdır ve belli aralıklarda düzenli olarak güncellenmelidir. Buna ek olarak anti-virüs yazılımı ve virüs tanımlamaları otomatik olarak güncellenmelidir. Virüs bulaşan makineler tam olarak temizleninceye kadar ağdan çıkarılmalıdır. Sistem yöneticileri anti-virüs yazılımının sürekli ve düzenli çalışması ve bilgisayarların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur. Zararlı programları (örnek, virüsler, solucanlar, truva atı, e-posta bombaları, vs.) kurum bünyesinde oluşturmak ve dağıtmak yasaktır. Hiçbir kullanıcı herhangi bir sebepten dolayı anti-virüs programını sisteminden kaldıramaz.

Türk Dil Kurumu Başkanlığının anti-virüs uygulaması işlemi, virüs problemlerinin ortadan kaldırılması için tavsiye edilen adımları açıklamaktadır.

Anti-Virüs uygulaması işlemi

Virüs problemlerine karşı tavsiye edilen adımlar:

a) Anti-virüs güncellemeleri bu iş için adanmış sunucular vasıtasıyla yapılacaktır. Sunucuların İnternet'e çevrimiçi bağlantısı olup otomatik olarak veritabanlarını güncelleyecektir. Ağa bağlı PC'ler otomatik olarak sunucudan en son sürümleri güncelleyeceklerdir. Ağa bağlı olmayan kullanıcılara ise gerekli scriptler 'le otomatik güncellenme sağlanacaktır.

b) Bilinmeyen kişilerden e-posta ile gelen dosya veya makroları kesinlikle açmayın. Bu ekli dosyaları hemen silin, daha sonra "silinmiş öğeler" den tekrar silin.

c) Spam, zincir ve diğer junk e-postalarını silin.

ç) Bilinmeyen veya şüpheli kaynaklardan asla dosya indirmeyin.

d) Kurumun ihtiyacı haricinde okuma/yazma hakkı ile direkt disk paylaşım hakkı vermekten kaçının.

e) Bilinmeyen kaynaklardan gelen USB flash diskleri, CD ve DVD'leri daima virüslere karşı tarama yapın.

f) ***Kritik veri ve sistem konfigürasyonlarını düzenli aralıklar ile yedekleyin ve güvenli bir yerde saklayın.***

4. İNTERNET ERİŞİM VE KULLANIM POLİTİKASI

4.1 Amaç

Türk Dil Kurumu Başkanlığının tüm birimlerinin güvenli İnternet erişimi için sahip olması gereken standartları belirlemektir. İnternetin uygun olmayan kullanımı, kurumun yasal yükümlülükleri, kapasite kullanımı ve kurumsal imajı açısından istenmeyen sonuçlara neden olabilir. Bilerek ya da bilmeden bu tür olumsuzluklara neden olunmaması ve İnternetin kurallarına, etiğe ve yasalara uygun kullanımının sağlanmasını amaçlamaktadır.

4.2 Kapsam

Bu politika Başkanlığının bütün birimlerinde bulunan bütün kullanıcılarını kapsamaktadır.

4.3 Politika

Bütün kullanıcılar ve bilgi işlem yöneticileri aşağıdaki İnternet erişim ve kullanım yönteminden dışarıya çıkmamalıdır.

a) Kurumun bilgisayar ağı erişim ve içerik denetimi yapan bir firewall üzerinden İnternete çıkacaktır. Ağ güvenlik duvarı (firewall), Kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve İnternet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır. Ağın dışından ağın içine erişim denetimi burada yapılır.

b) Kurumun ihtiyacı doğrultusunda içerik filtreleme sistemleri kullanılmalıdır. İstenilmeyen siteler (pornografik, oyun, kumar, şiddet içeren vs.) yasaklanabilmelidir.

c) Kurumun ihtiyacı doğrultusunda saldırı tespit ve önleme sistemleri kullanılmalıdır. (Intrusion Detection and Prevention Systems - IPS) Şüpheli olayları, nüfuz ve saldırıları tespit etmeyi hedefleyen bir sistemdir. IPS, şüpheli durumlarda e-posta veya SMS gibi yöntemlerle sistem yöneticisini uyarabilmektedir.

ç) İnternete giden veya gelen bütün trafik (smtp,pop3 ayrıca mümkünse http ve ftp vs.) virüslere karşı taranmalıdır.

d) Kurumlar İnternet erişimlerinde firewall, anti-virüs, içerik kontrol vs. güvenlik kriterlerini hayata geçirmelidirler.

e) Yetkilendirilmiş sistem yöneticileri İnternete çıkarken bütün servisleri kullanma hakkına sahiptir. Bunlar, www, ftp, telnet, ping, traceroute, vs.

f) Hiçbir kullanıcı peer-to-peer (eşler arası) bağlantı yoluyla İnternetteki servisleri kullanamayacaktır. (Örnek: Torrent, LimeWire, vb.)

g) Bilgisayarlar arası ağ üzerinden resmi görüşmeler haricinde, IM (Instant messaging) (mesajlaşma ve sohbet programları) chat programlarının kullanılmaması. Bu chat programları üzerinden dosya alışverişinde bulunulmamalıdır.

ğ) Hiçbir kullanıcı İnternet üzerinden akışkan multimedya (Multimedia Streaming) yapamayacaktır.

h) Çalışma saatleri içerisinde aşırı bir şekilde iş ile ilgili olmayan sitelerde gezinmek yasaktır.

ı) Bilgisayarlar üzerinden genel ahlak anlayışına aykırı İnternet sitelerine girilmemesi ve dosya indirimi yapılmamalıdır.

i) ***İş ile ilgili olmayan (resim, müzik, video dosyaları) yüksek hacimli dosyalar göndermek (upload) ve indirmek (download) etmek yasaktır.***

j) İnternet üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez ve kurum sistemleri üzerine bu yazılımlar kurulamaz. Kurumsal işlevlere yönelik yazılım ihtiyaçları için ilgili prosedürler dâhilinde ilgili bilgi işlem sorumlularına müracaat edilmesi gerekmektedir.

k) Üçüncü şahısların kurum İnternetini kullanmaları bilgi işlem sorumluların izni ve bu konudaki kurallar dâhilinde gerçekleştirilebilecektir.

5. SUNUCU GÜVENLİĞİ POLİTİKASI

5.1 Amaç

Bu politikanın amacı kurumun sahip olduğu sunucuların temel güvenlik konfigürasyonları için standartları belirlemektir. Bu politikanın etkili uygulanmasıyla başkanlık bünyesindeki bilgilere ve teknolojiye yetkisiz erişimler en aza indirilecektir.

5.2 Kapsam

Bu politika Kurumun sahip olduğu bütün dâhili sunucular için geçerlidir.

5.3 Politika

5.3.1 Sahip Olma ve Sorumluluklar

a) Kurumun bütün dahili sunucularının yönetiminden yetkilendirilmiş sistem yöneticileri sorumludur. Sunucular sadece bu kişiler tarafından yapılandırılacaktır.

b) Kurumun sahip olduğu bütün sunucular Kurumun yönetim sistemine kayıt olmalıdır ve en az aşağıdaki bilgileri içermektedir:

Sunucuların yeri ve sorumlu kişi,

Donanım ve işletim sistemi,

Ana görevi ve üzerinde çalışan uygulamalar,

İşletim Sistemi sürümleri ve yamalar.

c) Bütün bilgiler tek bir merkezde güncel olarak tutulmalıdır.

5.3.2 Genel Konfigürasyon Kuralları

a) İşletim sistemi konfigürasyonları Kurumun bilgi işlem biriminin talimatlarına göre yapılacaktır.

b) Kullanılmayan servisler ve uygulamalar kapatılmalıdır.

c) Servislere erişimler kayıt altına (log) alınacak ve erişim kontrol metotlarıyla koruma sağlanacaktır.

ç) Sunucu üzerinde çalışan işletim sistemlerinin, hizmet sunucu yazılımlarının ve antivirüs vb. koruma amaçlı yazılımların sürekli güncellenmesi sağlanmalıdır. Mümkünse, yama ve anti-virüs güncellemeleri otomatik olarak yazılımlar tarafından yapılmalı, ancak değişiklik yönetimi kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanmalıdır.

d) Sistem yöneticileri gerekli olmadığı durumlar dışında "Administrator" ve "root" gibi genel kullanıcı hesapları kullanmamalı, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmalıdır. Genel yönetici hesapları yeniden adlandırılmalıdır. Gerekli olduğunda önce kendi hesapları ile oturum açıp olup, daha sonra genel yönetici hesaplarına geçiş yapmalıdırlar.

e) Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSH veya SSL, IPSec, VPN gibi şifrelenmiş ağ) üzerinde yapılmalıdır.

f) Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdırlar.

5.3.3 Gözlemleme

a) Kritik sistemlerde oluşan bütün güvenlikle ilgili olaylar kayıt altına alınmalıdır ve aşağıdaki şekilde saklanmalıdır:

Bütün güvenlikle ilgili kayıtlara online olarak minimum 90 gün süreyle erişebilmelidir.

Günlük yedekler en az 1 ay saklanmalıdır.

Kayıtların haftalık yedeklemeleri en az 1 ay tutulmalıdır.

Aylık tam yedekler az 1 (bir) yıl tutulmalıdır.

b) Güvenlikle ilgili kayıtlar sorumlu kişi tarafından değerlendirilecek ve gerekli tedbirleri alacaktır. Güvenlik ile ilgili olaylar aşağıdaki gibi olabilir fakat bunlarla sınırlı değildir.

Port tarama atakları,

Yetkisiz kişilerin ayrıcalıklı hesaplara erişmeye çalışması,

Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar.

5.3.4 Uygunluk

a) Denetimler yetkili organizasyonlar tarafından Kurum bünyesinde belli aralıklarda yapılmalıdır.

b) Denetimler Bilgi İşlem tarafından yönetilecektir.

c) Denetimler Kurumun işleyişine zarar vermemesi için maksimum gayret gösterilecektir.

5.3.5 İşletim

a) Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir.

b) Sunucuların yazılım ve donanım bakımları üretici tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılmalıdır.

c) Sistem odalarına yetkisiz girişler engellenmelidir. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve bilgisayar sistemine kayıt edilmelidir.

6. VERİTABANI GÜVENLİK POLİTİKASI

6.1 Amaç

Kurumun veritabanı sistemlerinin kesintisiz ve güvenli şekilde işletilmesine yönelik standartları tanımlar. Kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kayıt altına. Kayıtlara idarenin izni olmadan kesinlikle hiçbir şekilde erişim yapılmamalıdır. Manyetik

kartuş, DVD, USB harici disk ortamlarında tutulan kayıtlar en az 5 (beş) yıl süre ile güvenli ortamlarda saklanmalıdır. Veritabanı sunucularının güvenliği hakkında daha detaylı bilgi ve uyulması gereken kurallar aşağıda belirtilmiştir.

6.2 Kapsam

Tüm veritabanı sistemleri bu politikaların kapsamı altında yer alır.

6.3 Politika

6.3.1.Veritabanı sistemleri envanteri ve bu envanterden sorumlu personel tanımlanmalı ve kayıt altına alınmalıdır.

6.3.2.Veritabanı işletim kuralları belirlenmeli ve kayıt altına alınmalıdır.

6.3.3.Veritabanı sistem kayıtları tutulmalı ve gerektiğinde idare tarafından izlenmelidir.

6.3.4.Veritabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli alınması kontrol altında tutulmalıdır.

6.3.5.Yedekleme planları kayıt altına alınmalıdır.

6.3.6.Veritabanı erişim politikaları "kimlik doğrulama ve yetkilendirme" politikaları çerçevesinde oluşturulmalıdır.

6.3.7.Hatadan arındırma, bilgileri yedekten geri döndürme kuralları "acil durum yönetimi" politikalarına uygun olarak oluşturulmalı ve kayıt altına alınmalıdır.

6.3.8.Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.

6.3.9.Veritabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmalarında yetkili bir personel bilgilendirilmelidir.

6.3.10.Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulmalı ve sonrasında ilgili uygulama kontrolleri gerçekleştirilmelidir.

6.3.11.Bilgi saklama medyaları Kurum dışına çıkartılmamalıdır.

6.3.12.Sistem dokümantasyonu güvenli bir şekilde saklanmalıdır.

6.3.13.İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için temas edilecek kişiler belirlenmelidir.

6.3.14.Veritabanı sunucusunda sadece SSH, RDP, SSL ve veritabanının orijinal yönetim yazılımına açık olmalı bunun dışında FTP, TELNET vb. gibi açık metin (clear text) şifreli bağlantılara kapalı olmalıdır. Ancak FTP, TELNET vb. clear text bağlantılar veritabanı sunucudan dışarıya yapılabilir.

6.3.15.Uygulama sunucularından veritabanına login vb. şekilde erişememelidir.

6.3.16.Veritabanı sunucularına erişim şifreleri kapalı bir zarfta imzalı olarak kurumun kasasında saklanmalı ve gereksiz yere açılmamalıdır. Zarfın açılması durumunda firma yetkilileri de bilgilendirilmelidir.

6.3.17.Arayüzden gelen kullanıcılar bir tabloda saklanmalı bu tablodaki kullanıcı adı ve şifreleri şifrelenmiş olmalıdır.

6.3.18.Veritabanı sunucusuna ancak zorunlu hallerde root veya admin olarak bağlanılmalı root veya admin şifresi tanımlanmış kişi/kişilerde olmalıdır.

6.3.19.Bağlanacak kişilerin kendi adına kullanıcı adı verilecek yetkilendirme yapılacaktır.

6.3.20. Bütün kullanıcıların yaptıkları işlemler kayıt altına alınmalıdır.

6.3.21.Veritabanı yöneticiliği yetkisi sadece bir kullanıcı da olmalıdır.

6.3.22.Veritabanında bulunan şemaların kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişmesi engellenmelidir.

6.3.23.Veritabanı sunucularına İnternet üzerinden erişimlerde vpn gibi güvenli bağlantılar tesis edilmelidir.

6.3.24.Veritabanı sunucularına ancak yetkili kullanıcılar erişebilmelidir.

6.3.25. Veritabanı sunucularına kod geliştiren kullanıcı dışında hiçbir kullanıcı bağlanıp sorgu yapamamalıdır. İstekler arayüzden sağlanmalıdır. (örnek: kullanıcılar tablolardan seçme yapamamalılar)

6.3.26. Veritabanı sunucularına giden veri trafiği mümkünse şifrelenmelidir. (Ağ trafiğini dinleyen casus yazılımların verilere ulaşamaması için)

6.3.27. Bütün şifreler düzenli aralıklarla değiştirilmelidir.

6.3.28. Veritabanı sunucuları için yukarıda bahsedilen ve uygulanabilen güvenlik kuralları uygulama sunucuları için geçerlidir.

7. BİLGİ SİSTEMLERİ YEDEKLEME POLİTİKASI

7.1 Amaç

Bilgi sistemlerinde oluşabilecek hatalar karşısında sistemlerin kesinti sürelerine ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigürasyon, sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmesi gerekir. Bu politika yedekleme kurallarına tanımlamaktadır

7.2 Kapsam

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

7.3 Politika

a) Bilgi sistemlerinde oluşabilecek hatalar karşısında, sistemlerin kesinti sürelerine ve olası bilgi kayıplarını en az düzeye indirmek için sistemler üzerindeki konfigürasyon, sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmesi gerekmektedir.

b) Verinin operasyonel ortamda online olarak aynı disk sisteminde farklı disk bölümlerinde ve offline olarak manyetik kartuş DVD ve CD ortamında yedekleri alınmalıdır.

c) Taşınabilir ortamlar (manyetik kartuş, DVD ve ya CD) fiziksel olarak bilgi işlem odalarından farklı odalarda veya binalarda güvenli bir şekilde saklanmalıdır, veriler offline ortamlarda en az 30 gün süreyle saklanmalıdır.

ç) Kurumsal kritik verilerin saklandığı sistemler ile sistem kesintilerin kritik olduğu sistemlerin bir varlık envanteri çıkarılmalı ve yedekleme ihtiyacı bakımından sınıflandırılarak kayıt altına alınmalıdır.

d) Düzenli yedeklemesi yapılacak varlık envanteri üzerinde hangi sistemlerde ne tür uygulamaların çalıştığı ve yedeği alınacak dizin, dosya, bilgi sistemlerinde değişiklik yapma yetkili personel ve yetki seviyeleri kayıt altına alınmalıdır.

e) Yedekleme konusu bilgi güvenliği süreçleri içinde çok önemli bir yer tutmaktadır bu konu ile ilgili sorumluluklar tamamlanmalı ve atamalar yapılmalıdır.

f) Yedeklerin alınacağı sistem, dosya ve veriler dikkatle belirlenmeli ve yedeği alınacak konu ile ilgili sorumluluklar tanımlanmalı ve atamalar yapılmalıdır.

g) Yedek ünite, gereksiz yer tutmamak üzere kritiklik düzeyi düşük olan veya sürekli büyüyen izleme dosyaları yedekleme listesine dâhil etmemelidir.

ğ) Yedeklenecek bilgiler değişik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilmeli ve güncellenmelidir.

h) Yeni sistem ve uygulamalar devreye alındığında yedekleme sistemleri güncellenmelidir.

ı) Yedekleme işlemi için gerekli sayı ve kapasiteye uygun yedek üniteler seçilmeli ve temin edilmelidir. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilmelidir.

i) Yedekleme ortamlarının düzenli periyotlarda test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanmalıdır.

j) Geri yükleme prosedürlerinin düzenli olarak ve test edilecek etkinlerinin doğrulanması ve operasyonel prosedürlerin ön gördüğü süreler dâhilinde tamamlanabileceğinden emin olunması gerekir.

k) Yedek ünitelerin saklandığı ortamların fiziksel uygunluğunun güvenliği sağlanmalıdır.

l) Yedekleme standartı ile doğru ve eksiksiz yedek kayıt kopyalarının bir felaket anında etkilenmeyecek bir ortamda bulundurulması gerekmektedir.

m) Veri yedekleme standartının, yedekleme sıklığı kapsamı, gün içinde ne zaman yapılacağı, ne koşullarda ve hangi aşamalarla yedeklerin yükleneceği ve yükleme sırasındaki sorunlardan nasıl geri dönüleceği, yedekleme ortamlarının ne şekilde işaretleneceği, yedekleme testlerinin ne şekilde yapılacağı ve bunun gibi konulara açıklık getirecek şekilde hazırlanması ve işlerliği periyodik olarak gözden geçirilmelidir.

n) Yedeklerin bir felaket anında kısa sürede devreye alınabilmesi için Kurum dışında bir yerde Felaket Kurtarma Merkezi (FKM)'nde tutulmalı ve bu veriler sürekli güncellenmelidir.

8. GÜVENLİK AÇIKLARINI TESPİT ETME POLİTİKASI

8.1 Amaç

Bu politikanın amacı kurumun bilgisayar ağının (PC, sunucu, firewall, ağ anahtarı vs.) güvenlik açıklarına karşı taranması hususunda politika belirlemektir.

Denetim sebepleri:

-Bilgi kaynaklarının bütünlüğünü ve gizliliğini sağlamak,

-Kurumun güvenlik politikalarına uyumunun kontrolü için güvenlik açıklarını tespit etmek,

-Gerektiği zaman kullanıcıların veya sistemin aktivitelerini kontrol etmek.

8.2 Kapsam

Bu politika başkanlığın bünyesinde sahip olunan bütün bilgisayar ve haberleşme cihazlarını kapsamaktadır. Bu politika kurumun bünyesinde bulunan fakat Kurumun sahip olmadığı herhangi bir sistemi de kapsamaktadır. Denetim yapan kişi veya kurum hizmetlerin durdurulması (Denial of Service) aktivitesi yapmayacaktır.

8.3 Politika

İstenildiğinde denetim yapan firmanın bireylerine erişim izni verilecektir. Bu anlaşmada Kurum denetim yapan firmaya kendi izni ile bilgisayar ağına erişim hakkı vermektedir. Kurumun birimleri denetim yapan firmaya ağ taraması yapması için protokol, adres bilgileri, ağ bağlantıları vs. hakkında bilgi verecektir. Bu istekler aşağıdaki bilgileri kapsamaktadır.

a) Bilgisayar veya haberleşme cihazlarına kullanıcı ve sistem seviyeli erişim bilgileri.

b) Kurumun bünyesinde üretilen, iletilen veya saklanan bilgilere (elektronik, hard copy vs.) erişim.

c) Çalışma alanlarına erişim (laboratuar, ofisler, sistem odaları, bilgi depolama alanları vs.).

ç) Başkanlık ağının trafiğini etkileşimli olarak gözlemleme ve trafiğin kayıt altına alınması isteği.

8.3.1 Tarama Esnasında Muhatap olan Kişi

Kurum denetimi yapan firmaya oluşabilecek sorunlar hakkında danışabileceği bir kişiyi yazılı olarak verecektir.

8.3.2 Tarama Periyodu

Kurum ve denetimi yapan firma denetim yapılacak zamanı yazılı olarak bildireceklerdir.

8.3.3 Gizlilik Anlaşması

Kurum ile güvenlik taraması yapacak firma, tarama sonucunda elde edilecek bilgilerin hiçbir şekilde üçüncü şahıslara aktarmayacağına dair gizlilik anlaşması yapacaktır.

9. AĞ CİHAZLARI GÜVENLİK POLİTİKASI

9.1. Amaç

Bu doküman Kurumun ağındaki yönlendirici (router) ve anahtarların (switch) sahip olması gereken minimum güvenlik konfigürasyonlarını tanımlamaktadır.

9.2 Kapsam

Kurumun ağına bağlı olan ağ cihazları için geçerlidir.

9.3 Politika

Bütün yönlendirici ve anahtarlar aşağıdaki konfigürasyon standartlarında sahip olmalıdır:

a) Bilgisayar ağında bulunan tüm cihazların IP ve MAC adres bilgileri envanter dosyasında Yer alacaktır.

b) Mümkün olduğunca yerel kullanıcı hesapları açılmamalıdır. Yönlendirici ve anahtarlar kimlik tanımlama için RADIUS veya TACAS+ protokolünü kullanmalıdır.

c) Yönlendirici ve anahtarlardaki “enable” şifresi kodlanmış formda saklanmalıdır. “enable” şifre tanımlamaları kurumun içerisinden yapılmalıdır.

ç) Aşağıdakilere izin vermeyiniz:

-IP yönlendirmeli yayın,

-RFC 1918 ve RFC 4193 (Özel ağlardaki IP düzenlemesi standartları)’de tanımlandığı şekilde yönlendirici giriş portuna gelen geçersiz IP adresleri,

-Kaynak yönlendirme,

-Yönlendiricide çalışan web siteleri,

d) Kurumun standart olan SNMP topluluk dizisini (community string) kullanmalıdır.

e) İhtiyaç duyulduğu zaman erişim listeleri eklenmelidir.

f) Yönlendirici ve anahtarlar kurumun yönetim sisteminde olmalıdır. h) Yazılım ve firmware güncellemeleri önce test ortamlarında denendikten sonra çalışma günlerinin dışında üretim ortamına taşınacaktır.

g) Cihazlar üzerinde kullanılmayan servisler kapatılacaktır. (Telnet, HTTP vb.)

ğ) Bilgisayar ağında bulunan kabinetler, aktif cihazlar, UTP ve fiber optik aktarma kabloları ile cihazların portları etiketlenecektir.

h) Her bir yönlendirici ve anahtar aşağıdaki uyarı yazısı ile yönlendiriciye erişen yasal veya yasadışı kullanıcıları uyarmalıdır. "BU CİHAZA YETKİSİZ ERİŞİMLER YASAKLANMIŞTIR" Bu cihaza erişim ve konfigürasyon için yasak hakkınız olmak zorundadır. Bu cihazla yapılan her şey kayıt altına alınabilir, bu politikaya uymamak disiplin kuruluna sevk ile sonuçlanabilir veya yasal yaptırım olabilir"

10. AĞ YÖNETİMİ POLİTİKASI

10.1 Amaç

Kurumun bilgisayar ağında yer alan bilgilerin ağ altyapısının güvenliği, gizlilik, bütünlük ve erişebilinirlik kavramları göz önüne alınarak sağlanmalıdır. Uzaktan erişim hususunda özel önem gösterilmelidir. Yetkisiz erişimle ilgili tedbirler alınmalıdır. Ağın güvenliği ve sürekliliğini sağlamak amacıyla bir takım kontroller gerçekleştirilmelidir. Ağ Yönetimi Politikası bu gereksinimleri karşılayan kuralları belirlemek kuralları belirlemek amacıyla geliştirilmiştir.

10.2 Kapsam

Türk Dil Kurumu Başkanlığının bilgisayar ağının sistem ve ağ yöneticileri, teknik sorumluları ve Bilgi işlem elemanları faaliyetlerini Ağ Yönetim Politikasına uygun şekilde yürütmekle yükümlüdür.

10.3 Politika

10.3.1 Ağın kontrol edeceği alan belirlenmelidir.

10.3.2 Bilgisayar ağları işletme sorumlulukları, bilgisayarların işletilmesinden ayrılmalıdır.

10.3.3 Gerek duyuluyorsa kamu şebekeleri üzerinden geçen verinin gizliliği ve doğruluğunu garanti etmek ve kendisine bağlı bilgisayar sistemlerini korumak için özel kontroller uygulanmalıdır.

10.3.4 Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliği sağlamak için özel kontroller uygulanmalıdır.

10.3.5 Ağ servisleriyle ilgili standartlarda, erişimine izin verilen ağlar ve ağ servisleri ve ilgili yetkilendirme yöntemleri belirtilmelidir.

10.3.6 Ağ üzerinde kullanıcının erişeceği servisler kısıtlanmalıdır.

10.3.7 Gerek görülen uygulamalar için, portların belirli uygulama servislerine veya güvenli ağ geçitlerine otomatik olarak bağlanması sağlanmalıdır.

10.3.8 Sınırsız ağ dolaşımı engellenmelidir.

10.3.9 Harici ağlar üzerinde kullanıcıları belirli uygulama servislerine veya güvenli ağ geçitlerine bağlanma zorlayıcı teknik önlemler alınmalıdır.

10.3.10 İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden teknik önlemler alınmalıdır. (Örnek: Güvenlik duvarı - firewall)

10.3.11 Ağ erişimi VPN, VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılmalıdır.

10.3.12 Uzaktan teşhis ve müdahale için kullanılacak portların güvenliği sağlanmalıdır.

10.3.13 Farklı alt ağlar tanımlanmalıdır.

10.3.14 Ağ bağlantıları periyodik olarak kontrol edilmelidir.

10.3.15 Gerek görülen uygulamalar için elektronik posta, tek yönlü dosya transferi, çift yönlü dosya transferi, etkileşimi erişim, günü ve günün saatine bağlı erişim gibi uygulama kısıtlamalarıyla ağ erişimi denetlimi yapılmalıdır.

10.3.16 Ağ üzerindeki yönlendirme kontrol edilmelidir.

10.3.17 Bilgisayar ağına bağlı bütün makinelerde kurulum ve konfigürasyon parametreleri Kurumun güvenlik politika ve standartlarıyla uyumlu olmalıdır.

10.3.18 Sistem tasarım ve geliştirmesi yapılırken onaylanmış olan ağ ara yüzü ve protokolleri kullanmalıdır.

10.3.19 İnternet trafiği Erişim ve Kullanımı İzleme Politikası ve ilgili standartlarda anlatıldığı şekilde izlenilebilecektir.

10.3.20 Bilgisayar ağındaki adresler, ağa ait konfigürasyon ve diğer tasarım bilgileri 3. Şahıs ve sistemlerin ulaşamayacağı bir şekilde saklanmalıdır.

10.3.21 Ağ üzerindeki güvenlik duvarları üzerinde, ilgili konfigürasyon dokümanlarında belirtilen servisler dışında tüm servisler kapatılmalıdır.

10.3.22 Güvenlik duvarı olarak kullanılan cihazlar başka amaç için kullanmamalıdır.

10.3.23 Güvenlik duvarı konfigürasyonu kesinlikle Bilgi Güvenliği Yöneticisinden yazılı izin alınmadan değiştirilmemeli, servisler açılmamalıdır.

11. UZAKTAN ERİŞİM POLİTİKASI

11.1 Amaç

Bu politikanın herhangi bir yerden Kurumun bilgisayar ağına erişilmesine ilişkin standartları saptamaktır. Bu standartlar kaynaklarının yetkisiz kullanımından dolayı Kuruma gelebilecek potansiyel zararları en aza indirmek için tasarlanmıştır. Bu zararlar şunlardır; Başkanlığın gizli ve hassas bilgilerin kaybı, beyin gücü kaybı, prestij kaybı ve içerideki kritik sistemlere meydana gelen zararlar vs.

11.2 Kapsam

Bu politika Kurumun bütün çalışanlarını, sözleşmelileri, IT hizmeti veren firmaları veya Kurum adına çalışanları ve kısaca Kurumun herhangi bir birimindeki bilgisayar ağına erişen bütün kişi ve kurumları kapsamaktadır. Bu politika, Kuruma bağlı bütün uzak erişim bağlantılarını kapsamaktadır ve bunun içerisine e-posta okuma veya gönderme ve intranet web kaynaklarını gözlemleme dahildir. Bütün uzaktan erişim uygulamaları bu politika tarafından kapsanmaktadır, aynı zamanda, sadece dial-up modemler, frame relay, ISDN, LL, xDSL, Metro Ethernet, SSL ve kablo modem vs. bağlantılarıyla sınırlı değildir.

11.3 Politika

11.3.1 Genel

a) Uzaktan erişim için yetkilendirilmiş Kurum çalışanları veya Kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir.

b) Uzaktan erişim metotları ile Kuruma bağlantılarda bilgi sistemlerinin güvenliğinin sağlanması için aşağıdaki politikalara göz atmak gerekmektedir.

- Kabul edilebilir Şifreleme Politikası
- Sanal Özel Ağ (VPN) Politikası
- Kablosuz haberleşme Politikası
- Kabul Edilebilir kullanım Politikası

11.3.2 Gereklilikler

a) İnternet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişi veya kurumlar VPN teknolojisini kullanacaklardır. Bu, veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlayacaktır. VPN teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vs. Protokollerinden birini içermelidir.

b) Mümkünse uzaktan erişim güvenliği sıkı bir şekilde denetlenmelidir. Kontrol tek yönlü şifreleme (one-time password authentication, örnek: token device) veya güçlü bir passphrase (uzun şifre) destekli public/private key sistemi kullanılması tavsiye edilmektedir. Daha fazla bilgi için Şifreleme Politikasına bakılabilir.

c) Kurum çalışanları hiçbir şekilde kendilerinin sisteme giriş ve e-posta şifrelerini aile bireyleri dahil olmak üzere hiç kimseye veremezler.

ç) Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşmeli sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmadıklarından emin olmalıdırlar. Kullanıcının tamamıyla kontrolünde olan ağlarda bu kural geçerli değildir.

d) ***Çalışanlar Kurum ile ilgili yazışmalarında Kurumun dışındaki e-posta hesaplarını (örnek: hotmail, gmail, mynet vs.) kullanamazlar.***

e) ISDN veya telefon hatları ile uzaktan erişen yönlendiriciler minimum olarak CHAP kimlik doğrulama protokolünü kullanmalıdırlar.

f) Uzaktan erişim yöntemi ile Kuruma erişen bütün bilgisayarlar en son güncellenmiş antivirüs yazılımına sahip olmalıdırlar.

g) Kurum ağına standart dışı erişim isteğinde bulunan organizasyon veya kişilere, Bilgi İşlem biriminin özel izni ile geçici olarak izin verilebilir.

ğ) Periyodik olarak yapılan kontrollerle Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcı kimlikleri ve hesapları kaldırılmalıdır.

12. SANAL ÖZEL AĞ (Virtual Private Network) POLİTİKASI

12.1 Amaç

Bu politikanın amacı VPN protokolünün kullanımı hakkında standartlarını belirlemektir.

12.2 Kapsam

Bu politika VPN ile Türk Dil Kurumu Başkanlığı bilgisayar ağına bağlanacak kurumları ve kişileri kapsamaktadır. Bu politika VPN danışmanları, geçici çalışanları ve diğer bütün personeli kapsamaktadır. Bu politika VPN bağlantılarının sonlandırıldığı ürünlere uygulanacaktır.

12.3 Politika

Başkanlığın yetkili çalışanları ve üçüncü şahıslar (programcılar, firmalar vs) VPN'den yararlanabilirler. Kullanıcılar herhangi bir internet servis sağlayıcısına seçmekle serbesttirler. Daha fazla detaylar "Uzaktan Erişim Politikası" nda mevcuttur. Buna ek olarak,

a) VPN kullanım hakkı verilen kişiler, yetkisiz kişilerin bu hakkı kullanamaması için gerekli tedbirleri almakla sorumludur.

b) VPN konfigürasyonu mümkünse tek yönlü şifreleme (one time passoword authentication) sistemi ile yapılmalıdır.

c) Kurum ağına bağlanıldığında, PC'den çıkan ve giren trafik sadece VPN kanalından iletilecektir ve diğer bütün trafik düşecektir.

ç) Çift tünel (split tunnel- aynı anda iki VPN bağlantısı) sistemine izin verilmemektedir, sadece bir ağ bağlantısına izin verilmektedir.

d) Kurumun VPN ağ geçitlerinin kurulması ve yönetimi yetkili kişiler tarafından (Bilgi İşlem personeli) yapılacaktır.

e) Başkanlığın ağına VPN veya başka bir yöntemle bağlanan bilgisayarlar en son güncellenmiş kurulumun standardı olan anti-virüs yazılımını kullanmak zorundadırlar.

f) VPN kullanıcıları hat kullanılmadığı takdirde kurumun ağından 5 dakika sonra otomatik olarak bağlantıları kesilecektir. Kullanıcı tekrar bağlanmak için giriş yapmak zorundadır. Ping veya diğer prosesler network bağlantısını açık tutmak için kullanılmamalıdır.

g) VPN cihazına bağlantı süresi 24 saat ile sınırlıdır.

ğ) Kuruma ait olmayan bilgisayarlara sahip kişiler Başkanlığın VPN ve ağ politikalarına uygun bir şekilde cihazlarını konfigüre etmelidirler.

h) Sadece Kurumun onay verdiği kullanıcılar VPN 'i kullanabilirler.

ı) VPN teknolojisini kendi kişisel cihazları ile kullanan kişiler şunu bilmelidirler ki, bütün makineler Kurum ağının bir parçasıdır, bundan dolayı Başkanlığın sorumlu olduğu cihazlar ile aynı kurallara sahiptir ve aynı güvenlik politikaları ile konfigüre edilmelidir.

13 RİSK DEĞERLENDİRME POLİTİKASI

13.1 Amaç

Kurumun bilgisayar ağında sistem açıklarını tespit etmek ve gerekli tedbirlerin alınmasını sağlamak amacıyla firmalara risk analizi yaptırılmasına dair kuralları belirlemektir.

13.2 Kapsam

Risk analizi Kurum içerisinde veya Kurum dışındaki herhangi bir cihaz üzerinden yapılabilir. Risk analizi, uygulama programlar, sunucuları, ağ veya yönetim sistemleri yapılabilir.

13.3 Politika

a) Sistemi mükemmelleştirmeyi amaçlayan bu politikanın çalıştırılması, geliştirilmesi ve uygulaması Kurum ve ilgili firmanın sorumluluğundadır. Risk analizi süresince çalışanlar gerekli noktalarda yardımcı olacaktır. Çalışanlar daha sonra Risk Değerlendirme takımı ile birlikte geliştirme ve iyileştirme prosesine katkıda bulunacaklardır.

b) Risk değerlendirme raporları Kuruma elden teslim edilecek ve rapor, söz konusu risk ve hassasiyetler giderilene dek Bilgi İşlem Biriminde çevresel ve fiziksel güvenlik önlemleri alınmış bir ortamda saklanacaktır.

c) Risk değerlendirme çalışmalarına başlamadan önce çalışma kapsamına konu, sistemler ve çalışma süreleri Başkanlığa bildirilecek ve bu çalışmalar Başkanlık tarafından izlenecektir. Risk

değerlendirme çalışmaları esnasında sistemler üzerinde servis reddi veya herhangi bir sebeple iş sürekliliği aksatılmayacaktır.

14. KABLOSUZ İLETİŞİM POLİTİKASI

14.1 Amaç

Bu politika cihazların gerekli güvenlik tedbirleri alınmaksızın Kurumun bilgisayar ağına erişimini engellemeyi amaçlamaktadır. Sadece bu politikanın güvenlik kriterlerine uyan cihazlar kurumun bünyesinde kullanabilirler.

14.2 Kapsam

Bu politika Kurum bünyesinde kullanılabilecek bütün kablosuz haberleşme cihazlarını (PC, Cep telefonları, PDA vs.) kapsamaktadır. Kablosuz veri transferi sağlayabilen herhangi bir cihaz bunun kapsamındadır. Kuruma bağlantısı olmayan herhangi bir cihaz veya bilgisayar ağı bu politikanın kapsamı içerisinde değildir.

14.3 Politika

14.3.1 Erişim Cihazları (Access Point) ve kartların kayıt olunması Kurumun bilgisayar ağına bağlanan bütün erişim cihazları ve ağ arabirim kartları (örnek, PC card) Bilgi işlem birimi tarafından kayıt altına alınması gerekmektedir. Erişim cihazları periyodik olarak güvenlik testinden geçirilmelidir. Ancak Mac adresleri kayıtlı olan cihazlar Kurumun bilgisayar ağına erişebilmelidir.

14.3.2 Bütün kablosuz erişim cihazları Bilgi işlem güvenlik birimi tarafından onaylanmış olmalıdır ve Bilgi İşlemin belirlediği güvenlik ayarlarını kullanmalıdır.

14.3.3 Güvenlik Ayarları

a) Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmalıdır. Bunun için Wi-Fi Protected Access (WPA) şifreleme kullanılmalıdır. IEEE 802.1x erişim kontrol protokolü ve TACACS+ ve RADIUS gibi güçlü kullanıcı kimlik doğrulama protokolleri kullanılabilmelidir.

b) Erişim cihazlarında ki firmware'leri düzenli olarak güncellenmelidir. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlanır.

c) Erişim cihazları kolayca erişilebilir bir yerde olmaması gereklidir. Çünkü, cihaz resetlendiğinde fabrika ayarlarına geri dönebilmekte ve güvenlik açığı oluşturabilmektedir.

ç) Cihaza erişim için güçlü bir şifre kullanılmalıdır. Erişim şifreleri varsayılan ayarda bırakılmamalıdır.

d) SSID numaraları yayınlanmamalıdır. Böylece sniffer tarzı cihazların otomatik olarak bu numaraları çözmesi engellenecektir.

e) Varsayılan SSID isimlerini kullanmalıyız. SSID ayarı bilgisi içerisinde kurumla ilgili bilgi olmamalıdır, mesela Kurum ismi, ilgili bölüm, çalışanların ismi vs.

f) Radyo dalgalarının binanın dışına taşmamasına özen gösterilmelidir. Bunun için bidirectional antenler kullanılarak radyo sinyallerinin çalışma alanında yoğunlaşması sağlanmalıdır.

g) Erişim Cihazları üzerinde gelen kullanıcılar güvenlik duvarı üzerinden ağa dahil olmalıdırlar.

ğ) Kullanıcı bilgisayarlarında kişisel güvenlik yazılımları yüklü olmalıdır.

h) Kritik yerlerde kullanıcılar VPN teknolojilerini kullanarak kurum ağına erişmelidirler.

ı) Hem kullanıcılar hem de erişim cihazları statik ip adresleri kullanmalıdır. Aynı zamanda donanım adresleme (örnek: mac adresleme) kullanılmalıdır.

i) Erişim cihazları bir yönetim yazılımı ile devamlı olarak gözlemlenmelidir. Sistemde hackerlar tarafından konulmuş casus bir erişim cihazı olabilir veya mevcut erişim cihazı resetlenmiş olup Kurumun güvenlik politikalarına aykırı bir şekilde ayar yapılmış olabilir.

15. BİLGİ SİSTEMLERİNİN GENEL KULLANIM POLİTİKASI

15.1. Genel Bakış

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 eylemlere karşı çalışanların ve Kurumun haklarını korumakla yükümlüdür. Bilişimle alakalı sistemler (bilgisayar, yazılım, işletim sistemleri, kayıt cihazları, e-mail, vs.) Kurumun sahip olduğu değerlerdir. Bu sistemler sadece kamuya hizmet için kullanılmalıdır. Güçlü bir güvenlik, bütün çalışanların dahil olduğu takım çalışmasıyla oluşturulabilir. Bütün bilgisayar kullanıcıları günlük

aktivitelerini yerine getirebilmesi için bu kuralları iyi bilmeli ve uygulamanın sorumluluğunu taşımalıdır.

15.2 Amaç

Bu politikanın amacı Kurum bünyesindeki bilişim cihazlarının uygun kullanımı hakkında taslak oluşturmaktır. Uygunsuz kullanım Kurumu virüs saldırılarına, ağ sistemlerinin çökmesine, hizmetlerin aksamasına sebep olabilir ve bunlar yasal yaptırımlara dönüşebilir.

15.3 Kapsam

Bu politika Kurumun bütün çalışanları, sözleşmelileri ve Kurum adı altında çalışan bütün kişiler için geçerlidir. Aynı zamanda Kurumun sahip olduğu ve kiraladığı bütün cihazlar içinde geçerlidir.

15.4 Politika

15.4.1 Genel Kullanım ve Sahip Olma

a) Kullanıcılar şunun farkında olmalıdırlar; kurumun güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da Kurumun bünyesinde oluşturulan tüm veriler Kurumun mülkiyetindedir.

b) Çalışanlar bilgi sistemlerini kendi kişisel kullanımı için makul seviyede kullanabilirler. Her bir birim kendi sistemlerinin kişisel kullanımı için gerekli kuralları koymalıdır. Birimler böyle kural koymamış ise Kurumun koyduğu güvenlik politikaları geçerlidir.

c) Kullanıcı herhangi bir bilginin çok kritik olduğunu düşünüyorsa o bilgi şifrelenmelidir.

ç) Güvenlik ve ağın bakımı amacıyla yetkili kişiler cihazları, sistemleri ve ağ trafiğini "Denetim Politikası" çerçevesinde gözlemleyebilir.

d) Kurum, bu politika çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir

e) Yirmi beş kullanıcıdan daha büyük ağlarda domain oluşturmalıdır. Bu durumda bütün bilgisayar mutlaka domaine login olmalıdır. Domain'e bağlı olmayan bilgisayarların yerel ağdan çıkartılmaları, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alış verişi yapılmamalıdır.

f) Bilgisayarlarda oyun ve eğlence amaçlı programların çalıştırmamalı / kopyalanmamalıdır.

g) Bilgisayarlar üzerinden resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunmamalıdır.

ğ) Kurumda bilgi işlem biriminin bilgisi olmadan başkanlık ağ sisteminde (web hosting servisi, e-posta servisi vb.) sunucu nitelikli bilgisayar bulundurulmamalıdır.

h) Birimlerde sorumlu bilgi işlem personeli ve ilgili teknik personel bilgisi dışında bilgisayarlar üzerinde ağ ayarları, kullanıcı tanımları, kaynak profilleri vb. üzerinde mevcut yapılan düzenlemelerin hiçbir surette değiştirilmemelidir.

ı) Bilgisayara herhangi bir şekilde lisanssız program yüklenmemelidir.

i) Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.

15.4.2 Güvenlik ve Kişiye Ait Bilgiler

a) Bilgi sistemlerinde bulunan kritik bilgilere yetkisiz kişilerin erişimini engellemek için gerekli erişim hakları tanımlanmalıdır.

b) Şifreleri güvenli bir şekilde tutun ve hesabınızı başka kimselerle paylaşmayın. Sistem seviyeli şifreler üç ayda bir kullanıcı seviyeli şifreler ise en az altı ayda bir değiştirilmelidir.

c) Bütün PC ve dizüstü bilgisayarlar otomatik olarak 10 dakika içerisinde şifreli ekran korumasına geçebilmelidir.

ç) Dizüstü bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. Bios ve işletim sistemi şifreleri aktif hale getirilmelidir. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmalıdır.

d) Dizüstü bilgisayarların çalınması/ kaybolması durumunda, durum fark edildiğinde en kısa zamanda Bilgi işlem birimine de haber verilmelidir.

e) Bütün cep telefonu ve PDA (Personal Dijital Assistant) cihazları kurumun ağı ile senkronize olsun veya olmasın şifreleri aktif halde olmalıdır. Kullanılmadığı durumlarda kablosuz erişim (Kızılötesi, Blutetooth, vs.) özellikleri aktif halde olmamalıdır ve mümkünse anti virüs programları ile yeni nesil virüslere karşı korunmalıdır.

f) Çalışanlar tarafından haber gruplarına gönderilen maillerde şöyle bir açıklama olmalıdır: "Bu e-posta işi için gönderilenler hariç sadece yukarıda isimleri belirtilen kişiler arasında özel

haberleşme amacını taşımaktadır. Size yanlışlıkla ulaşmışsa lütfen gönderen kişiyi bilgilendiriniz ve mesajı sisteminizden siliniz. Türk Dil Kurumu Başkanlığı bu mesajın içeriği ile ilgili olarak hiçbir hukuksal sorumluluğu kabul etmez.

g) Türk Dil Kurumu Başkanlığı ağına bağlı bütün bilgisayarlar düzenli olarak güncel antivirüs yazılımı ile taranmalıdır.

ğ) Çalışanlar bilinmeyen kimselerden gelen dosyaları açarken çok dikkatli olmalıdırlar. Çünkü bu dosyalar virüs ve truva atı gibi zararlı kodları içerebilirler.

h) Bütün kullanıcılar ağın kaynaklarının verimli kullanımı konusunda dikkatli olmalıdırlar. E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olun ve gerekirse dosyaları sıkıştırın.

ı) Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek kuruma veya kişiye yönelik saldırılardan (örnek, elektronik bankacılık vs.) sistemin sahibi sorumludur.

15.4.3 Uygunsuz kullanım

Genel olarak aşağıdaki eylemler yasaklanmıştır. Sistem yöneticileri bu kapsamın dışında olabilir (örnek: Sistem yöneticisi sisteme zarar vermeye çalışan bir makinenin ağ bağlantısını kesebilir).

Herhangi bir kullanıcı Kurumun kaynaklarını kullanarak hiçbir şart altında herhangi bir yasadışı bir işlemde bulunamaz.

A-Sistem ve Ağ İşlemleri

Aşağıdaki işlemler hiçbir istisna olmadan kesinlikle yasaklanmıştır;

a) Herhangi bir kişi veya kurumun ticari sır, patent veya diğer şirket bilgileri, yazılım lisansları vs. haklarını çiğnemek,

b) Kitapların izinsiz kopyalanması, magazinlerdeki fotoğrafların dijital formata dönüştürülmesi, lisans gerektiren yazılımların kopyalanması,

c) Zararlı programların (örnek: virüs, solucan, truva atı vs.) ağa veya sunuculara bulaştırılması,

ç) Kendi hesabınızın şifresini başkalarına vermek veya kendi hesabınızı kullandırmak. (Bu, evden çalışırken aile bireylerini de kapsar.)

d) Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışmak,

e) Ağ güvenliğini etkilemek (örnek, bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ haberleşmesini bozmak. (paket sniffing, paket spoofing, denial of service vs.)

f) Port veya ağ taraması,

g) Kullanıcı kimlik tanıma yöntemlerinden kaçmak,

ğ) Program/script/ komut kullanarak kullanıcının bağlantısını etkilemek,

h) Kurum bilgilerini kurum dışında üçüncü şahıslara iletmek,

ı) Kullanıcıların kişisel bilgisayarları üzerine bilgi işlem biriminin onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapması,

i) Cihaz, yazılım ve verinin izinsiz olarak Kurum dışında çıkarılması,

j) Kurumun politikaları olarak belirlediği programlar dışında kaynağı belirsiz olan programları (Dergi Cd 'leri veya İnternetten indirilen programlar vs.) kurmak ve kullanmak yasaktır.

B-E-Posta ve Haberleşme İşlemleri

a) Kurum dışında web posta sistemini güvenliğinden emin olunmayan bir bilgisayardan kullanmak,

b) İstenilmeyen e-posta mesajlarının iletilmesi. Bunlar karşı tarafın özellikle istemediği reklam mesajlarını içeren mailler (spam mail) olabilir,

c) E-posta veya telefon vasıtası ile taciz etmek,

ç) E-posta başlık bilgilerini yetkisiz kullanmak veya değiştirmek,

d) Zincir e-postları oluşturmak veya iletmek,

e) İş ile alakalı olmayan mesajları haber gruplarına iletmek.

16. DONANIM VE YAZILIM ENVANTERİ OLUŞTURULMA POLİTİKASI

16.1 Amaç

Bu politika Kurumun sahip olduğu donanım ve yazılımların envanterinin oluşturulması ile ilgili kuralları belirlemektir.

16.2 Kapsam

Bu politika Kurum bünyesinde kullanılan bütün donanım ve yazılımları (PC, sunucu, yazıcı, işletim sistemleri vs.) kapsamaktadır. Bu politikanın uygulanmasından bilgi işlem sorumluları ve ilgili birim yöneticileri sorumludur.

16.3 Politika

Bütün cihazların doğru donanım ve yazılım envanteri oluşturulmalı ve güncel tutulmalıdır.

a) Oluşturulan envanter tablosunda şu bilgiler olmalıdır; sıra no, bilgisayar adı, bölüm, marka, model, seri no, özellikler, ek aksamlar, işletim sistemi vs.

b) Bu tablolar belirli periyotlarda güncellenecektir. Girişler isim ve şifre kontrolü ile olacaktır.

c) Bilgi güncelleme denetimi bilgi işlem birimi tarafından yapılacaktır.

ç) Envanter bilgisi doğru bir şekilde tutulmalıdır. Eksik veya yanlış envanter bilgisi ileride yapılacak donanım ve yazılım değişikliklerinde doğru karar alınmasını engelleyebilir.

d) Envanter bilgileri sık sık kontrol edilmelidir. Envanter bilgisi eksikliğinden dolayı oluşacak hırsızlık veya değişim ciddi kayıplara yol açabilir.

17. KRİZ / ACİL DURUM YÖNETİMİ POLİTİKASI

17.1 Amaç

Bu politika Kurum çalışanlarının, bilgi güvenliği ve iş sürekliliği ile ilgili acil bir durum oluştuğunda sorumlulukları dahilinde gerekli müdahale yapabilmelerine yönelik standartları belirlemektedir. İzlenen olayın uygun şekilde raporlanması ve belirlenen önlem ve acil durum faaliyetlerinin uygulanması önemlidir. Kurum çalışanlarının, bilgi güvenliği veya iş sürekliliği ile ilgili acil bir durum oluştuğunda sorumlulukları dahilinde gerekli müdahaleyi yapabilmelerine yönelik normlar aşağıda belirtilmiştir.

17.2 Kapsam

Acil durum senaryoları yaşanmadan önce uygun acil durum hareket planının yapılması esastır. Bilgi güvenliğine yönelik tehlike senaryolarından bazıları sistemlere yapılacak direkt saldırılar, zararlı kod içeren programların, kişilerin sisteme sızması, bilginin hırsızlığı, dışarıdan veya içten gerçekleştirebilecek saldırı öncesi taramalar olarak tanımlanabilir.

17.3 Politika

a) Acil durum sorumluları atanmalı ve yetki ve sorumlulukları belirlenmeli ve kayıt edilmelidir.

b) Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınmalıdır. Örneğin, uygulama veya veri tabanı sunucularında donanım ve yazılıma ait problemler oluştuğunda, yerel veya uzak sistemden (FKM) yeniden kesintisiz (veya makul kesinti süresi içerisinde) çalışma sağlanabilmelidir.

c) Kurum bilişim sistemlerinin kesintisiz çalışmasını sağlaması için aynı ortamda kümeleme (cluster) veya uzaktan kopyalama (remote replication) veya yerel kopyalama (local replication) veya pasif sistem çözümlerini hayata geçirebilir. Kurum sistemlerini tasarlarken ne kadar süre iş kaybını tolere edeceklerini göz önüne almalıdır.

ç) Acil durumlarda Kurum içi işbirliği gereksinimleri tanımlanmalıdır.

d) Acil durumlarda sistem kayıtları incelenmek üzere saklanmalıdır.

e) Güvenlik açıkları ve ihlallerini rapor edilmesi için kurumsal bir mekanizma oluşturulmalıdır.

f) Yaşanan acil durumlar sonrası politikalar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilmelidir.

g) Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulmalı ve bu bildirim süreçleri tanımlanmış olmalıdır.

ğ) Acil durum kapsamında değerlendirilen olaylar aşağıda farklı seviyelerde tanımlanmıştır:

Seviye A: Bilgi kaybı. Kurumsal değerli bilgilerin yetkisiz kişilerin eline geçmesi,·bozulması, silinmesi.

Seviye B: Servis kesintisi. Kurumsal servislerin kesintisi veya kesintisine yol· açabilecek durumlar.

Seviye C: Şüpheli durumlar. Yukarıda tanımlı ilk iki seviyedeki duruma sebebiyet· verebileceğinden şüphe duyulan ancak gerçekliği ispatlanmamış durumlar.

h) Her bir seviyede tanımlı acil durumlarda karşılaşabilecek riskler, bu riskin Kuruma getireceği kayıplar ve bu riskler oluşmadan önce ve oluştuktan sonra hareket planları tanımlanmalı ve kayıt edilmelidir.

ı) Acil durumlarda bilgi güvenliği yöneticisine erişilmeli, ulaşılamadığı durumlarda koordinasyonu sağlamak üzere önceden tanımlanmış ilgili yöneticiye bilgi verilmeli ve zararın tespit edilerek süratle daha önceden tanımlanmış felaket kurtarma faaliyetleri yürütülmelidir.

i) Bilgi güvenliği yöneticisi tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmek üzere ilgili makamlara iletilmelidir.

j) Olayın türü ve boyutuna göre emniyet veya diğer kurumlara başvurmak gerekebilir. Bu özel olaylar (hırsızlık vb.), başvurulacak kurumlar başvuru şekli (telefon, dilekçe vb.), başvuruyu yapacak Kurum yetkilisi önceden belirlenmiş ve kayıt altına alınmış olmalıdır.

18. FİZİKSEL GÜVENLİK POLİTİKASI

18.1 Amaç

Bu politika Kurum personeli ve kritik kurumsal bilgilerinin korunması amacıyla sistem odasına, kurumsal bilgilerin bulundurulduğu sistemlerin yer aldığı tüm çalışma alanlarına ve Kurum binalarına yetkisiz girişlerin yapılmasını önlemek amacını taşımaktadır.

18.2 Kapsam

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

18.3 Politika

a) Kurumun binalarının fiziksel olarak korunması, farklı koruma mekanizmaları ile donatılması temin edilmelidir.

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

c) Kurum dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili güvenlik görevlileri gözetiminde gerçekleştirilmelidir.

ç) Kritik bilgilerin bulunduğu alanlara girişlerin kontrolü akıllı kartlar veya biyometrik sistemler ile yapılmalı ve izlenmelidir.

d) Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin güncelliği sağlanmalıdır.

e) Personel kimliği ve yetkilerini belirten kartların ve ziyaretçi kartlarının düzenli olarak taşınması sağlanmalıdır.

f) Kritik sistemler özel sistem odalarında tutulmalıdır.

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

ğ) Fotokopi, yazıcı vs. türü cihazlar mesai saatleri dışında kullanıma kapatılmalı, mesai saatleri içerisinde yetkisiz kullanıma karşı koruma altına alınmalıdır.

h) Kuruma giriş yapacak ziyaretçi veya kurye teslimatlarının, gerekli fiziksel güvenlik kontrollerinden geçirildikten sonra geçişine izin verilmelidir.

ı) Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve kontrol altında tutulması temin edilmelidir.

i) Fotoğraf, video, ses vb. kayıt cihazlarının yetki verilmeyen kişiler tarafından güvenli alanlara sokulmasının yasaklanmalıdır.

19. KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI

19.1 Amaç

Kurumun bilgi sistemlerine erişiminde kimlik doğrulanması ve yetkilendirme politikalarını tanımlamaktır.

19.2 Kapsam

Türk Dil Kurumu Başkanlığı bilgi sistemlerine erişen Kurum personeli ile Kurum dışı kullanıcılar bu politika kapsamı altındadır.

19.3 Politika

a) Kurum sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yönetimi ile erişeceği belirlenecek ve kayıt edilecektir.

b) Kurum sistemlerine erişmesi gereken firma personeline yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanacak ve kayıt edilecektir.

c) Kurum bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veritabanları, işletim sistemleri ve giriş yapılarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkiler belirlenmeli, kayıt edilmeli ve denetim altında tutulmalıdır.

ç) Tüm kurumsal sistemler üzerindeki kullanım hakları (kullanıcıların kendi sistemlerine yönelik olarak birbirlerine verdikleri haklar dahil) periyodik olarak gözden geçirilmeli ve gereksinimler ve gerekli minimum yetkinin verilmesi prensibi doğrultusunda revize edilmelidir.

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

e) Kullanıcılar da Kurum tarafından kullanımlarına tahsis edilen sistemlerin güvenliğinden sorumludurlar.

f) Sistemlere başarılı ve başarısız erişim kayıtları düzenli olarak tutulmalı, tekrarlanan başarısız sisteme giriş girişimleri incelenmelidir.

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

ğ) Sistemlere giren kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve yetki ihlalleri kontrol edilmelidir.

h) Kullanıcılara erişim haklarını yazılı olarak beyan edilmelidir.

ı) Kullanıcı hareketlerini izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.

i) Sistemler üzerindeki tüm roller, rollere sahip kullanıcılar ve rollerin sistem kaynakları üzerindeki yetkileri uygun araçlar kullanılarak belirli aralıklarla listelenmelidir. Bu listeler yetki matrisleri ile karşılaştırılmalıdır. Eğer uyumsuzluk var ise nedenleri araştırılmalı ve dokümanlar veya yetkiler düzeltilerek uyumlu hale getirilmelidir.

20. DEĞİŞİM YÖNETİMİ POLİTİKASI

20.1 Amaç

Kurumun bilgi sistemlerinde yapılması gereken konfigürasyon değişikliklerinin güvenlik ve sistem sürekliliğini aksatmayacak şekilde yönetilmesine yönelik politikaları belirler.

20.2 Kapsam

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

20.3 Politika

a) Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri kayıt edilmelidir.

b) Yazılım ve donanım envanteri oluşturularak yazılım sürümleri kontrol edilmelidir.

c) Herhangi bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenmeli ve kayıt edilmelidir.

ç) Değişiklikler gerçekleştirilmeden önce güvenlik politikaları yöneticisi ve ilgili diğer yöneticilerin onayı alınmalıdır.

d) Tüm sistemlere yönelik konfigürasyon kaydı oluşturulmalı, yapılan her değişikliğin bu kayıtlarda güncellenmesi sağlanarak kurumsal değişiklik yönetimi ve takibi temin edilmelidir.

e) Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanmalı ve ilgili yöneticiler tarafından onaylanması sağlanmalıdır.

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

g) Yapılan değişiklikler sonrasında oluşabilecek güvenlik zafiyetleri güvenlik açıkları tespit etme politikası çerçevesinde kontrol edilmelidir.

ğ) Sistemler üzerinde yapılan değişiklikler elektronik ortamda sistem kayıtları vasıtasıyla da kontrol altında bulundurulmalıdır.

h) Teknoloji değişikliklerinin Kurumun sistemlerine etkileri belirli aralıklarla gözden geçirilmelidir.

21. PERSONEL GÜVENLİĞİ POLİTİKASI

21.1 Amaç

Kurumun bilgi kaynaklarının güvenliğinin sağlanması, çalışanlarının bu konuya duyarlı olması, bilinç seviyesi kendisine verilen yetki ve sorumlulukları iyi anlaması ve yerine getirmesiyle çok yakından bağlantılıdır. Bu nedenle Kurumun, ilgili personelin seçimi, sorumluluk ve yetkilerin atanması, eğitilmesi, işten ayrılması, görev değişiklikleri vb. konuların güvenlik ile ilgili boyutunu ne şekilde ele alacağını bu politika belirler.

21.2 Kapsam

Personel güvenlik politikası, Kurumun bilgi sistemlerini kullanan tüm yönetici ve çalışanları kapsamaktadır.

21.3 Politika

a) Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılmalıdır.

b) Kullanıcılara erişim haklarını açıklayan yazılı bildiriler verilmeli ve teyit alınmalıdır.

c) Yetkisi olmayan personelin, Kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.

ç) Bilgi sistemlerinde sorumluluk verilecek kişinin özgeçmişi araştırılmalı, beyan edilen akademik ve profesyonel bilgiler teyit edilmeli, karakter özellikleriyle ilgili tatmin edici düzeyde bilgi sahibi olmak için çevresinde ve dışında referans sorulması sağlanmalıdır.

d) Bilgi sistemleri ihalelerinde sorumluluk alacak firma personeli için güvenlik gereksinim ve incelemeleriyle ilgili koşullar eklenmelidir.

e) Kritik bilgiye erişim hakkı olan çalışanlar ile gizlilik anlaşmaları imzalanmalıdır.

f) Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenmelidir.

g) Güvenlik olaylarının rapor edilmesi için kurumsal bir mekanizma oluşturulmalıdır.

ğ) Çalışanlara telefon görüşmeleri yaparken civardakiler tarafından işitebileceği veya dinlenebileceği için hassas bilgilerin konuşulmaması hatırlatılmalıdır.

h) Çalışanlara kamuya açık alanlarda, açık ofis ortamlarında ince duvarları olan odalarda gizliliği olan konuşmaların yapılmaması hatırlatılmalıdır.

ı) İş tanımı değişen veya Kurumdan ayrılan kullanıcıların erişim hakları hemen silinmelidir.

i) Güvenlikle ilgili tüm görevler Türk Dil Kurumu Başkanlığı Güvenlik Politikası bildirisinde tanımlanan roller çerçevesinde ve atanan kişiler tarafından üstlenilecektir.

j) Tüm çalışanların kimliklerini belgeleyen kartları görünür şekilde üzerinde bulundurulmalıdır ve bu kartları taşımayan kişilerin Kurum içinde dolaşımının fark edilir kılınması gerekir.

k) Kurum bilgi sistemlerinin işletmesinden sorumlu personelin konularıyla ilgili teknik bilgi düzeylerini güncel tutmaları çalışma sürekliliği açısından önemli olduğundan eğitim planlamaları periyodik olarak yapılmalı, bütçe ayrılmalı, eğitimlere katılım sağlanmalı ve eğitim etkinliği değerlendirilmelidir.

l) Yetkiler, "görevler ayrımı" ve "en az ayrıcalık" esaslı olmalıdır. "görev ayrımı" , rollerin ve sorumlulukların paylaştırılması ile ilgilidir ve bu paylaşım sayesinde kritik bir sürecin tek kişi tarafından kırılma olasılığını azaltılır. "En az ayrıcalık" ise kullanıcıların gereğinden fazla yetkiyle donatılmamaları ve sorumlu oldukları işleri yapabilmeleri için yeterli olan asgari erişim yetkisine sahip olmaları demektir.

m) Kritik bir görevin tek kişiye bağımlılığını azaltmak ve aynı işi daha fazla sayıda çalışanın yürütebilmesini sağlamak amacıyla, yetkilerin izin verdiği ölçüde, bir sıra (rotasyon) dahilinde çalışanlara görev ve sorumluluk atanmalıdır. Böylece kritik bir iş birden fazla kişi tarafından öğrenilmiş olacaktır.

n) Çalışanlar, kendi işleri ile ilgili olarak bilgi güvenliği sorumlulukları, riskleri, görev ve yetkileri hakkında periyodik olarak eğitilmelidir. Yeni işe alınan elemanlar için bu eğitim, Kuruma uyum sğlama sırasında verilmelidir.

o) Çalışanların güvenlik ile ilgili aktiviteleri izlenmelidir.

ö) Çalışanların başka görevlere atanması ya da işten ayrılması durumunda işletilecek süreçler tanımlanmalıdır. Erişim yetkilerinin, kullanıcı hesaplarının, token, akıllı kart gibi donanımların iptal

edilmesi, alınması veya güncellenmesi sağlanmalı, varsa devam eden sorumluluklar kayıt altına alınmalıdır.

22. BAKIM POLİTİKASI

22.1 Amaç

Kurum bilgi sistemlerinde kullanılan sistemlerin bakımı ile ilgili politikaları belirlemektir.

22.2 Kapsam

Bakım politikası, Kurumun bilgi sistemlerini işletmekle sorumlu sistem yöneticilerini kapsar.

22.3 Politika

a) Kurum sistemlerinin tamamı (donanım, uygulama yazılımları, paket yazılımları, işletim sistemleri) periyodik bakım güvencesine alınmalıdır. Bunun için gerekli anlaşmalar için yıllık bütçe ayrılmalıdır.

b) Üreticilerden sistemler ile ilgili bakım prosedürleri sağlanmalıdır.

c) Firma teknik destek elemanlarının bakım yaparken "TÜRK DİL KURUMU BAŞKANLIĞI- Bilgi Güvenlik Politikaları"na uygun davranmaları sağlanmalı ve kontrol edilmelidir.

ç) Sistem üzerinde yapılacak değişiklikler ile ilgili olarak "Değişim Yönetimi Politikası" ve ilişkili standartlar uygulanmalıdır.

d) Bakım yapıldıktan sonra tüm sistem kayıtları güncellenmelidir.

e) Sistem bakımlarının ilgili politika ve standartlar tarafından belirlenmiş kuralara aykırı bir sonuç vermediğinden ve güvenlik açıklarına yol açmadığından emin olmak için periyodik uygunluk ve güvenlik testleri yapılmalıdır.

f) Sistem bakımlarından sonra bir güvenlik açığı yaratıldığından şüphelenilmesi durumunda "TÜRK DİL KURUMU BAŞKANLIĞI-Bilgi Güvenliği Politikası" uyarınca hareket edilmelidir.

23. UZAKTAN ERİŞİM POLİTİKASI

23.1 Amaç

Bu politikanın amacı firmaların, herhangi bir yerden Kurumun bilgi sistemlerine erişmesine ilişkin normları belirlemektir.

23.2 Kapsam

Bu politika Kuruma uzaktan hizmet veren kişi veya firmaları kapsamaktadır.

23.3 Politika

Kurum ve firma arasında şifreli iletişim hatları kullanılacaktır. İnternet üzerinden Kurumun herhangi bir yerindeki bilgisayara erişen kişi veya kurumlar VPN (IPSec, SSL vb.) teknolojisini kullanacaktır.

a) Uzaktan erişilen yer mutlaka statik IP'ye sahip olmalı ve bu IP Kurumun güvenlik cihazlarında tanımlı olmalıdır.

b) Firma uzaktan kimlerin hangi rollerde Kurum bilgisayarlarına eriştiğini belirtecek ve ayrıca ilgili kişilerin bilgisayara erişimde kullandığı kullanıcı adı ve şifreleri kapalı zarf ortamında tutanakla Kurumdaki en üst yetkiliye teslim edilecektir.

c) Kullanıcıların erişim şifreleri en az üç ayda bir değiştirilecektir. Verilen şifreler Kurumun şifreleme politikasına uygun olacaktır.

ç) Firma, kurumun hiçbir bilgisini (idari, mali, bilimsel vb.) görüntüleyemez, ekran çıktısını alamaz, transfer edemez ve Kurum dışına çıkartamaz. Aksi takdirde oluşacak yasal yükümlülüklerden firma sorumlu olacaktır.

d) Uzaktan erişim için mümkünse tek yönlü şifreleme (one-time password authentication, örnek: token device) veya güçlü bir passphrase (uzun şifre) destekli public/private key sistemi (akıllı kart) kullanılması tavsiye edilmektedir.

e) Firma çalışanları hiçbir şekilde kendilerinin giriş şifrelerini aile bireyleri dahil olmak üzere hiç kimseye veremezler.

f) Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar bağlantı esnasında aynı anda başka bir ağa bağlı olmadıklarından emin olmalıdırlar.

g) Uzaktan erişim yöntemi ile Kuruma erişen bütün bilgisayarlar en son güncellenmiş anti-virüs yazılımına sahip olmalıdırlar.

ğ) Uzaktan bağlanan kişi makinesinde zararlı kod, Truva atı vs. olduğundan şüpheleniyorsa bağlantıyı gerçekleştirmemelidir.

h) Uzaktan erişim yöntemi ile Kuruma erişen bilgisayar ağında güvenlik tedbirleri alınmış olmalıdır. (örnek, firewall, Saldırı Tespit ve Önleme Sistemleri, Domain altyapısı, sistem yazılımları güncelleme sistemleri vb.)

ı) Kurum ağına standart dışı erişim isteğinde bulunan organizasyon veya kişiler Kurumun bilgi işlem biriminden izin almak zorundadırlar.

i) Firma, periyodik olarak kullanıcı kimlikleri ve hesaplarını kontrol etmeli gereksiz kullanıcı kimlikleri ve hesapları kaldırmalıdır.

j) Firma, Kurum ile hassas veriye erişim hakkında gizlilik anlaşması imzalamalıdır.

k) Kurum, firmanın alması gereken güvenlik tedbirlerinde herhangi bir aksaklık gördüğünde Kurum ve firma arasında uzaktan erişim bağlantısını eksiklik düzeltilinceye kadar kesebilir.

l) Kurum, güvenli erişimin sağlanabilmesi için gerekli gördüğü takdirde firmanın sadece belli zaman aralıklarında veya istek yapılan durumda uzaktan erişimine izin verebilir.

24. YAZILIM GELİŞTİRME

24.1 Amaç

Yazılım geliştirme üzerindeki kontroller, Kurumun günlük operasyonlarını yürütmek için kullandıkları yazılımların oluşturulması esnasında kullanılan kontrol mekanizmalarıdır. Programların geliştirilmesi esnasında uygulanması gereken kontroller, yazılımların kontrollü bir şekilde geliştirilmesini sağlamayı hedeflemektedir. Bu şekilde güvenlik kriterlerinin hem yazılımın geliştirilmesi aşamasında, hem de geliştirilen yazılım uygulamaya alındıktan sonra gözetilmesi sağlanır. Bu politika yazılım geliştirme hakkındaki kriterleri ortaya koymaktadır.

24.2 Kapsam

Bu politika Kurumda yazılım geliştirme alanında faaliyet gösteren kişi ve firmaları kapsamaktadır.

24.3 Politika

Yazılım geliştirme üzerindeki kontroller şu temel kriterlere uygun şekilde oluşturulmalıdır:

a) Sistem yazılımında mevcut olan kontroller, kullanılacak yeni bir yazılım veya mevcut sistem yazılımına yapılacak olan güncellemeler ile etkisiz hale getirilmemelidir.

b) Yönetim sadece uygun yazılım projelerinin başlatıldığından ve proje alt yapısının uygun olduğundan emin olmalıdır.

c) İhtiyaçlar uygun bir şekilde tanımlanmalıdır.

ç) Sistem geliştirmede, ihtiyaç analizi, fizibilite çalışması, tasarım, geliştirme, deneme ve onaylama safhalarını içeren sağlıklı bir metodoloji kullanılmalıdır.

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

e) Kurumda kişisel olarak geliştirilmiş yazılımların kullanılması kısıtlanmalıdır. Bilgi

f) Hazırlanan sistemler mevcut prosedürler dahilinde, işin ve iç kontrol gerekliliklerini yerine getirdiklerinden emin olunması açısından test edilmeli ve yapılan testler ve test sonuçları belgelenerek onaylanmalıdır.

g) Yeni alınmış veya revize edilmiş bütün yazılımlar test edilmeli ve onaylanmalıdır.

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

h) Uygulama ortamına aktarılma kararı uygun bilgilere dayalı olarak ilgili yönetim tarafından verilmelidir.

ı) Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.

i) Yazılımlar sınıflandırılmalı / etiketlenmeli ve envanterleri çıkarılarak bir yazılım kütüğünde muhafaza edilmelidir.

25. PERSONEL VE EĞİTİM

25.1 Amaç

Bilişim sistemlerinin kaynaklanan sorunların büyük bir kısmı insanlar tarafından yapılan hata, ihmal ve suistimallerden kaynaklanmaktadır. Bu nedenle kurumların, personelin hata yapma riskini düşürecek kontroller kurmaları önem kazanmaktadır. Bu uygun personel ve eğitim politikalarının benimsenmesi sayesinde başarılıdır. Farklı kişiler tarafından yerine getirilmesi gereken görevlerin ayrılması, işlemlerin yetkilendirilmesi, kaydedilmesi ve varlıkların korunması açısından önemlidir. Görevlerin ayrılması, bir kişinin diğer bir kişinin yaptığı faaliyetleri kontrol etme imkanı vermesi

nedeniyle de hata riskini düşürür. Bu politika personel ve eğitim hakkındaki kriterleri ortaya koymaktadır.

25.2 Kapsam

Bu politika Kurum yönetimini kapsamaktadır.

25.3 Politika

Personel ve eğitim politikaları şu temel kriterlere uygun oluşturulmalıdır:

a) Eğitim stratejisi birbirleriyle aynı doğrultuda olmalıdır. Bu sayede bilişim stratejisinin başarılı bir şekilde uygulanması sağlanır.

b) Personelin sisteme tanımlanması ve yetkilerinin belirlenmesi işlemi yönetim tarafından onaylanmış bir prosedür dahilinde yapılmalıdır.

c) Kurum yapısı içindeki yetki ve sorumluluklar açıkça tanımlanmış olmalıdır.

ç) İşe alınan personel mevcut yapı güvenlik sistemleri hakkında bilgilendirilmelidir.

d) Kurum tarafından, kimin hangi yöneticiye rapor vereceğini gösteren organizasyon tabloları oluşturulmuştur.

e) Kurum tarafından, bilişim sistemi kuran, geliştiren ve kullanan personelin görev tanımları yapılmış olmalıdır.

f) Personelin işe alınması, görev yerlerinin değiştirilmesi, görevlerine son verilmesi ve performanslarının değerlendirilmesinde güvenlik göz önünde bulundurulmalıdır. Personel, yeteneklerine uygun işlerde çalıştırılmalıdır.

g) Bilişim alanında istihdam edilecek daimi personel ile sözleşmeli veya danışman olarak çalıştırılarak personelin seçiminde, bu kişilerin işin gerektirdiği örenim ve eğitimi almış yetenekli ve dürüst kişiler olmalarına azami dikkat gösterilmelidir.

ğ) Bilişim yöneticileri, personelin bugün ve yakın gelecekte ihtiyaç duyulan yeteneklere sahip olup olmadıklarını bilmeli ve onlara bu ihtiyaçları karşılayacak eğitimi verdirmelidir. Bilişim eğitimi pahalı bir eğitim olduğu için eğitim planları ve bütçeleri kontrol edilmelidir.

h) Bilişim personelinin Kurumun mevcut ve uzun vadeli politikaları ile paralellik gösteren bir şekilde sertifika programlarına katılımı ve sertifikasyonlarını tamamlaması gerekmektedir.

ı) Kurumda görev dağılımı yapılırken, birbirleriyle bağdaşmayacak nitelikteki işlevler ve rollerin birbirinden ayrılması ve buna ilişkin politikalar geliştirilmelidir.

i) Görevlerin ayrılması bir kişinin diğer bir kişinin yaptığı faaliyetleri kontrol etme imkanı verecek şekilde olmalıdır.

j) Çalışanlar görev ve sorumluluklarının neler olduğunu bilmelidir.

k) Yönetim, kullanılan kontrollerin ne derecede etkin olduğu değerlendirilmelidir.

l) Personelin faaliyetleri, resmi çalışma prosedürleri, denetim ve gözden geçirme yollarıyla kontrol altında tutmalıdır.

m) Bütün çalışanlar aktif gözetim yönlendirmeye tabi tutularak desteklenmelidir.

26. BELGELENDİRME

26.1 Amaç

Kurumun belgeleme politikalarının yetersiz olması, personelin hatalı veya yetkisiz işlem yapma riskini yükseltebilir. Ayrıca, sistemde bir hata meydana geldiği zaman, eğer işlemler yeterli bir şekilde belgelenmemişse, hatanın sebebinin tespiti de güçleşebilir.

26.2 Kapsam

Bu politika Kurum yönetimini kapsamaktadır.

26.3 Politika

Belgeleme politikaları şu temel kriterlere uygun oluşturulmalıdır:

a) Bilişim sisteminin yapısı ile bütün iş ve işlemler açıkça belgelenmeli ve bu belgeleme inceleme amacıyla kolaylıkla ulaşılabilir durumda olmalıdır.

b) İş akışları uygun şekilde belgelenmelidir.

c) Belgeleme, tarih belirterek yapılmalı ve yedek kopyaları güvenli bir yerde muhafaza edilmelidir.

ç) Girdi türleri ve girdi form örnekleri belgelenmelidir.

d) Ana dosyalar ile diğer dosyaların içerik ve şekilleri belgelenmelidir.

e) Çıktı form örnekleri ve çıktıların kimlere dağıtılacağı belgelenmelidir.

f) Programların nasıl test edildiği ve test sonuçları belgelenmelidir.

g) Bütün program değişikliklerinin detayları belgelenmelidir.