KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI.

GENEL KULLANIM POLİTİKASI..... 2

AĞ CİHAZLARI GÜVENLİĞİ POLİTİKASI..... 2

AĞ YÖNETİMİ POLİTİKASI..... 3

ANTİVİRÜS POLİTİKASI..... 3

BAKIM POLİTİKASI..... 4

DEĞİŞİM YÖNETİMİ POLİTİKASI..... 4

DONANIM VE YAZILIM ENVANTERİ OLUŞTURMA POLİTİKASI..... 4

E-POSTA POLİTİKASI..... 5

FİZİKSEL GÜVENLİK POLİTİKASI..... 5

İNTERNET ERİŞİM POLİTİKASI..... 6

KABLOSUZ İLETİŞİM POLİTİKASI..... 6

KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI..... 7

KRİZ/ACİL DURUM POLİTİKASI..... 7

PAROLA POLİTİKASI..... 8

PERSONEL GÜVENLİĞİ POLİTİKASI..... 9

PERSONEL VE EĞİTİM POLİTİKASI..... 9

UZAKTAN ERİŞİM POLİTİKASI..... 10

FİRMALAR İÇİN UZAKTAN ERİŞİM POLİTİKASI..... 11

GÜVENLİK AÇIKLARI TESPİT ETME POLİTİKASI..... 11

SUNUCU GÜVENLİK POLİTİKASI..... 12

TEMİZA MASA TEMİZ EKRAN POLİTİKASI..... 12

VERİ TABANI GÜVENLİK POLİTİKASI..... 13

VPN POLİTİKASI..... 14

YEDEKLEME POLİTİKASI..... 14

Genel Kullanım Politikası

KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI.'nin bütün çalışanları, sözleşmelileri ve kurum adı altında çalışan bütün kişiler için geçerllidir. Aynı zamanda kurumun sahip olduğu ve kiraladığı bütün cihazlar için geçerlidir.

Bilgi sistemleri genel kullanım

1. KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI. 'in güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da, KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI.'in bünyesinde oluşturulan tüm veriler XXFirmaXX 'in mülkiyetindedir.
2. Kullanıcılar bilgi sistemlerini kişisel amaçlarla kullanmamalıdır. Bu konuda ilgili politikalar dikkate alınmalıdır.
3. KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI., bu politika çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.
4. KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI.bilgisayarları etki alanına dahil edilmelidir. Etki alanına bağlı olmayan bilgisayarlar yerel ağdan çıkarılmalı, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi olmamalıdır.
5. Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı ve kopyalanmamalıdır.
6. KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI.yetkilileri bilgisi ve onayı olmadan KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI.Ağ sisteminde (web hosting, e- posta servisi vb.) sunucu nitelikli bilgisayar bulundurulmamalıdır.
7. Birimlerde sorumlu bilgi işlem personeli ve ilgili teknik personel haricindeki kullanıcılar tarafından ağa bağlı cihazlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri gibi ayarlar değiştirilememelidir.
8. Bilgisayarlara lisanssız program yüklenmemelidir.
9. Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır. Kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.
10. Dizüstü bilgisayarın çalınması/kaybolması durumunda, durum fark edildiğinde en kısa zamanda Başkanlık'a da haber verilmelidir.
11. Bütün cep telefonu ve PDA (Personal Digital Assistant) cihazları KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI.'in ağı ile senkronize olsun veya olmasın şifreleri aktif halde olmalıdır. Kullanılmadığı durumlarda kablosuz erişim (kızılötesi, bluetooth, vb) özellikleri aktif halde olmamalıdır ve mümkünse anti-virüs programları ile yeni nesil virüslere karşı korunmalıdır.
12. Kullanıcılar ağ kaynaklarının verimli kullanımı konusunda dikkatli olmalıdır. E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olunmalı ve mümkünse dosyalar sıkıştırılmalıdır.

Ağ Cihazları Güvenliği Politikası

Ağ cihazları güvenlik politikası ile ilgili kurallar aşağıda belirtilmiştir.

1. Ağ cihazlarının IP ve MAC adres bilgileri envanter dosyasında yer almalıdır.
2. Yönlendirici ve anahtarlardaki tam yetkili şifre olan 'enable şifresi' kodlanmış formda saklanmalıdır. Bu şifrenin tanımlanması kurumun içerisinden yapılmalıdır.
3. İhtiyaç duyulduğu zaman erişim listeleri eklenmelidir.
4. Yönlendirici ve anahtarlar kurumun yönetim sisteminde olmalıdır.
5. Yazılım ve firmware güncellemeleri önce test ortamlarında denenmeli, sonra çalışma günlerinin dışında üretim ortamına taşınmalıdır.
6. Cihazlar üzerinde kullanılmayan servisler kapatılmalıdır.
7. Bilgisayar ağında bulunan kabinetler, aktif cihazlar, ağ kabloları (UTP ve fiber optik aktarma kabloları), cihazların portları etiketlenmelidir.
8. Her bir yönlendirici ve anahtar aşağıdaki uyarı yazısına sahip olmalıdır. Yönlendiriciye erişen tüm kullanıcıları uyarmalıdır.

"BU CİHAZA YETKİSİZ ERİŞİMLER YASAKLANMIŞTIR. Bu cihaza erişim ve yapılandırma için yasal hakkınız olmak zorundadır. Bu cihaz üzerinde işletilen her komut loglanabilir, bu politikaya uymamak disiplin kuruluna sevk ile sonuçlanabilir veya yasal yaptırım olabilir."

Ağ Yönetimi Politikası

1. Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için düzenli denetimler yapılmalı ve güncellemeler uygulanmalıdır.
2. Erişimine izin verilen ağlar, ağ servisleri ve ilgili yetkilendirme yöntemleri belirtilmeli ve yetkisiz erişimle ilgili tedbirler alınmalıdır.
3. Gerek görülen uygulamalar için, portların belirli uygulama servislerine veya güvenli ağ geçitlerine otomatik olarak bağlanması sağlanmalıdır.
4. Sınırsız ağ dolaşımı engellenmelidir. Ağ servisleri, varsayılan durumda erişimi engelleyecek şekilde olup, ihtiyaçlara göre serbest bırakılmalıdır.
5. Harici ağlar üzerindeki kullanıcıları belirli uygulama servislerine veya güvenli ağ geçitlerine bağlanmaya zorlayıcı teknik önlemler alınmalıdır.
6. İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden güvenlik duvarı gibi ağ cihazları yoluyla önlemler alınmalı ve kayıtlar tutulmalıdır.
7. Ağ erişimi VPN, VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılmalıdır. Kurum kullanıcılarının bilgisayarlarının bulunduğu ağ, sunucuların bulunduğu ağ, DMZ ağı birbirlerinden ayrılmalı ve ağlar arasında geçiş güvenlik sunucuları (firewall) üzerinden sağlanmalıdır.
8. Uzaktan teşhis ve müdahale için kullanılacak portların güvenliği sağlanmalıdır.
9. Bilgisayar ağına bağlı bütün makinelerde kurulum ve yapılandırma parametreleri, Kurumun güvenlik politika ve standartlarıyla uyumlu olmalıdır.
10. Sistem tasarımı ve geliştirilmesi yapılırken Kurum tarafından onaylanmış olan ağ ara yüzü ve protokolleri kullanılmalıdır.
11. İnternet trafiği, İnternet Erişim ve Kullanım Politikası ve ilgili standartlarda anlatıldığı şekilde izlenebilmelidir.
12. Bilgisayar ağındaki adresler, ağa ait yapılandırma ve diğer tasarım bilgileri 3. şahıs ve sistemlerin ulaşamayacağı şekilde saklanmalıdır.
13. Ağ cihazları görevler dışında başka bir amaç için kullanılmamalıdır.
14. Ağ cihazları yapılandırılması Sistem Yöneticisi tarafından veya Sistem Yöneticisinin denetiminde yapılmalı ve değiştirilmelidir.
15. Ağ dokümantasyonu hazırlanmalı ve ağ cihazlarının güncel yapılandırma bilgileri gizli ortamlarda saklanmalıdır.

ANTİVİRUS POLİTİKASI

1. Kurumun tüm istemcileri ve sunucuları antivirüs yazılımına sahip olmalıdır. Ancak sistem yöneticilerinin gerekli gördüğü sunucular üzerine istisna olarak antivirüs yazılımı yüklenmeyebilir.
2. İstemcilere ve sunuculara virüs bulaştığı fark edildiğinde etki alanından çıkartılmalıdır.
3. Sistem yöneticileri, antivirüs yazılımının sürekli ve düzenli çalışmasından ve istemcilerin ve sunucuların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur.
4. Kullanıcı hiç bir sebepten dolayı antivirüs yazılımını bilgisayarından kaldırmamalıdır.
5. Antivirüs güncellemeleri antivirüs sunucusu ile yapılmalıdır.
6. Sunucular internete sürekli bağlı olup, sunucuların veri tabanları otomatik olarak güncellenmelidir. Etki alanına bağlı istemcilerin, otomatik olarak antivirüs sunucusu tarafından antivirüs güncellemeleri yapılmalıdır.
7. Etki alanına dâhil olmayan kullanıcıların güncelleme sorumluluğu kendilerine ait olup, herhangi bir sakınca tespit edilmesi durumunda, sistem yöneticileri bu bilgisayarları ağdan çıkartabilmelidir.
8. Bilinmeyen veya şüpheli kaynaklardan dosya indirilmemelidir.
9. Kurumun ihtiyacı haricinde okuma/yazma hakkı veya disk erişim hakkı tanımlamaktan kaçınılmalıdır. İhtiyaca binaen yapılan bu tanımlamalar, ihtiyacın ortadan kalkması durumunda iptal edilmelidir.
10. Optik Media ve harici veri depolama cihazları antivirüs kontrolünden geçirilmelidir.
11. Kritik veriler ve sistem yapılandırmaları düzenli aralıklar ile yedeklenmeli ve bu yedekler farklı bir elektronik ortamda güvenli bir şekilde saklanmalıdır. Yedeklenen verinin kritik bilgiler içermesi durumunda, alınan yedekler şifre korumalı olmalıdır.

Bakım Politikası

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

2. Üreticilerden sistemler ile ilgili bakım prosedürleri sağlanmalıdır.
3. Sistem üzerinde yapılacak değişiklikler ile ilgili olarak "Değişim Yönetimi Politikası" ve ilişkili standartlar uygulanmalıdır.
4. Bakım yapıldıktan sonra tüm sistem dokümantasyonu güncellenmelidir.
5. Sistem bakımlarının ilgili politika ve standartlar tarafından belirlenmiş kurallara aykırı bir sonuç vermediğinden ve güvenlik açıklarına yol açmadığından emin olmak için periyodik uygunluk ve güvenlik testleri yapılmalıdır.
6. Sistem bakımlarından sonra bir güvenlik açığı yaratıldığından şüphelenilmesi durumunda " KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI. Bilgi Güvenlik Politikaları " uyarınca hareket edilmelidir.

Değişim yönetim politikası

1. Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümante edilmelidir.
2. Yazılım ve donanım envanteri oluşturularak, yazılım sürümleri kontrol edilmelidir.
3. Herhangi bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenmeli ve dokümante edilmelidir.
4. Değişiklikler gerçekleştirilmeden önce Güvenlik Politikaları yöneticisi ve ilgili diğer yöneticilerin onayı alınmalıdır.
5. Tüm sistemlere yönelik yapılandırma dokümantasyonu oluşturulmalı, yapılan her değişikliğin bu dokümantasyonda güncellenmesi sağlanarak kurumsal değişiklik yönetimi ve takibi temin edilmelidir.
6. Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanmalı ve ilgili yöneticiler tarafından onaylanması sağlanmalıdır.
7. Ticari programlarda yapılacak değişiklikler, ilgili üretici tarafından onaylanmış kurallar çerçevesinde gerçekleştirilmelidir.
8. Teknoloji değişikliklerinin Kurumun sistemlerine etkileri belirli aralıklarla gözden geçirilmeli ve dokümante edilmelidir.

DONANIM VE YAZILIM ENVANTERİ OLUŞTURMA POLİTİKASI

1. KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI.sistem biriminin admin/root yetkisi bulunmalıdır. Yapılacak tüm işlemler sistem güvenlik birimi nezaretinde yürütülmelidir. Kuruma ait sunucularda, sadece yetkili kişilerin erişebileceği administrator/root yetkisi bulunmalıdır.
2. Kuruma ait sunucular üzerinde bulunan, tüm kullanıcı hesapları (administrator ve root hesaplarıda dahil olmak üzere) güçlü şifreler ile korunmalıdır.
3. Yapılacak tüm işlemler düzgün bir şekilde dokümante edilmeli ve ilgili birim sorumlularına iletilmelidir.
4. Güvenlik yazılım ve donanımlarının erişim logları, merkezi log sisteminde tutulmalı ve izlenmelidir.
5. Güvenlik yazılım ve donanımlarının logları, her bir yazılım ve donanım için belirlenen disk alanlarında tutulmalı ve ilgili birim tarafından yönetilmelidir.
6. Güvenlik donanımları, yetkisiz kişiler tarafından erişilememesi için gerekli güvenlik tedbirleri alınmış sistem odalarında tutulmalıdır.
7. Güvenlik donanımlarının konfigürasyon yedekleri düzenli olarak alınmalı ve bir back-up sunucusunda tutulmalıdır.
8. Kurumda kullanılan güvenlik yazılım ve donanımları en güncel ve stabil yamaya (patch) sahip olmalıdır.
9. Kurumda kullanılan güvenlik donanımları, harici izleme yazılım ya da donanımları ile izlenmeli ve cihazlarda oluşan sorunlar sms ve/veya eposta aracılığı ile ilgili sorumlulara iletilmelidir.
10. Kurumun tüm istemcileri ve sunucuları anti-virüs yazılımına sahip olmalıdır.

11. Ancak sistem yöneticilerinin gerekli gördüğü sunucular üzerine istisna olarak anti-virüs yazılımı yüklenmeyebilir.
12. İstemcilere ve sunuculara virüs bulaştığı fark edildiğinde etki alanından çıkartılmalıdır. Sistem yöneticileri, anti-virüs yazılımının sürekli ve düzenli çalışmasından ve istemcilerin ve sunucuların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur.
13. Kullanıcı hiç bir sebepten dolayı anti-virüs yazılımını bilgisayarından kaldırmamalıdır.
14. Anti-virüs güncellemeleri anti-virüs sunucusu ile yapılmalıdır.
15. Sunucular internete sürekli bağlı olmalı, sunucuların veri tabanları otomatik olarak güncellenmelidir.
16. Etki alanına bağlı istemcilerin, anti-virüs sunucusu tarafından anti-virüs güncellemeleri otomatik olarak yapılmalıdır. Etki alanına dâhil olmayan kullanıcıların güncelleme sorumluluğu kendilerine ait olup, herhangi bir sakınca tespit edilmesi durumunda, sistem yöneticileri bu bilgisayarların internet bağlantılarını kesebilme opsiyonuna sahip olmalıdır.
17. Bilinmeyen veya şüpheli kaynaklardan dosya indirilmemelidir.
18. Kurumun ihtiyacı haricinde okuma/yazma hakkı veya disk erişim hakkı tanımlamaktan kaçınılmalıdır.
19. İhtiyaca binaen yapılan bu tanımlamalar, ihtiyacın ortadan kalkması durumunda iptal edilmelidir.
20. Optik Media ve harici veri depolama cihazları anti-virüs kontrolünden geçirilmelidir

EPOSTA POLİTİKASI

E-Posta ile ilgili yasaklanmış kullanım kuralları aşağıda belirtilmiştir.

1.Kullanıcı hesaplarına ait parolalar ikinci bir şahsa verilmemelidir.

2. KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI.ile ilgili olan gizli bilgi, gönderilen mesajlarda yer almamalıdır. Bunun kapsamı içerisine iliştirilen öğeler de dâhildir.

3.Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir.

4.Kullanıcı, KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI.e-posta sistemini taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında ilgili birime haber verilmelidir.

5.Kullanıcı hesapları, ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçlar ile e-posta gönderilmemelidir.

6.Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip, ilgili birime haber verilmelidir.

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

8.Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.

Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul edip; suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların yollanmasından sorumludur.

FİZİKSEL GÜVENLİK POLİTİKASI

1. Kurumun binalarının fiziksel olarak korunması gerekli önlemler ile yapılmalıdır.
2. 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.
3. Kurum dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili güvenlik görevlileri gözetiminde gerçekleştirilmelidir.
4. Kritik bilgilerin bulunduğu alanlara girişlerin kontrolü akıllı kartlar veya biyometrik sistemler ile yapılmalı ve izlenmelidir.
5. Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin güncelliği sağlanmalıdır.
6. Personel kimliği ve yetkilerini belirten kartların ve ziyaretçi kartlarının düzenli olarak taşınması sağlanmalıdır.

7. Kritik sistemler özel sistem odalarında tutulmalıdır.
8. Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmalı, yangın ve benzer felaketlere karşı koruma altına alınmalı ve iklimlendirilmesi sağlanmalıdır.
9. Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve kontrol altında tutulması temin edilmelidir.

İNTERNET ERİŞİM VE KULLANIM POLİTİKASI

1. Kurumun bilgisayar ağı, erişim ve içerik denetimi yapan ağ güvenlik duvar(lar)ı üzerinden internete çıkmalıdır. Ağ güvenlik duvarı, kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve İnternet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır.
2. Kurumun politikaları doğrultusunda içerik filtreleme sistemleri kullanılmalıdır. İstenilmeyen siteler (pornografi, oyun, kumar, şiddet içeren vs.) yasaklanmalıdır.
3. Kurumun ihtiyacı doğrultusunda Saldırı Tespit ve Önleme Sistemleri kullanılmalıdır.
4. Kurumun ihtiyacı ve olanakları doğrultusunda antivirüs sunucuları kullanılmalıdır.
5. İnternete giden ve gelen bütün trafik virüslere karşı taranmalıdır.
6. Kullanıcıların internet erişimlerinde firewall, antivirüs, içerik kontrol vs. güvenlik kriterleri hayata geçirilmelidir.
7. Ancak yetkilendirilmiş kişiler internete çıkarken, Kurumun normal kullanıcılarının bulunduğu ağdan farklı bir ağda olmak kaydıyla, bütün servisleri kullanma hakkına sahiptir.
8. Çalışma saatleri içerisinde iş ile ilgili olmayan sitelerde gezinilmemelidir.
9. İş ile ilgili olmayan (müzik, video dosyaları) dosyalar gönderilmemeli ve indirilmemelidir.
10. Bu konuda gerekli önlemler alınmalıdır. Üçüncü şahısların internet erişimleri için misafir ağı erişimi verilmelidir.

KABLOSUZ İLETİŞİM POLİTİKASI

1. Kurumun bilgisayar ağına bağlanan bütün erişim cihazları ve ağ arabirim kartları kayıt altına alınmalıdır.
2. Bütün kablosuz erişim cihazları Bilgi İşlem Güvenlik Birimi tarafından onaylanmış olmalı ve Bilgi İşlemin belirlediği güvenlik ayarlarını kullanmalıdır.
3. Kablosuz iletişim ile ilgili gereklilikler aşağıda belirtilmiştir.
    a. Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmalıdır. Bunun için Wi-Fi Protected Access2 (WPA2-kurumsal) şifreleme kullanılmalıdır.
    b. IEEE 802.1x erişim kontrol protokolü ve TACACS+ ve RADIUS gibi güçlü kullanıcı kimlik doğrulama protokolleri kullanılmalıdır
4. Erişim cihazlarındaki firmwareler düzenli olarak güncellenmelidir. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlamaktadır.
5. Cihaza erişim için güçlü bir parola kullanılmalıdır. Erişim parolaları varsayılan ayarda bırakılmamalıdır.
6. Radyo dalgalarının binanın dışına taşmamasına özen gösterilmelidir. Bunun için çift yönlü antenler kullanılarak radyo sinyallerinin çalışma alanında yoğunlaşması sağlanmalıdır.
7. Cihazları üzerinden gelen kullanıcılar Firewall üzerinden ağa dâhil olmalıdırlar.
8. Erişim cihazları üzerinden gelen kullanıcıların internete çıkış bant genişliğine sınırlama getirilmeli ve kullanıcılar tarafından Kurum'un tüm internet bant genişliğinin tüketilmesi engellenmelidir.
9. Erişim cihazları üzerinden gelen kullanıcıların ağ kaynaklarına erişim yetkileri, internet üzerinden gelen kullanıcıların yetkileri ile sınırlı olmalıdır.
10. Kullanıcı bilgisayarlarında kişisel antivirüs ve güvenlik duvarı yazılımları yüklü olmalıdır.

KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI

1. Kurum sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenecek ve dokümante edilecektir.
2. Kurum sistemlerine erişmesi gereken firma kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanacak ve dokümante edilecektir.
3. Kurum bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veritabanları, işletim sistemleri ve log-on olarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkiler belirlenmeli, dokümante edilmeli ve denetim altında tutulmalıdır.
4. Tüm kurumsal sistemler üzerindeki kullanım hakları (kullanıcıların kendi sistemlerine yönelik olarak birbirlerine verdikleri haklar dahil) periyodik olarak gözden geçirilmeli ve bu gereksinimler gerekli minimum yetkinin verilmesi prensibi doğrultusunda revize edilmelidir.
5. Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilmelidir.
6. Sistemlere başarılı ve başarısız erişim istekleri düzenli olarak tutulmalı, tekrarlanan başarısız erişim istekleri/girişimleri incelenmelidir.
7. Kullanıcı hareketlerini izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır. Sistemler üzerindeki tüm roller, rollere sahip kullanıcılar ve rollerin sistem kaynakları üzerindeki yetkileri uygun araçlar kullanılarak belirli aralıklarla listelenmelidir. Bu listeler yetki seviyeleri ile karşılaştırılmalıdır. Eğer uyumsuzluk varsa dokümanlar ve yetkiler düzeltilerek uyumlu hale getirilmelidir.

POLİTİKA

1. Acil durum sorumluları atanmalı ve yetki ve sorumlulukları belirlenmelidir.
2. Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınmalıdır. Örneğin uygulama veya veritabanı sunucularından donanım ve yazılıma ait problemler oluştuğunda yerel veya uzak sistemden yeniden kesintisiz çalışma sağlanabilmelidir.
3. Kurum bilişim sistemlerinin kesintisiz çalışmasını sağlaması için aynı ortamda kümeleme veya uzaktan kopyalama veya pasif sistem çözümlerini hayata geçirilebilir. Kurumlar sistemlerini tasarlarken ne kadar süre iş kaybını tolere edeceklerini göz önüne almalıdırlar.
4. Acil durumlarda kurum içi işbirliği gerksinimleri tanımlanmalıdır.
5. Acil durumlarda sistem logları incelenmek üzere saklanmalıdır.
6. Güvenlik açıkları ve ihlallerinin rapor edilmesi için kurumsal bir mekanizma oluşturulmalıdır.
7. Yaşanan acil durumlar sonrası politikalar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilmelidir.
8. Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulmalı ve bu bildirim süreçleri tanımlanmış olmalıdır.
9. Acil durum kapsamında değerlendirilen olaylar aşağıda farklı seviyelerde tanımlanmıştır.
    a. Seviye A: Bilgi kaybı. Kurumsal değerli bilgilerin yetkisiz kişilerin eline geçmesi, bozulması, silinmesi
    b. Seviye B: Servis kesintisi. Kurumsal servislerin kesintisi veya kesintisine yol açabilecek durumlar
    c. Seviye C: Şüpheli durumlar. Yukarıda tanımlı ilk iki seviyedeki duruma sebebiyet verebileceğinden şüphe duyulan ancak gerçekliği ispatlanmamış durumlar.
10. 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.
11. Bilgi güvenliği yöneticisi tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmek üzere ilgli makamlara iletilmelidir.

PAROLA POLİTİKASI

1. Parola Politikası ile ilgili genel kurallar aşağıda belirtilmiştir.

1. Sistem hesaplarına ait parolalar (örnek; root, administrator, enable, vs.) en geç 6(altı) ayda bir değiştirilmelidir.
2. Kullanıcı hesaplarına ait parolalar (örnek, e-posta, web, masaüstü bilgisayar vs.) en geç 45(kırk beş) günde bir değiştirilmelidir.
3. Sistem yöneticisi sistem ve kullanıcı hesapları için farklı parolalar kullanmalıdır.
4. Parolalar e- posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
5. Kullanıcı, parolasını başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlara yazmaması konusunda bilgilendirilmeli ve eğitilmelidir.

6. Kurum çalışanı olmayan kişiler için açılan kullanıcı hesapları da kolayca kırılamayacak güçlü bir parolaya sahip olmalıdır.
7. Bir kullanıcı adı ve parolası, birim zamanda birden çok bilgisayarda kullanılmamalıdır.

2. Kullanıcı güçlü bir parola oluşturmak için aşağıdaki parola özelliklerini uygulamalıdır.

1. En az 6 haneli olmalıdır.
2. İçerisindeenaz1taneharfbulunmalıdır.(a,b,C...)
3. İçerisinde en az 2 tane rakam bulunmalıdır. (1, 2, 3...)
4. İçerisinde en az 1 tane özel karakter bulunmalıdır. (@, !,?,a,+,$,#,&,/,{,*,-,],=,...)
5. Aynı karakterler peş peşe kullanılmamalıdır. (aaa, 111, XXX, ababab...)
6. Sıralı karakterler kullanılmamalıdır. (abcd, qwert, asdf,1234,zxcvb...)
7. Kullanıcıya ait anlam ifade eden kelimeler içermemelidir. (Aileden birisinin, arkadaşının, bir sanatçının, sahip olduğu bir hayvanın ismi, arabanın modeli vb.)

3. Şifre koruma standartları ile ilgili kurallar aşağıda belirtilmiştir.

1. Bütün parolalar Kuruma ait gizli bilgiler olarak düşünülmeli ve kullanıcı, parolalarını hiç kimseyle paylaşmamalıdır.
2. Web tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki "parola hatırlama" seçeneği kullanılmamalıdır.
3. Parola kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir.

Güvenlik taraması sonucunda parolalar tahmin edilirse veya kırılırsa kullanıcıdan parolasını değiştirmesi talep edilebilir.

Personel Güvenliği Politika

1. Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılmalıdır.
2. Kullanıcılara erişim haklarını açıklayan yazılı bildiriler verilmeli ve teyit alınmalıdır.
3. Yetkisi olmayan personelin, kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.
4. 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 iş çevresinden ve dışından referans sorulması sağlanmalıdır.
5. Bilgi sistemleri ihalelerinde sorumluluk alacak firma personeli için güvenlik gereksinim ve incelemeleriyle ilgili koşullar eklenmelidir.
6. Kritik bilgiye erişim hakkı olan çalışanlar ile gizlilik anlaşmaları imzalanmalıdır.
7. Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenmelidir.
8. Çalışanlara telefon görüşmeleri yaparken civardakiler tarafından işitilebileceği veya dinlenebileceği için hassas bilgilerin konuşulmaması hatırlatılmalıdır.
9. Çalışanlara kamuya açık alanlarda, açık ofis ortamlarında ve ince duvarları olan odalarda gizliliği olan konuşmaların yapılmaması hatırlatılmalıdır.
10. İş tanımı değişen veya kurumdan ayrılan kullanıcıların erişim hakları hemen silinmelidir.
11. Kurum bilgi sistemlerinin işletilmesinden 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.
12. Yetkiler "görevler ayrımı" ve "en az ayrıcalık" esaslı olmalıdır. "Görevler ayrımı " rollerin sorumlulukların paylaştırılması ile ilgilidir ve bu paylaşım sayesinde kritik bir sürecin tek kişi tarafından kırılma olasılığı azaltılır. "En az ayrıcalık" ise kullanıcıların gereğinden fazla

yetkiyle donatılmamaları ve sorumlu oldukları işleri yapabilmeleri için yeterli olan asgari erişim yetkisine sahip olmaları demektir.

13. Kritik bir görevin tek kişiye bağımlılığını azaltmak ve aynı işi daha fazla sayıda çalışanın yürütebilmesini sağlamak amacıyla, bir sıra dâhilinde çalışanlara görev ve sorumluluk atanmalıdır. Böylece kritik bir iş birden fazla kişi tarafından öğrenilmiş olacaktır.

14. Çalışanlar kendi işleri ile ilgili olarak bilgi güvenliği sorumlulukları, riskler görev ve yetkileri hakkında periyodik olarak eğitilmelidir. Yeni işe alınan elemanlar içinde bu eğitim, oryantasyon sırasında verilmelidir.

PERSONEL VE EĞİTİM POLİTİKA

1. Eğitim stratejisi ile bilişim stratejisi birbiriyle aynı doğrultuda olmalıdır. Bu sayede bilişim stratejisinin başarılı bir şekilde uygulanması sağlanır.
2. Personelin sisteme tanımlanması ve yetkilerinin belirlenmesi işlemi yönetim tarafından onaylanmış bir prosedür dahilinde yapılmalıdır.
3. Kurum yapısı içinde yetki ve sorumluluklar açıkça tanımlanmış olmalıdır.
4. İşe alınan personel mevcut yapı ve güvenlik sistemleri hakkında bilgilendirilmelidir.
5. Kurum tarafından, bilişim sistemini kuran, geliştiren ve kullanan personelin görev tanımları yapılmış olmalıdır.
6. Personelin işe alınması, görev yerlerinin değiştirilmesi, görevlerine son verilmesi ve performanslarının değerlendirilmesinde güvenlik göz önünde bulundurulmalıdır.
7. Kurum çalışanları işin gerektirdiği vasıflara sahip olmalı, yeterli seviyede eğitim almalı ve yeteneklerine uygun işlerde çalıştırılmalıdır.
8. Bilişim alanında istihdam edilecek daimi personel ile sözleşmeli veya danışman olarak çalıştırılacak personelin seçiminde, bu kişilerin işin gerektirdiği öğrenim ve eğitimi almış yetenekli ve dürüst kişiler olmalarına azami dikkat gösterilmelidir.
9. 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.
10. Bilişim personelinin kurumun mevcut ve uzun vadeli politikaları ile paralellik gösteren bir şekilde sertifika programlarına katılımı ve sertifikasyonlarını tamamlaması gerekmektedir.
11. Görevlerin ayrılması bir kişinin diğer bir kişinin yaptığı faaliyetleri kontrol etme imkanı verecek şekilde olmalıdır.
12. Çalışanlar görev ve sorumluluklarının neler olduğunu bilmelidir.
13. Yönetim, kullanılan kontrollerin ne derecede etkin olduğunu değerlendirmelidir.

Uzaktan Erişim Yönetimi

1. Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahip olmalıdır.
2. İnternet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar VPN teknolojisini kullanmalıdırlar.
3. Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlamalıdır. VPN teknolojileri İpSec, SSL, VPDN, PPTP, L2TP vs. protokollerinden birini içermelidir.
4. Uzaktan erişim güvenliği sıkı şekilde denetlenmelidir. Kontrol İki yönlü şifreleme (Two-Factor password authentication) veya güçlü bir passphrase (uzun şifre) destekli public/private key sistemi kullanılması tavsiye edilmelidir. Daha fazlası için parola politikasına bakınız.
5. Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır. Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır. Mobile VPN ile uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile yapılmalıdır.
6. Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve anti virüs yazılımı güncellemeleri yapılmış olmalıdır.

7. Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.
8. Uzak erişim için kullanılacak olan servisler ve protokoller ön tanımlı olmalıdır.
9. Uzak erişim verilecek olan kullanıcılara sözleşmesine göre günlük saatlik izinler verilmelidir.
10. Sınırsız izin verilmekten kaçınılmalıdır. VPN ile erişecek olan kullanıcı VPN Erişim formunu doldurmak zorundadır.
11. Uzak erişim bağlantısında boşta kalma süresi (Herhangi bir işlem yapılmadığı takdirde connection time out süresi) kurumun ihtiyacına göre limitlenmelidir.

Firmalar için erişim Politikası

1.0 AMAÇ - KAPSAM

Bu politikanın amacı, firmaların herhangi bir yerden KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI.'nin bilgi sistemlerine erişmesine ilişkin normları belirlemektir.

Bu politika, KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI.uzaktan hizmet veren kişi veya kurumları kapsamaktadır.

2.0 POLİTİKA

Kurum ve firma arasında şifreli iletişim hatları kullanılacaktır; internet üzerinden kurumun herhangi bir yerindeki bilgisayara erişen kişi veya kurumlar VPN teknolojisini kullanacaklardır.

Uzaktan erişilen yer mutlaka statik IP ye sahip olmalı ve bu IP kurumun güvenlik cihazlarında tanımlanmış olmalıdır.

Firma uzaktankimlerin hangi rollerde kurum bilgisayarlarına eriştiğini belirtecek ve ayrıca ilgili kişilerin bilgisayarlara erşimde kullandığı kullanıcı adı ve şifreleri kurumdaki en üst yetkiliye teslim edecektir.

Kullanıcıların erişim şifrelerien az 4 ayda bir değiştirilecektir. Verilen şifreler kurumun şifreleme politikasına uygun olacaktır.

Firma, kurumun hiçbir bilgisini görüntüleyemez, ekran çıktısını alamaz, transfer edemez ve kurum dışına çıkartamaz. Aksi takdirde oluşacak yasal yükümlülüklerden firma sorumlu olacaktır.

Uzaktan erişim için mümkünse tek yönlü şifreleme veya güçlü bir uzun şifre destekli ppublic/private key sistemi kullanılması tavsiye edilmektedir.

Firma çalışanları hiçbir şekilde kendilerinin login şifrelerini aile bireyleri dahil olmak üzere hiç kimseye veremezler

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

Uzaktan bağlanan kişi makinasında zararlı kod, truva atı, vs. olduğundan şüpheleniyorsa bağlantıyı gerçekleştirmemlidir.

Uzaktan erişim yöntemi ile kuruma erişen bilgisayar ağında güvenlik tedbirleri alınmış olmalıdır.(örn, firewall, Domain altyapısı vs.)

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

Firma, periyodik olarak kullanıcı kimlikleri ve hesapları kontrol etmeli gereksiz kullanıcı kimlikleri ve hesapları kaldırılmalıdır.

Firma, kurum ile hassas veriye erişim hakkında gizlilik anlaşması imzalamalıdır.

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

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

Güvenlik açıklarını tespit etme politikası

1.0 AMAÇ – KAPSAM

Bu politikanın amacı, kurumun bilgisayar ağının (firewall, sunucu vs.) güvenlik açıklarına karşı taranması hususunda politikaların belirlenmesidir.
Denetim sebepleri aşağıdaki gibidir;

- Bilgi kaynaklarının bütünlüğü ve gizliliğini sağlamak
- Kurumun güvenlik politikalarına uyumunun kontrolü için güvenlik açıklarının tespit edilmesi
- Gerektiği zaman kullanıcıların veya sistemin aktivitelerini kontrol etmek

Bu politika, KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI. bünyesinde sahip olunan bütün bilgisayar ve haberleşme cihazlarını kapsamaktadır. Bu politika kurumun bünyesinde bulunan fakat kurumun sahip olmadığı herhangi bir sistemide kapsamaktadır. Denetim yapan kişi veya kurum hizmetlerin durdurulması aktivitesi yapmayacaktır.

2.0 POLİTİKA

İstenildiğinde denetim yapan firmanın bireylerine erişim izni verilecektir. Kurumun birimleri denetim yapan firmaya ağ taraması yapması için protokol, adres bilgileri, ağ bağlantıları hakkında bilgi verecektir.

2.1. Tarama esnasında muhatap olan kişi

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

2.2. Tarama Periyodu

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

2.3. Gizlilik Anlaşması

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

Sunucu Güvenliği Politikası

AMAÇ - KAPSAM

Bu politikanın amacı, KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI.' Nin sahip olduğu sunucularının temel güvenlik yapılandırması için standartları belirlemektir. Bu politikanın etkili kullanılması ile KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI.bünyesindeki bilgilere ve teknolojiye yetkisiz erişimler minimize edilecektir.

Bu politika, KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI.'nin sahip olduğu bütün dâhili sunucuları kapsamaktadır.

2.0 POLİTİKA

2.1. Sahip Olma ve Sorumluluklar

Kurum bünyesindeki bütün dâhili sunucuların yönetiminden sadece yetkilendirilmiş sistem yöneticileri sorumludur. Sunucu konfigürasyonları sadece bu gruptaki kişiler tarafından yapılacaktır.
Bütün sunucular (kurumun sahip olduğu) ilgili kurumun yönetim sistemine kayıt olmalı ve en az aşağıdaki bilgileri içermelidir.
Sunucuların yeri ve sorumlu kişi
Donanım ve işletim sistemi
Ana görevi ve üzerinde çalışan uygulamalar
İşletim sistemi sürümleri ve yamalar
Bütün bilgiler tek bir merkezde güncel olarak tutulmalıdır.

2.2. Genel Konfigurasyon Kuralları

İşletim sistemi konfigurasyonları kurumun bilgi işlem biriminin talimatlarına göre yapılacaktır.
Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
Active directory de 1 hafta süreyle loglanacaktır. (IP bazlı)
Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (IPSEC, SSL,VPN) üzerinden yapılmalıdır.
Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdırlar.

2.3. Gözlemleme

1. Kritik sistemlerde oluşan bütün güvenlikle ilgili olaylar loglanmalı ve aşağıdaki şekilde saklanmalıdır.
    - Active directory IP bazlı olarak bir hafta süreyle erişilebilmelidir.

- Önem derecesine göre exchange veritabanı haftalık, müşteri kaynak kodları haftalık, tüm kaynak kodları database günlük, iletşim sistemleri günlük alınır ve 15 gün saklanır.
- Aylık full backuplar en az 1 yıl tutulmalıdır.

2. Güvenlikle ilgili loglar sorumlu kişi tarafından değerlendirilecek ve gerekli tedbirleri alacaktır. Güvenlikle ilgili olaylar aşağıdaki gibi olabilir fakat bunlarla sınırlı değildir.
    - Yetkisiz kişilerin ayrıcalıklı hesaplara erişmeye çalışması
    - Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar

2.4. Uygunluk

Denetimler yetkili organizasyonlar tarafından kurum bünyesinde belli aralıklarda yapılmalıdır.

Denetimlerde kurumun işleyişine zarar vermemesi için maksimum gayret gösterilecektir.

2.5. İşletim

Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir.
Sunucuların yazılım ve donanım bakımları 2 aylık sürelerde, sistem yöneticileri tarafından yapılmalıdır.
Sistem odalarına yetkisiz girişler engellenmelidir. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı.

Temiz Masa Temiz Ekran Politikası

Bu politika, KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI. bünyesindeki kâğıtlar, taşınabilir depolama ortamları ve kişisel bilgisayar için mesai saatleri içinde ve dışında bilgiye yetkisiz erişim ve bilginin hasar görmesi gibi riskleri azaltmak amacıyla gerekli olan şartları tamamlamak amacıyla hazırlanmıştır.

2. Kapsam:

Bu politika, KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI. bünyesinde çalışan tüm personelleri kapsamaktadır.

3. Tanımlar:

Bu politikada geçen;
Hassas Bilgi: Yönetimin isteği dışında açığa çıkması ile kuruma ciddi maddi ve manevi zararlar verebilecek verileri
Sınıflandırılmış Bilgi: Bilgilerin gizlilik derecelerine göre (gizli, çok gizli vs.) sınıflandırılmasını,
Windows + L: Windows işletim sistemlerinde bilgisayarın kilitli konuma getirmeyi yarayan, klavyede yer alan Windows simgeli tuş ile L tuşunun birlikte kullanımı
Taşınabilir Medya: CD, DVD, USB Disk, USB Bellek vb. aygıtları
Mobil Cihaz: Özel bir işletim sistemi ile kullanılmakta olan dizüstü bilgisayarları, tablet bilgisayarları, masaüstü bilgisayarları, ifade eder.

4. Politika Metni:

- Tüm bilgisayar oturumları parola korumalı olup, bilgisayar boş kaldığında 3 (üç) dakika içinde otomatik kilitlenir.
- Çalışma saatleri dışında bilgisayarlar kapalı tutulmalıdır.
- Çalışma saatleri içerisinde bilgisayar başından ayrılırken bilgisayarlar mutlaka kilitli bırakılmalıdır. Bunun için Windows işletim sisteminde Windows +L tuşları kısayol olarak kullanılabilir.
- Bilgisayar gibi elektronik ortamlarda bulunan bilginin korunması için çalışma saatleri dışında ofis kapılarının kilitli tutulmalıdır.
- Bilgisayar ekranları ve klavyeler kullanıcı haricindeki kişilerin göremeyeceği şekilde konumlandırılmalıdır.
- Taşınabilir medya ve mobil cihazlar daima kullanıcısının yanında bulundurulur. Kullanılmadığı durumlarda mutlaka kilitli dolaplarda muhafaza edilir.
- Masa üstlerinde KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI. e ait özel nitelikli kişisel veriler ve kişisel veriler kullanım haricinde bulundurulamaz.
- Kişisel gizli bilgiler başkaları tarafından fark edilmeyecek şekilde muhafaza edilmelidir.
- Hassas ve sınıflandırılmış bilgi uzak ağ yazıcılarından yazdırılamaz. Uzak yazıcılardan yazdırma yapılacak ise korumalı yazdırma özelliği kullanılır.
- Yazıcı ve fotokopi cihazlarının belleğinde kayıtlı bulunan hassas ve sınıflandırılmış bilgiler silinmelidir.

Kısa süreli ayrılmalarda dahi, cep telefonu, taşınabilir bellek, harici hard disk, CD, DVD gibi eşyalar çalışma masası üzerinde bırakılmamalıdır.

Veritabanı güvenlik politikası

AMAÇ -KAPSAM

Bu politikanın amacı, KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI.veritabanı sistemlerinin kesintisiz ve güvenli şekilde işletilmesine yönelik standartları tanımlamaktır. Kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) loglanmalıdır. Log kayıtlarına idarenin izni olmadan kesinlikle hiçbir şekilde erişim yapılamamalıdır. Manyetik kartuş DVD veya CD ortamlarında tutulan log kayıtları en az 5 yıl süre ile güvenli ortamlarda saklanmalıdır. Veritabanı sunucularının güvenliği hakkında daha detaylı bilgi ve uyulması gereken kurallar aşağıda belirtilmiştir.

Tüm veritabanı sistemleri bu politikaların kapsamı altında yer alır.

2.0 POLİTİKA

- Veritabanı sistemleri envanteri ve bu envanterden sorumlu personel tanımlanmalı ve dokümante edilmelidir.
- Veritabanı işletim kuralları belirtilmeli ve ve dokümante edilmelidir.
- Veritabanı sistem logları tutulmalı ve gerektiğinde idare tarafından izlenmelidir.
- Veritabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli alınması kontrol altında tutulmalıdır.
- Yedekleme planları dokümante edilmelidir.
- Veritabanı erişim politikaları “Kimlik Doğrulama ve Yetkilendirme” politikaları çerçevesinde oluşturulmalıdır.
- Hatadan arındırma, bilgileri yedekten dönme kuralları “Acil Durum Yönetimi” politikalarına uygun olarak oluşturulmalı ve dokümante edilmelidir.
- Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.
- Veritabanı sistemlerinde oluşacak problemlere yönelik bakım onarım çalışmalarında yetkili bir personel bilgilendirilmelidir.
- Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulmalı ve sonrasında ilgili uygulama kontrolleri gerçekleştirlmelidir.
- Bilgi saklama medyaları kurum dışına çıkartılmamalıdır.
- Sistem dokümantasyonu güvenli şekilde saklanmalıdır.
- İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için temas edilecek kişiler belirlenmelidir.
- Veritabanı sunucu sadece ssh, ssl, rdp veritabanının orijinal yönetim yazılımına açık olmalı, bunun dışında ftp, telnet vb. gibi açık metin şifreli bağlantılara kapalı olmalıdır. Ancak ftp ,telnet clear text bağlantılar veritabanı sunucudan dışarıya yapılabilir.
- Application Serverlardan veritabanına rlogin vb. şekilde erişememelidir.
- Veritabanı sunucularına erişim şifreleri kapalı bir zarfta imzalı olarak kurumun kasasında saklanmalı ve gereksiz yere açılmamalıdır. Zarfın açılması durumunda firma yetkilileride bilgilendirilmelidir
- Arayüzden gelen kullanıcılar bir tabloda saklanmalı bu tablodaki kullanıcı adı ve şifreleri şifrelenmiş olmalıdır.
- Veritabanı sunucusuna ancak zorunlu hallerde root veya admin olarak bağlanılmalı. Root veya admin şifresi tanımlanmış kişi /kişilerde olmalıdır.
- Bağlanacak kişilerin kendi adına kullanıcı adı verilecek yetkilendirme yapılacaktır.
- Bütün kullanıcıların yaptıkları işlemler loglanmalıdır.
- Veritabanı yöneticiliği yetkisi sadece bir kullanıcıda olmalıdır.
- Veritabanında bulunan farklı Schemaların kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişmesi engellenmelidir.
- Veritabanı sunucularına internet üzerinden erişimlerde VPN gibi güvvenli bağlantılar tesis edilmelidir.
- Veritabanı sunucularına ancak yetkili kullanıcılar erişmelidir.
- Veritabanı sunucularına kod geliştirien kullanıcı dışında hiçbir kullanıcı bağlanıp sorgu yapamamalıdır. İstekler arayüzden sağlanmalıdır.
- Veritabanı sunucularına giden veri trafiği mümkünse şifrelenmelidir.
- Bütün şifreler düzenli aralıklarla değiştirilmelidir.
- Veritabanı sunucuları için yukarıda bahsedilen ve uygulanabilen güvenlik kuralları uygulama sunucuları içinde geçerlidir.

Vpn Politikası

Bu politikanın amacı, KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI. 'e ait Sanal Özel Ağ(VPN) protokolünün kullanımı hakkında standartlarını belirlemektir.

Bu politika Sanal Özel Ağ(VPN) ile KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI.ağına bağlanacak kurumları, çalışanları, sözleşmelileri, danışmanları, geçici çalışanları ve diğer bütün personeli kapsamaktadır. Bu politika VPN bağlantılarının sonlandırıldığı ürünlere uygulanacaktır.

1.0 POLİTİKA

KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI. yetkili çalışanları ve üçüncü şahıslar, Sanal Özel Ağ(VPN)ıin faydalarından yararlanabilirler. Kullanıcılar herhangi bir internet servis sağlayıcısını seçmekte serbesttirler.
Buna ek olarak,

- VPN kullanım hakkı verilen kişiler yetkisiz kişilere bu hakkı kullandırmaması için gerekli tedbirleri almakla sorumludur.
- Kurum ağına bağlanıldığında, PC'den çıkan ve giren trafik sadece VPN kanalından iletilecektir ve diğer bütün trafik düşecektir.
- Çift tünel sistemine izin verilmemektedir; sadece tek ağ bağlantısına izin verilmektedir.
- Kurumun VPN ağ geçitlerinin kurulması ve yönetimi yetkili personel tarafından yapılacaktır.
- Kuruma ait bilgisayarlara sahip olmayan kişiler KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI.'nin VPN ve ağ politikalarına uygun bir şekilde cihazlarını konfigure etmelidirler.
- Sadece kurumun onay verdiği kullanıcılar VPN'i kullanabilir.
- VPN teknolojisini kendi kişisel cihazları ile kullanan kişiler şunu bilmelidirler ki, bütün makineler kurum ağının bir parçasıdır bundan dolayı KEY MUHENDISLIK PROJE VE TAAH. TIC. LTD. STI 'insorumlu olduğu cihazlar ile aynı kurallara sahiptir ve aynı güvenlik politikaları ile konfigure edilmelidir

Bilgi sistemleri Yedekleme Politikası

1. Bilgi sistemlerinde oluşabilecek hatalar karşısında; sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigurasyon,sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmesi gerekmektedir.
2. Verinin operasyonel ortamda online olarak aynı disk sisteminde farklı disk volumlerinde yedekleri alınmalıdır.
3. Taşınabilir ortamlar fiziksel olarak bilgi işlem odalarından farklı odalarda ve güvenli bir şekilde saklanmalıdır.
4. Bu konuyla ilgili sorumluluklar tanımlanmalı ve atamalar yapılmalıdır.Yedekeleri alınacak sistem, dosya ve veriler dikkatle belirlenmeli ve yedeği alınacak sistemleri belirleyen bir yedekleme listesi oluşturulmalıdır.Yedek ünite üzerinde gereksiz yer tutmamak üzere, kritiklik düzeyi düşük olan veya sürekli büyüyen izleme dosyaları yedekleme listesine dahil edilmemelidir.
5. Yedeklenecek bilgiler değişiklik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilmeli ve güncellenmelidir.
6. Yeni sistem ve uygulamalar devreye alındığında yedekleme listeleri güncellenmelidir.
7. Yedekleme işlemi için geçerli sayı ve kapasitede yedek üniteler seçilmeli ve temin edilmelidir.
8. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilmelidir.Yedekleme ortamlarının düzenli periyotlarda test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanmalıdır.
9. Geri yükleme prosedürlerinin düzenli olarak kontrol ve test edilerek etkinliklerinin doğrulanması ve operasyonel prosedürlerin öngördüğü süreler dahilinde tamamlanabileceğinden emin olunması gerekir.
10. Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanmalıdır.
11. Yedekleme standardı ile doğru ve eksiksiz yedek kayıt kopyalarının bir felaket anında etkilenmeyecek bir ortamda bulundurulması gerekmektedir.