RTSO

BİLGİ GÜVENLİĞİ

POLİTİKASI

HAZIRLAYAN/KALİTE YÖNETİM TEMSİLCİSİ	ONAYLAYAN/GENEL SEKRETER

İÇİNDEKİLER

HAZIRLAYAN/KALİTE YÖNETİM TEMSİLCİSİ	ONAYLAYAN/GENEL SEKRETER

ÖNSÖZ

Kurumsal bilgi güvenliğini tehdit eden saldırıların bilinmesi, bilgi güvenliğinin sağlanmasına yönelik kurumsal stratejilerin geliştirilmesinde önemli bir role sahiptir. Bilgi sistemlerine yönelik olarak yapılan saldırılar incelendiğinde; saldırıların çok geniş bir yelpazede yapıldığı, e-posta ve anlık mesajlaşma yoluyla gelen tehditlerin yanı sıra, web 'de de ciddi bir tehdit unsurunun varlığı bilinmektedir. Günümüzde e-posta ve web tehditlerinin birleşmesiyle çok zararlı ve bulaşıcı virüsler doğmaktadır.

Elektronik ortamın doğasında var olan güvensizlik unsuru, elektronik ortamlardaki uygulamaları tehdit eden en büyük unsurdur. Geçmiş yıllarda saldırılar, yaygın ve hedef gözetmeksizin yapılmaktayken artık nokta hedefi gözeten ve bölgesel olarak düzenlenen saldırılar yapılmaktadır.

Son yıllarda bilgi ve bilgisayar güvenliğini sekteye uğratmaya hatta yıkmaya çalışan, kurumlar üzerinde maddi manevi büyük kayıplara yol açan, kişi, kurum ve kuruluşları tehdit ederek zararlara uğramasına yol açan bilgi güvenliği tehditlerinin engellenmesi için kurumsal bilgi güvenliği sağlanmalıdır. Kurumsal Bilgi güvenliği standartlarının yüksek seviyede bir güvenlik sağlanmasında etkili olduğu muhakkaktır. Bunun ötesinde de sistemlerde açıklar olabileceği, özellikle web uygulamalarında daha dikkatli olunması gerektiği, yeni eğilim ve yaklaşımların keşfedildikçe kurumsal güvenliğinin arttırılması yönünde hayata geçirilmesi gerektiği de asla unutulmamalıdır.

Elektronik platformlar dünyada ve ülkemizde her geçen gün hızla yaygınlaşmakta, ticari ve günlük yaşantımızdaki varlığını hissedilir oranda arttırmaktadır. Kurumsal bilgi güvenliğinin sağlanması amacıyla, saldırı türlerinin takip edilmesi, saldırganların kullandığı yöntemlerin saptanması, ülkemizde ve dünyada bu konuda yapılan araştırmalar, raporlar ve çalışmalar ile tespit edilen açıkların takip edilmesi ve giderilmesi bilgi güvenliği ihlalinin yaşanmaması için gerekli önlemlerin zamanında alınması, güvenlik ihlallerine anında müdahale edilerek saldırı zararlarından en az şekilde etkilenme, felaket anında uygulanabilecek felaket ve iş sürekliliği planlarının uygulanması gibi stratejiler, kurumlar tarafından oluşturularak, bilgi güvenliğinin sağlanması, bu tür saldırıların ve tehditlerin önüne geçilmesi elzemdir.

Şaban Aziz KARAMEHMETOĞLU
RTSO Yönetim Kurulu Başkanı

HAZIRLAYAN/KALİTE YÖNETİM TEMSİLCİSİ	ONAYLAYAN/GENEL SEKRETER

MİSYON

Üye memnuniyetinin ön planda tutulduğu kalite yönetim anlayışı ile 5174 sayılı kanun, buna bağlı yönetmelikler ve genel etik çerçevesinde, katılımcı, yeniliğe açık yaklaşımı ile üyelerine ve şehrine değer katan projeler yapan, hizmet kalitesini sürekli geliştiren, girişimcilik, markalaşma ve kurumsallaşmayı destekleyen, ulusal ve uluslararası ticari fırsatlar oluşturan dinamik ve şeffaf bir kurum olmak ve bu ilkeler doğrultusunda hizmet vermek.

VİZYON

Paydaşlarımızdan aldığımız güç ve destek ile ilimiz ve ülkemizi uluslararası ticaretten daha fazla pay alan, küresel boyutlardaki siyasi ve ekonomik oluşumları kendi yararları doğrultusunda yönlendirebilen ve üyelerin rekabet gücünü arttıran bölgesel bir güç ve model olmak

KALİTE POLİTİKASI

Rize Ticaret ve Sanayi Odası olarak; üyelerimize yerel, ulusal ve uluslararası alanlarda hizmet sunarken, müşterilerin ihtiyaç ve beklentilerine öncelik vererek, hızlı, doğru, tarafsız, güler yüzlü ve müşteri odaklı davranış biçimi ile çoğulcu, katılımcı ve aktif yönetim anlayışını benimseyerek, ekip ruhunu teşvik etmek, kolektif çalışma bilincini oluşturmak. Sürekli iyileştirmeye açık, üyeleri, organları, personeli ve paydaşları ile işbirliği içinde, güçlü, daima yol gösteren bir kurum olmak.

HAZIRLAYAN/KALİTE YÖNETİM TEMSİLCİSİ	ONAYLAYAN/GENEL SEKRETER

1. BİLGİ SİSTEMLERİNİN GENEL KULLANIM POLİTİKASI

1. 1 Genel Bakış

Rize Ticaret ve Sanayi Odası'nın amacı herhangi kimse üzerinde kısıtlayıcı politikalar üretmek değil, aksine açıklık, güven ve bütünlüğe yönelik kültürü yerleştirmektir. Kurum, bilerek veya bilmeyerek yapılan yasadışı veya zararlı eylemlerine karşı çalışanların ve Kurumun haklarını korumaya adanmıştır. Bilişim ile alakalı sistemler (bilgisayar, yazılım, işletim sistemleri, kayıt cihazları, e-mail, *sms, kayıtlı elektronik posta (kep) sosyal hesaplar*, www, ftp vs) Kurumun sahip olduğu değerlerdir. Güçlü bir güvenlik bütün çalışanların içerisine dâhil olduğu takım çalışmasıyla oluşturulabilir. Bütün bilgisayar kullanıcıları günlük aktivitelerini yerine getirebilmesi için bu kuralları iyi bilmeli ve uygulamanın sorumluluğunu taşımalıdır.

1. 2 Amaç

Bu politikanın amacı Rize Ticaret ve Sanayi Odası'nın bünyesindeki bilişim cihazlarının uygun kullanımı hakkında taslak oluşturmaktır. Uygunsuz kullanım Kurumu virüs saldırılarına, ağ sistemlerinin çökmesine, hizmetlerin aksamasına, *kurumsal bilginin güvenliğinin saldırıya uğramasına* sebep olabilir ve bunlar yasal yaptırımlara dönüşebilir.

1. 3 Kapsam

Bu politika Kurumun bütün çalışanları (sözleşmeli/kadrolu), yöneticileri, Kurum ile işbirliği içerisinde çalışan herkes için geçerlidir.

Politika

Güvenli olmayan servis ve protokoller daha güvenli olan servis ve protokoller ile değiştirilmelidir.

1. 4 Genel Kullanım ve Sahip Olma

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

Çalışanlar bilgi sistemlerinden, kendi kişisel kullanımı için makul seviyede yararlanabilirler. Her bir departman kendi bilgi sistemlerinin kişisel kullanımı için gerekli kuralları koymalıdır. Departmanlar böyle bir kural koymamış ise Kurumun koyduğu genel güvenlik politikaları geçerlidir.

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

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

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

Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/ kopyalanmamalıdır.

Bilgisayarlar üzerinden resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.

Kurum Bilgi İşlem biriminin bilgisi olmadan Kurum ağ sisteminde (web hosting servisi, e-posta servisi vb.) sunucu nitelikli bilgisayar bulundurulmamalıdır.

Birimlerde sorumlu bilgi işlem personeli ve ilgili teknik personel bilgisi dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vb. veriler hiçbir surette değiştirilmemelidir.

Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir.

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

1. 5 Güvenlik ve Kişiye Ait Bilgiler

Bilgi sistemlerinde bulunan kritik bilgilere yetkisiz kişilerin erişimini engellemek için gerekli erişim hakları tanımlanmalıdır. *Bu nedenle kullanıcı adı ve şifreleri bulunmaktadır.*

Şifreleri güvenli bir şekilde tutun ve hesabınızı başka kimselerle paylaşmayın.

Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmalıdır.

Laptop bilgisayarın çalınması/kaybolması durumunda, durum fark edildiğinde en kısa zamanda Genel Sekreterliğe haber verilmelidir.

Çalışanlar bilinmeyen kimselerden gelen dosyaları açarken çok dikkatli olmalıdırlar. Çünkü bu mailler virüs, e-mail bombaları ve Truva atı gibi zararlı kodları içerebilirler.

Bütün kullanıcılar ağın kaynaklarının verimli kullanımı konusunda dikkatli olmalıdırlar. E-posta, *Kayıtlı Elektronik Posta (Kep) ile gönderilen verilerin sadece ilgili kullanıcılara gönderildiğinden emin olunmalıdır.*

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

1. 6 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 aktivitede bulunamaz.

Sistem ve Ağ Aktiviteleri

Aşağıdaki aktiviteler hiçbir istisna olmadan kesinlikle yasaklanmıştır.

Herhangi bir kişi veya kurumun izinsiz kopyalama, ticari sır, patent veya diğer kurum bilgileri, yazılım lisanları vs. haklarını çiğnemek.

Kitapların izinsiz kopyalanması, magazinlerdeki fotoğrafların dijital formata dönüştürülmesi, lisan gerektiren yazılımların kopyalanması.

Zararlı programların (örnek, virus, solucan, Truva atı, e-mail bombaları vs) ağa veya sunuculara bulaştırılması.

Kendi hesabınızın şifresini başkalarına vermek veya kendi hesabınızı kullandırmak.

Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışmak.

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

Kurum bilgilerini Kurum dışından üçüncü şahıslara iletmek.

Cihaz, yazılım ve verinin izinsiz olarak kurum dışına çıkarılması, kurumun politikaları olarak belirlediği programlar dışında kaynağı belirsiz olan programları (Dergi CD'leri veya internetten indirilen programlar vs) kurmak ve kullanmak yasaktır.

E-mail ve Haberleşme Aktiviteleri

Kurum dışından güvenliğinden emin olunmayan bilgisayarlardan web sayfası, e-posta, kep, sosyal hesaplar, toplu sms sitemlerine giriş yapmak.

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

E-posta, *toplu sms, sosyal hesapların* başlık bilgilerini yetkisiz kullanmak veya değiştirmek.

İş ile alakalı olmayan iletileri *üçüncü kişilere iletmek.*

2. AĞ CİHAZLARI GÜVENLİK POLİTİKASI

2. 1 Amaç

Bu doküman Rize Ticaret ve Sanayi Odasının ağındaki yönlendirici (router) ve anahtarların (switch) sahip olması gereken minimum güvenlik konfigürasyonlarını tanımlamaktadır.

2. 2 Kapsam

Kurumun ağına bağlı olan ağ cihazları için geçerlidir.

2. 3 Politika

Bütün yönlendirici ve anahtarlar aşağıdaki konfigürasyon standartlarına sahip olmalıdır:

-Mümkün olduğunca yerel kullanıcı hesapları açılmamalıdır.

-Yönlendiriciye erişen yasal veya yasadışı kullanıcıları uyarmalıdır.

-Her bir yönlendirici ve anahtar aşağıdaki uyarı yazısına sahip olmalıdır.
"Bu cihaza erişim ve konfigürasyon için yasal hakkınız olmak zorundadır. Bu cihazla yapılan her şey loglanabilir, bu politikaya uymamak disiplin kuruluna sevk ile sonuçlanabilir veya yasal yaptırım olabilir."

3. VERİTABANI GÜVENLİK POLİTİKASI

3. 1 Amaç

Rize Ticaret ve Sanayi Odası'nın veri tabanı sistemlerinin kesintisiz ve güvenli şekilde işletilmesine yönelik standartları tanımlar. Kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) loglanmalıdır. Log kayıtlarına Yönetimin izni olmadan kesinlikle hiçbir şekilde erişim yapılmamalıdır. Manyetik kartuş, DVD veya CD ortamlarında tutulan log kayıtları en az 5 (beş) yıl süre ile güvenli ortamlarda saklanmalıdır. Veri tabanı sunucularının güvenliği hakkında daha detaylı bilgi ve uyulması gereken kurallar aşağıda belirtilmiştir.

3. 2 Kapsam

Tüm veri tabanı sistemleri bu politikaların kapsamı altında yer alır.

3. 3 Politika

-Veri tabanı sistemleri envanteri ve bu envanterden sorumlu personel tanımlanmalı ve dokümante edilmelidir.
-Veri tabanı işletim kuralları belirlenmeli ve dokümante edilmelidir.
-Veri tabanı sistem logları tutulmalı ve gerektiğinde Yönetim tarafından izlenmelidir.
-Veri tabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli alınması kontrol altında tutulmalıdır.
-Veri tabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmalarında yetkili bir personel bilgilendirilmelidir.
-Güncelleme çalışmaları yapılmadan önce bildirimde bulunulmalı ve sonrasında ilgili uygulama kontrolleri gerçekleştirilmelidir.
-Bilgi saklama materyalleri Kurum dışına çıkartılmamalıdır.

-Sistem dokümantasyonu güvenli şekilde saklanmalıdır.
-Veri tabanı 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.
-Veri tabanı yöneticiliği yetkisi sadece bir kullanıcıda olmalıdır.
-Veri tabanı sunucuları için yukarıda bahsedilen ve uygulanabilen güvenlik kuralları uygulama sunucuları içinde geçerlidir.

4. İNTERNET ERİŞİM VE KULLANIM POLİTİKASI

4. 1 Amaç

İnternet'in uygun olmayan kullanımı, Kurumun yasal yükümlülükleri, kapasite kullanımı ve Rize Ticaret ve Sanayi Odası'nın imajı açısından istenmeyen sonuçlara neden olabilir.

Bilerek ya da bilmeyerek bu türden olumsuzluklara neden olunmaması ve internetin kurallarına, etiğe ve yasalara uygun kullanımının sağlanmasını amaçlamaktadır.

4. 2 Kapsam

Bu politika Rize Ticaret ve Sanayi Odası'nda bulunan bütün kullanıcıları kapsamaktadır.

4. 3 Politika

Kurumun bilgisayar ağı, erişim ve içerik denetimi yapan bir firewall üzerinden internete 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 erişimin denetimi burada yapılır. Güvenlik duvarı aşağıda belirtilen hizmetlerle birlikte çalışarak ağ güvenliğini sağlayabilmelidir.

Kurumun ihtiyacı doğrultusunda içerik filtreleme sistemleri kullanılmalıdır. İstenilmeyen siteler yasaklanabilmelidir.

Kurumun ihtiyacı doğrultusunda Saldırı Tespit ve Önleme Sistemleri kullanılmalıdır. Şüpheli olayları, nüfuz ve saldırıları tespit etmeyi hedefleyen bir sistemdir. IPS, şüpheli durumlarda e-posta veya SMS gibi yöntemlerle sistem yöneticisini uyarabilmektedir.

Anti-virüs gateway sistemleri kullanılmalıdır. İnternete giden veya gelen bütün trafik virüslere karşı taranmalıdır.

Ancak Yetkilendirilmiş Sistem Yöneticileri internete çıkarken bütün servisleri kullanma hakkına sahiptir.

Bilgisayarlar arası ağ üzerinden resmi görüşmeler haricinde, mesajlaşma ve sohbet programları gibi Programlarının kullanılmamalı, bu Chat programları üzerinden dosya alışverişinde bulunulmamalıdır.

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

Bilgisayarlar üzerinden genel ahlak anlayışına aykırı Internet sitelerine girilmemeli ve dosya indirimi yapılmamalıdır.

İnternet üzerinden Kurum tarafından onaylanmamış yazılımlar indirilemez ve Kurum sistemleri üzerine bu yazılımlar kurulamaz. Kurumsal işlevlere yönelik yazılım ihtiyaçları için ilgili prosedürler dâhilinde ilgili birim sorumlularına müracaat edilmesi gerekmektedir.

Üçüncü şahısların Kurum internetini kullanmaları Genel Sekreterliğin izni ve bu konudaki kurallar dâhilinde gerçekleştirilebilecektir.

5. AĞ YÖNETİMİ POLİTİKASI

5. 1 Amaç

Rize Ticaret ve Sanayi Odası'nın bilgisayar ağında yer alan bilgilerin ve ağ altyapısının güvenliği, gizlilik, bütünlük ve erişilebilirlik 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 amacıyla geliştirilmiştir.

5. 2 Kapsam

Kurum bilgisayar ağının sistem ve ağ yöneticileri, teknik sorumluları faaliyetlerini Ağ Yönetimi Politikasına uygun şekilde yürütmekle yükümlüdür.

5. 3 Politika

-Ağın kontrol edeceği alan belirlenmelidir.
-Bilgisayar ağları işletme sorumlulukları bilgisayarların işletmesinden mümkünse ayrılmalıdır.
-Gerek duyuluyorsa şube şebekeleri üzerinden geçen datanın gizliliği ve doğruluğunu garanti etmek ve kendisine bağlı bilgisayar sistemlerini korumak için özel kontroller uygulanmalıdır.
-Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için özel kontroller uygulanmalıdır.
-Ağ servisleriyle ilgili standartlarda, erişimine izin verilen ağlar ve ağ servisleri ve ilgili yetkilendirme yöntemleri belirtilmelidir.
-Ağ üzerinde kullanıcının erişeceği servisler kısıtlanmalıdır.
-Gerek görülen uygulamalar için, portların belirli uygulama servislerine veya güvenli ağ geçitlerine otomatik olarak bağlanması sağlanmalıdır.
-Sınırsız ağ dolaşımı engellenmelidir.
-Harici ağlar üzerindeki kullanıcıları belirli uygulama servislerine veya güvenli ağ geçitlerine bağlanmaya zorlayıcı teknik önlemler alınmalıdır.
-İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden teknik önlemler alınmalıdır,
-Ağ bağlantıları periyodik olarak kontrol edilmelidir.
-Gerek görülen uygulamalar için elektronik posta, tek yönlü dosya transferi, çift yönlü dosya transferi, etkileşimli erişim, güne ve günün saatine bağlı erişim gibi uygulama kısıtlamalarıyla ağ erişimi denetimi yapılmalıdır,
-Ağ üzerindeki yönlendirme kontrol edilmelidir.
-Bilgisayar ağına bağlı bütün makinelerde kurulum ve konfigürasyon parametreleri Kurumun güvenlik politika ve standartlarıyla uyumlu olmalıdır,

-Sistem tasarım ve geliştirmesi yapılırken Kurum tarafından onaylanmış olan ağ ara yüzü ve protokolleri kullanmalıdır, internet trafiği Erişim ve Kullanımı İzleme Politikası ve ilgili standartlarda anlatıldığı şekilde izlenebilecektir.

6. ŞİFRE POLİTİKASI

6 .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. Kurum çalışanları ve uzak noktalardan erişenler aşağıda belirtilen kurallar dâhilinde şifreleme yapmakla sorumludurlar.

6.2 Amaç

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

6 .3 Kapsam

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

6.4 Genel

Bütün sistem seviyeli şifreler en az üç ayda bir değiştirilmelidir.

Bütün kullanıcı seviyeli şifreler en az altı ayda bir değiştirilmelidir.

Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.

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

Kullanıcı, şifresini başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlara yazmaması konusunda *bilgilendirilmelidir.*

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

Şifrelerin ilgili kişiye gönderilmesi "kişiye özel" olarak yapılmalıdır.

Bir kullanıcı adı ve şifresinin birim zamanda birden çok bilgisayarda kullanılmamalıdır.

6 .5 Bütün kullanıcı ve sistem seviyeli şifrelemeler aşağıdaki ana noktalara uymalıdır:

Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.

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

Kullanıcı, şifresini başkası ile paylaşmaması, kağıtlara ya da elektronik ortamlara yazmaması konusunda eğitilmelidir.

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

Şifrelerin ilgili kişiye gönderilmesi "kişiye özel" olarak yapılmalıdır.

Bir kullanıcı adı ve şifresinin birim zamanda birden çok bilgisayarda kullanılmamalıdır.

Bütün kullanıcı ve sistem seviyeli şifrelemeler “6 .6 Genel Şifre Oluşturma Kuralları” başlığı altındaki hususlara uymalıdır.

6 .6 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.

Şifre Koruma Standartları

Kurum bünyesinde kullanılan şifreleri Kurum dışında herhangi bir şekilde kullanmayınız, değişik sistemler için farklı şifreleme kullanınız. Kurum bünyesinde kullanılan şifreleri herhangi bir kimseyle paylaşmayınız. Bütün şifreler Kuruma ait gizli bilgiler olarak düşünülmelidir.

Uzaktan Erişen Kullanıcılar için Şifre Kullanımı

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

7. E-POSTA POLİTİKASI

7 .1 Amaç

Bu politikanın amacı, Rize Ticaret ve Sanayi Odası'nın e-posta altyapısına yönelik kurallarını ortaya koymaktır. Kurumda oluşturulan e-postalar, kurumsal bir kimlik taşımaktadırlar. E-posta, Rize Ticaret ve Sanayi Odası'nın 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.

7 .2 Kapsam

Bu politika RTSO'da oluşturulan e-postaların doğru kullanımını içermektedir ve bütün çalışanları kapsamaktadır.

7 . 3 Yasaklanmış Kullanım

Kurumun e-posta sistemi, taciz, suiistimal 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.

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

Kurumla ilgili olan hiçbir gizli bilgi, gönderilen mesajlarda yer alamaz. Bunun kapsamına içerisine iliştirilen öğeler de dâhildir.

Kişisel kullanım için Internet'teki sitelere üye olunması durumunda Kuruma ait e-posta adresleri kullanılmamalıdır.

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

7. 4 Kişisel Kullanım

Kurum çalışanlarının kişisel amaçlar için e-posta kullanımı mümkün olduğunca makul seviyede olmalıdır. Ayrıca iş dışındaki e-postalar farklı bir klasör içerisinde saklanmalıdır.

Kurum personeli tarafından Internet ortamı aracılığı ile iletilen her türlü kişisel e-posta mesajının altında, Kurum tarafından belirlenen "gizlilik notu" ve "sorumluluk notu" bilgileri yer almalıdır. Bu bilgiler, e-posta iletisinin içeriğinden ve niteliğinden Kurumun sorumlu tutulamayacağı gibi açıklamalar içermelidir.

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

Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-maillerin sahte e-mail olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.

Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve Kurumsal mesajları cevaplandırmalıdırlar.

Kurum çalışanları Kurumsal e-postaların Kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesi ve okunmasını engellemekten sorumludurlar.

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

Elektronik postaların sık sık gözden geçirilmesi, gelen mesajların uzun süreli olarak genel elektronik posta sunucusunda bırakılmaması gerekmektedir.

Gözlemleme

Kurum çalışanları gönderdikleri, aldıkları veya sakladıkları e-maillerde kişisellik aramamalıdır. Bu yüzden yetkili kişiler önceden haber vermeksizin e-mail mesajlarını denetleyebilirler.

E-Posta Yönetimi

Kurum e-postaların kendi bünyesinde güvenli ve başarılı bir şekilde iletilmesi için gerekli yönetim ve alt yapıyı sağlamakla sorumludur.

E-Posta Virüs Koruma

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

8. SUNUCU GÜVENLİK POLİTİKASI

8. 1. Amaç

Bu politikanın amacı RTSO sahip olduğu sunucularının temel güvenlik konfigürasyonları için standartları belirlemektir. Bu politikanın etkili uygulanmasıyla Kurum bünyesindeki bilgilere ve teknolojiye yetkisiz erişimler minimize edilecektir.

8. 2 Kapsam

Bu politika Kurumun sahip olduğu bütün dahili sunucular için geçerlidir.

8. 3 Sahip Olma ve Sorumluluklar

Rize Ticaret ve Sanayi Odası'nın bünyesindeki bütün dahili sunucuların yönetiminden yetkilendirilmiş sistem yöneticileri sorumludur. Sunucu konfigürasyonları sadece bu gruptaki kişiler tarafından yapılacaktır. Bütün sunucular (Kurumun sahip olduğu) ilgili Kurumun yönetim sistemine kayıt olmalıdır. Bütün bilgiler tek bir merkezde (ana bilgisayarda) güncel olarak tutulmalıdır.

8.4 Genel Konfigürasyon Kuralları

İşletim sistemi konfigürasyonları Kurumun Bilgi İşlem Biriminin talimatlarına göre yapılacaktır.

Sunucu üzerinde çalışan işletim sistemlerinin, hizmet sunucu yazılımlarının ve anti-virüs 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.

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 log-on olup, daha sonra genel yönetici hesaplarına geçiş yapmalıdırlar.

8. 5 Gözlemleme

Kritik sistemlerde oluşan bütün güvenlikle ilgili olaylar loglanmalıdır ve saklanmalıdır. Güvenlikle ilgili loglar sorumlu kişi tarafından değerlendirilecek ve gerekli tedbirleri alacaktır.

8. 6 Uygunluk

Denetimler, yetkili organizasyonlar tarafından Kurum bünyesinde belli aralıklarda yapılmalıdır.

Denetimler, Kalite Yönetim Sistemi tarafından yönetilecektir.

Denetimlerin, Kurumun işleyişine zarar vermemesi için maksimum gayret gösterilecektir.

8. 7 İşletim

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

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

Sistem odalarına yetkisiz girişler engellenmelidir. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalıdır.

9. ANTİ-VİRÜS POLİTİKASI

9. 1 Amaç

Rize Ticaret ve Sanayi Odası'nda ki bütün bilgisayarların efektif virüs algılama ve engelleme standardına sahip olması için gereklilikleri belirlemektir.

9. 2 Kapsam

Bu politika Kurumun PC-tabanlı bütün bilgisayarlarını kapsamaktadır. Bunlar desktop bilgisayarlar, laptop ve sunuculardır.

9. 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 parterleri otomatik olarak güncellenmelidir. Virüs bulaşan makineler tam olarak temizleninceye kadar ağdan çıkarılmalıdır.

Rize Ticaret ve Sanayi Odası virüs problemlerini ortadan kaldırılması için tavsiye edilen adımları şu şekilde açıklamaktadır:

Anti-virüs güncellemeleri bu iş için adanmış Sunucular vasıtası ile yapılacaktır. Sunucular internete online bağlantısı olup otomatik olarak veritabanlarını güncelleyecektir. Domaine bağlı PC'ler otomatik olarak sunucudan en son versiyonları update edeceklerdir. Domaine bağlı olmayan kullanıcılara ise gerekli scriptler yazılıp otomatik update olmaları sağlanacaktır.

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

Bilinmeyen veya şüpheli kaynaklardan asla dosya indirmeyin.

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

Bilinmeyen kaynaklardan gelen floppy disketlerini, USB bellekleri ve CDROM'ları daima virüslere karşı tarama yapın.

Kritik data ve sistem konfigürasyonlarını düzenli aralıklar ile yedekleyin ve güvenli bir yerde saklayın.

10. GÜVENLİK AÇIKLARI TESPİT ETME POLİTİKASI

10. 1 Amaç

Bu politikanın amacı Rize Ticaret ve Sanayi Odası'nın 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.

10. 2 Kapsam

Bu politika Kurumun bünyesinde sahip olunan bütün bilgisayar ve haberleşme cihazlarını kapsamaktadır. Bu politika Kurumun bünyesinde bulunan fakat Kurumun sahip olmadığı herhangi bir sistemi de kapsamaktadır.

11. UZAKTAN ERİŞİM POLİTİKASI

11. 1 Amaç

Bu politikanın amacı, herhangi bir yerden Rize Ticaret ve Sanayi Odası'nın bilgisayar ağına erişilmesine ilişkin standartları saptamaktır. Bu standartlar kaynaklarının yetkisiz kullanımından dolayı Kuruma gelebilecek potansiyel zararları minimize etmek için tasarlanmıştır. Bu zararlar şunlardır; Kurumun gizli ve hassas bilgilerinin kaybı, beyin gücü kaybı, prestij kaybı ve içerideki kritik sistemlere meydana gelen zararlar vs.

11. 2 Kapsam

Bu politika Kurumun herhangi bir birimindeki bilgisayar ağına erişen bütün kişi ve firmaları kapsamaktadır. Bu politika, Kuruma bağlı bütün uzak erişim bağlantılarını kapsamaktadır ve bunun içerisine e-posta okuma veya gönderme ve intranet web kaynaklarını gözlemleme dâhildir.

11.3 Politika

Gerekler:

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

Uzaktan erişim metotları ile Kuruma bağlantılarda bilgi sistemlerinin güvenirliğinin sağlanması için aşağıdaki politikalara göz atmak gerekmektedir:

Şifreleme Politikası, Sanal Özel Ağ (VPN) Politikası, Kablosuz İletişim Politikası

Bilgi Sistemlerinin Genel Kullanım Politikası

Gereklilikler:

Internet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişi veya firmalar VPN teknolojisini kullanacaklardır. Bu, veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlayacaktır.

Mümkünse uzaktan erişim güvenliği sıkı bir şekilde denetlenmelidir. Kontrol tek yönlü şifreleme veya güçlü bir uzun şifre destekli public/private key sistemi kullanılması tavsiye edilmektedir.

Kurum çalışanları hiç bir şekilde kendilerinin login ve e-posta şifrelerini aile bireyleri dâhil olmak üzere hiç kimseye veremezler.

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

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

12. RİSK DEĞERLENDİRME POLİTİKASI

12. 1 Amaç

Rize Ticaret ve Sanayi Odası'nın bilgisayar ağında sistem açıklarını tespit etmek ve gerekli tedbirlerin alınmasını sağlamak amacıyla yetkili firma, kuruluşlara risk analizi yaptırılmasına dair kuralları belirlemektir.

12. 2 Kapsam

Risk analizi Kurum içerisinde veya Kurum dışındaki herhangi bir cihaz üzerinden yapılabilir. Risk analizi, uygulama programları, sunucular, ağ veya yönetim sistemleri üzerinde yapılabilir.

12. 3 Politika

Sistemi mükemmelleştirmeyi amaçlayan bu programın çalıştırılması, geliştirilmesi ve uygulaması Kurum ve ilgili firmanın sorumluluğundadır. Risk analizi süresince çalışanlar gerekli noktalarda yardımcı olacaklardır.

Risk değerlendirme raporları Kuruma elden teslim edilecek ve rapor, söz konusu risk ve hassasiyetler giderilene dek bilgi işlem biriminde çevresel ve fiziksel güvenlik önlemleri alınmış bir ortamda saklanacaktır.

Risk değerlendirme çalışmalarına başlamadan önce çalışma kapsamına konu sistemler ve çalışma süreleri Kuruma bildirilecek ve bu çalışmalar Kurum tarafından izlenecektir. Risk değerlendirme çalışmaları esnasında sistemler üzerinde servis reddi veya herhangi bir sebeple iş sürekliliği aksatmayacaktır.

13. KABLOSUZ İLETİŞİM POLİTİKASI

13. 1 Amaç

Bu politika kablosuz cihazların gerekli güvenlik tedbirleri alınmaksızın Rize Ticaret ve Sanayi Odası'nın bilgisayar ağına erişimini engellemeyi amaçlamaktadır. Sadece bu politikanın güvenlik kriterlerine uyan cihazlar Kurumun bünyesinde kullanabilirler.

13. 2 Kapsam

Bu politika Rize Ticaret ve Sanayi Odası'nın bünyesinde kullanılabilecek bütün kablosuz haberleşme cihazlarını (PC, Cep telefonları, PDA vs)

kapsamaktadır. Kablosuz veri transferi sağlayabilen herhangi bir cihaz bunun kapsamındadır. Kurum ile bağlantısı olmayan herhangi bir cihaz veya bilgisayar ağı bu politikanın kapsamı içerisinde değildir.

13. 3 Politika

Onaylanmış Teknoloji

Bütün kablosuz erişim cihazları onaylanmış olmalıdır ve bilgi işlemin belirlediği güvenlik ayarlarını kullanmalıdır.

Güvenlik Ayarları

-Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmalıdır.

-Erişim cihazlarındaki firma vereleri düzenli olarak güncellenmelidir. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlar.

-Erişim cihazlarını kolayca erişilebilir bir yerde olmaması gereklidir. Çünkü cihaz resetlendiğinde fabrika ayarlarına geri dönebilmekte ve güvenlik açığı oluşturabilmektedir.

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

14. KRİZ / ACİL DURUM YÖNETİMİ POLİTİKASI

14.1 Amaç

Bu politika Rize Ticaret ve Sanayi Odası'nın çalışanlarının, bilgi güvenliliği ve iş sürekliliği ile ilgili acil bir durum oluştuğunda sorumlulukları dâhilinde 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 dâhilinde gerekli müdahaleyi yapabilmelerine yönelik normlar aşağıda belirtilmiştir.

14. 2 Kapsam

Bahse konu 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 içeriden gerçekleştirilebilecek saldırı öncesi taramalar olarak tanımlanabilir.

14. 3 Politika

Acil durum sorumluları atanmalı ve yetki ve sorumlulukları belirlenmeli ve dokümante edilmelidir.

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

Kurum bilişim sistemlerinin kesintisiz çalışmasını sağlaması için aynı ortamda kümeleme ,uzaktan kopyalama , yerel kopyalama , pasif sistem çözümlerini hayata geçirilebilir. Kurum, sistemlerini tasarlarken ne kadar süre iş kaybını tolere edeceklerini göz önüne almalıdırlar.

Güvenlik açıkları ve ihlallerinin rapor edilmesi için Kurumsal bir mekanizma oluşturulmalıdır.

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

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

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.

Her bir seviyede tanımlı acil durumlarda karşılaşılabilecek riskler, bu riskin Kuruma getireceği kayıplar ve bu riskler oluşmadan önce ve oluştuktan sonra hareket planları tanımlanmalı ve dokümante edilmelidir.

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.

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

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 dokümante edilmiş olmalıdır.

15. BİLGİ SİSTEMLERİ YEDEKLEME POLİTİKASI

15. 1 Amaç

Rize Ticaret ve Sanayi Odası'nın Bilgi sistemlerinde oluşabilecek hatalar karşısında sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigürasyonu, sistem bilgilerinin ve Kurumsal verilerin düzenli olarak yedeklenmesi gerekir. Bu politika yedekleme kurallarını tanımlamaktadır.

15.2 Kapsam

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

15. 3 Politika

Bilgi sistemlerinde oluşabilecek hatalar karşısında; sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler

üzerindeki konfigürasyon, sistem bilgilerinin ve Kurum verilerin düzenli olarak yedeklenmesi gerekmektedir.

Verinin operasyon el ortamda online olarak aynı disk sisteminde farklı disk volümlerinde ve offline olarak Manyetik kartuş, DVD veya CD ortamında yedekleri alınmalıdır.

Taşınabilir ortamlar (Manyetik kartuş, DVD veya CD) fiziksel olarak bilgi işlem odalarından faklı odalarda veya binalarda güvenli bir şekilde saklanmalıdır.

Veriler offline ortamlarda en az 1**0 (on) yıl süreyle saklanmalıdır.**

Yedekleme konusu bilgi güvenliği süreçleri içinde çok önemli bir yer tutmaktadır. Bu konuyla ilgili sorumluluklar tanımlanmalı ve atamalar yapılmalıdır.

Geri yükleme prosedürlerinin düzenli olarak kontrol ve test edilerek etkinliklerinin doğrulanması ve operasyon el prosedürlerin öngördüğü süreler dahilinde tamamlanabileceğinden emin olunması gerekir.

Veri Yedekleme Standardı; yedekleme sıklığı, kapsamı, gün içinde ne zaman yapılacağı, ne koşullarda ve hangi aşamalarla yedeklerin yükleneceği ve yükleme sırasında sorunlar çıkarsa nasıl geri dönüleceği, yedekleme ortamlarının ne şekilde işaretleneceği, yedekleme testlerinin ne şekilde yapılacağı ve bunun gibi konulara açıklık getirecek şekilde hazırlanmalı ve işlerli ligi periyodik olarak gözden geçirilmelidir.

16. PERSONEL GÜVENLİĞİ POLİTİKASİ

16.1 Amaç

Rize Ticaret ve Sanayi Odasının 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 Kurum, ilgili personelin seçimi, sorumluluk ve yetkilerin atanması, eğitilmesi, işten ayrılması, görev değişiklikleri vb konularının güvenlik ile ilgili boyutunu ne şekilde ele alacağını bu politika ile belirler.

16. 2 Kapsam

Personel Güvenlik Politikası, Rize Ticaret ve Sanayi Odasının bilgi sistemlerini kullanan tüm yönetici ve çalışanlarını kapsamaktadır.

16.3 Politika

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

Kullanıcılara erişim haklarını açıklayan yazılı bildiriler verilmeli ve teyit alınmalıdır.

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

Çalışanlara telefon görüşmeleri yaparken civardakiler tarafından işitilebileceği veya dinlenebileceği için hassas bilgilerin konuşulmaması hatırlatılmalıdır.

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

Güvenlikle ilgili tüm görevler Kurumun Bilgi Güvenliği Politikası bildirisinde tanımlanan roller çerçevesinde ve atanan kişiler tarafından üstlenilecektir.

Tüm çalışanların kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmaları ve bu kartları taşımayan kişilerin Kurum içinde dolaşımının fark edilir kılınması gerekir.

Yetkiler, "görevler ayrımı" ve "en az ayrıcalık' esaslı olmalıdır. "Görevler 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.

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.

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

17. BAKIM POLİTİKASI

17.1 Amaç

Rize Ticaret ve Sanayi Odasının bilgi sistemlerinde kullanılan sistemlerin bakımı ile ilgili politikaları belirlemektir.

17. 2 Kapsam

Bakım Politikası, Rize Ticaret ve Sanayi Odasının bilgi sistemlerini işletmekle sorumlu sistem yöneticilerini kapsar.

17. 3 Politika

Rize Ticaret ve Sanayi Odasının sistemlerinin tamamı (donanım, uygulama yazılımları, paket yazılımları, işletim sistemleri) periyodik bakım güvencesine alınmalıdır. Bunun için gerekli anlaşmalar için yıllık bütçe ayrılmalıdır. Sistem bakımlarından sonra bir güvenlik açığı yaratıldığından şüphelenilmesi durumunda "Bandırma Ticaret Borsası" uyarınca hareket edilmelidir.

18.YAZILIM GELİŞTİRME

18. 1 Amaç

Yazılım geliştirme üzerindeki kontroller, Rize Ticaret ve Sanayi Odasının 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.

18. 2 Kapsam

Bu politika Rize Ticaret ve Sanayi Odasının yazılım geliştirme alanında faaliyet gösteren kişi ve kuruluşları kapsamaktadır.

18. 3 Politika

Yazılım geliştirme üzerindeki kontroller şu temel kriterlere uygun şekilde oluşturulmalıdır;

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

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

İhtiyaçlar, uygun bir şekilde tanımlanmalıdır.

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

Kurum içinde geliştirilmiş yazılımlar ve seçilen paket sistemler ihtiyaçları karşılamalıdır.

Kurumda kişisel olarak geliştirilmiş yazılımların kullanılması kısıtlanmalıdır.

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.

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

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

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

Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.

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

19. RTSO BİLGİ GÜVENLİĞİNİN SAĞLANMASI YÖNTEMLERİ

Odamız ve üyelerimize ait dokümante edilmiş her türlü bilgi ve belgenin güvenliği sağlanmıştır.

Odamız hizmet binası içerisinde yer alan kablosuz internetler uygun nitelikteki karakterler ile şifreleme altına alınmıştır, habersiz yapılabilecek girişler engellenmiştir.

Odamız hizmet binası içerisinde yer alan fiziksel arşivlerimizin giriş kapıları uygun nitelikteki karakterler ile şifreleme altına alınmıştır, yetkisiz kişilerin girişleri engellenmiştir.

Odamız hizmet binası içerisinde ve hizmet binası çevresinde yer alan güvenlik kameraları ile gözlemleme sağlanmaktadır.

Birim temsilcilerinin kullandıkları bilgisayarlarda, dizüstü bilgisayarlarda şifreleme yapılmıştır.

Tarama: *Rize Ticaret ve Sanayi Odasının Servis Büro ve Paper Plas Programları (dijital arşivleme) aracılığıyla Oda Sicil, Ticaret Sicil vb. evraklarının Tarama Cihazı yardımıyla taranarak bilgisayar üzerinde açılan klasörlerde PDF Olarak saklanmasıdır.*

Yedekleme (Bulut Depolama): *Dijital arşivleme ile taranan Oda evraklarının Türk Telekomdan alınan Bulut Sistemindeki alanımıza verilerin aktarılmasıdır. Bulut sistemi ile: elektronik ortamda tutulan bu klasörlerin dosyaların kaybolmaması, yazışmalarda ve dosya çıkarılmadan zaman ve hızlılık bakımından odamızın verimliliğinin arttırılması, bilgilerimizin güvenliği sağlanmaktadır. Bu sistem ile veri kaybı önlenmiş, bilgilerimizin güvenliği sağlanmış olmaktadır.*

Asustor Network Harici Yedekleme Ünitesi: *Haftalık periyotlarda yapılan yedekleme ile bilgilerin yedeklemesi yapılır, bilgi güvenliği sağlanmış olur. Pc bozulması, işletim sistemi çökmesi vb. durumlarda veriler, network üzerinden harici bir belleğe kaydedildiğinden dolayı veri kaybı önlenmiş olur.*

Server (Ateş Duvarı)*: Odamızın Bilgi işlem bölümünde bulunan Server sistemi içerisindeki Ateş duvarı sayesinde: Odamıza gelen zararlı dosyalardan, virüslerden, casus yazılımlardan vb. tehlikelerden bilgilerimizin, sistemimizin korunmasını sağlamaktadır.*

Alpemixs Yazılımı: *Bu yazılımla internet üzerinden odamız bilgi sistemine zarar verebilecek casus yazılımlar, virüsler, fiber saldırılar vb. tehditlere karşı, tehdit kaynağının tespit edilmesi bu program ile sağlanmaktadır. Bu sistem ile tehditin hangi ip adresinden yapıldığı, kaynağının ne olduğu tespit edilebilmektedir. Aynı şekilde oda içerisinden yapılan olumsuz bir işleminde, oda içerisindeki hangi PC'den yapıldığı tespit edilebilmektedir. Bu sistem ile odamız bilgi sisteminde olabilecek bir tehditin kaynağı tespit edilmekte ve çözüme ulaşılabilmektedir.*

20. BİLGİ GÜVENLİĞİ POLİTİKASI ONAYI

Bilgi Güvenliği Politikasının okunduğu, anlaşıldığı ve kabul edildiğinin Rize Ticaret ve Sanayi Odasının Yönetim Kurulu tarafından onaylandığı bir dokümandır.

Bu politikanın uygulanabilirliğinden RTSO Genel Sekreteri ve tüm Personel sorumludur.

İzlenecek Prosedür

Aşağıdaki adımlar takip edilmelidir.

Genel Sekreterlikçe Rize Ticaret ve Sanayi Odası Bilgi Güvenliği Politikası Okunur Onaylanır.

RTSO Yönetim Kurulu tarafından onaylanan politika tüm birimlere iletilir.

RTSO Bilgi Güvenliği Politikasının yürütülmesinden Genel Sekreter ve tüm Birimler sorumludur.

HAZIRLAYAN/KALİTE YÖNETİM TEMSİLCİSİ	ONAYLAYAN/GENEL SEKRETER

21. RİZE TİCARET VE SANAYİ ODASI İLETİŞİM BİLGİLERİ

Adres : Atatürk Caddesi No:359 RİZE
Telefon : (90-464-2171082)
(90-464-2171569)
(90-464-2148855)
(90-464-2148384)
Faks : (90-464-2122200)
Web : www.rtso.org.tr
E-Posta : rtso@rizertso.org.tr