



T.C.

SAĞLIK BAKANLIĞI

SAĞLIK BİLGİ SİSTEMLERİ

GENEL MÜDÜRLÜĞÜ

BİLGİ GÜVENLİĞİ POLİTİKALARI KILAVUZU


V.1

2014




T.C. Sağlık Bakanlığı

*Bilgi Güvenliği Politikaları Kılavuzu
Bakanlık Makamının 28/02/14 tarihli ve 5181.1272 sayılı
onayı ile Bilgi Güvenliği Politikalar Yönergesinin eki
olarak yürürlüğe konulmuştur.*



Bu kılavuz çevre duyarlılığı kapsamında kâğıt ortamda basılmayarak; elektronik ortamda kullanıma sunulacak olup, revizyonların hızla gerçekleştirilmesine ve yayınlanmasına katkı sağlayacaktır.



EDİTÖRLER

Dr. Hakkı ÖZTÜRK
Cumali YÜKSEK
Mustafa ASLAN

İÇİNDEKİLER

ÖNSÖZ	1
BİLGİ GÜVENLİĞİ POLİTİKALARI YÖNERGESİ VE KILAVUZA DAİR GENEL AÇIKLAMALAR	2
A. BİLGİ GÜVENLİĞİ	5
A.1. TEMEL İLKELER	7
A.1.1. Bilgi Güvenliği Politikası	7
A.1.2. Bilgi Güvenliği Organizasyonu	8
A.1.3. Bilgi Güvenliği İhlâl Yönetimi	9
A.1.4. Bilgi Güvenliği Denetimleri	9
A.1.5. Bilgi Güvenliği Politikaları Kılavuzu	10
A.1.6. Kılavuzun Uygulanması	10
A.1.7. Bilgi Güvenliği Eğitimleri	10
A.1.8. Bilgi Güvenliği Standartları	10
B. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS)	10
B.1. Risk Yönetimi	14
B.1.1. Varlıkların Belirlenmesi	14
B.1.2. Tehditlerin Belirlenmesi	14
B.1.3. Açıklıkların Belirlenmesi	16
B.1.4. Olasılık Değerlendirmesi	16
B.1.5. Etki Analizi	16
B.1.6. Risk Derecelendirmesi	17
B.1.7. Risk Derecelendirme Matrisi	17
B.1.8. Risk Derecelerinin Tanımı	18
B.1.9. Uygun Kontrollerin Belirlenmesi	18
B.1.10. Sonuçların Dokümantasyonu	18
C. POLİTİKALAR	19
C.1. İnsan Kaynakları ve Zafiyetleri Yönetimi	19
C.2. Fiziksel ve Çevresel Güvenlik	19
C.3. Ekipman Güvenliği	23
C.4. İşletim Sistemleri ve Son Kullanıcı Güvenliği	25
C.4.1. İşletim Sistemleri Güvenliği	25
C.4.2. Son Kullanıcı Güvenliği	26
C.5. Parola Güvenliği	28

C.6. Kriptolama Yönetimi.....	29
C.7. İnternet ve Elektronik Posta Güvenliği	30
C.8. Sunucu ve Sistem Güvenliği.....	31
C.9. Ağ Cihazları Güvenliği	34
C.9.1. Ağ Cihazları Güvenlik Politikası	34
C.9.2. Kablosuz Ağlar Güvenliği	34
C.10. Mal ve Hizmet Alımları Güvenliği.....	35
C.11. Uygulama Yazılımları Güvenlik Yönetimi	38
C.11.1. Yazılım Geliştirme Politikası.....	38
C.11.2. Belgelendirme Politikası.....	39
C.12. Güvenlik Yazılım ve Donanımları Yönetimi	40
C.13. Bilgi Güvenliği Teknolojileri Güvenliği	41
C.13.1. Yazılım Güvenliği.....	41
C.13.2. Donanım Güvenliği	42
C.14. Bulut Teknolojileri Güvenliği	42
C.15. Mobil Cihazlar Güvenliği.....	43
C.16. İletişim ve İşletim Güvenliği	44
C.17. Kullanıcı Hesabı Açma, Kapatma Yönetimi	49
C.18. Erişim Yönetimi ve Erişim Kaydı Tutulması	50
C.18.1. Erişim Yönetimi.....	50
C.18.2. Kayıt Tutulması (Log tutulması)	51
C.19. Uzaktan Erişim Yönetimi	51
C.20. Acil Erişim Yetkilendirme Yönetimi	52
C.21. Veri Merkezi Standartları ve Yönetimi.....	53
C.22. Veri Tabanı Güvenliği.....	55
C.23. Kaydedilebilir Taşınır Materyaller Güvenliği.....	57
C.24. Bilgi Sistemleri Edinim Geliştirme ve Bakımı.....	58
C.25. Yedekleme ve İş Sürekliliği Yönetimi	63
C.25.1. Veri Yedekleme	63
C.25.2. İş Sürekliliği Yönetimi	64
C.26. Bilgi Kaynakları Atık ve İmha Yönetimi	66
C.27. Bilgi Güvenliği Teknik ve Farkındalık Eğitimleri.....	66
C.28. Değişim Yönetimi	67
C.29. İhlal Bildirim ve Yönetimi	67

C.30. Bilgi Güvenliđi İzleme ve Denetleme Yönetimi.....	69
C.31. Bilgi Güvenliđi Testleri	69
C.32. Acil Durum Yönetimi	69
C.33. Bilgi Güvenliđi Ulaştırma Güvenliđi Yönetimi	71
C.34. Sosyal Mühendislik Zafiyetleri	72
C.35. Sosyal Medya Güvenliđi.....	72
C.36. Sistem Akreditasyonu.....	72
C.37. Medikal Cihazlar Güvenliđi	72
D. KISALTMALAR.....	73
E. SÖZLÜK.....	73
F. KAYNAKLAR.....	79
G. YARARLI BAĞLANTILAR	80
H. KATKIDA BULUNANLAR	81
İ. İLETİŞİM	82

Günümüzde hızla gelişen bilim ve teknoloji insan hayatını oldukça kolaylaştırmaktadır. Bilgisayarlar, tabletler, akıllı cep telefonları vb. elektronik aletler günlük hayatımızda sürekli kullandığımız cihazlardır. İnternet teknolojisi ile bu cihazların kullanımı artmış, bilgiye ulaşmak kolaylaşmıştır. Bu küresel iletişim ağı bilimsel araştırmaların, üretkenliğin, kültürel değişmelerin, küresel ticaretin ve küresel eğitimin ana bilgi kaynağı olmuştur. Bu ağ dünyada yaşayan tüm insanlar arasında yazılı, sözlü ve görüntülü iletişim kurmak için küresel bir merkez oluşturmuştur. Dünyanın bir ucundaki kütüphanede bulunan bilgilere çok hızlı ve çok kolay bir şekilde ulaşabilmektedir. Artık kâğıt ortam yerini elektronik ortama bırakmış ve böylece bilgi akışı hızlanmış, bilgi ile belge saklama, depolama ve korumada büyük kolaylık sağlanmıştır. İstenilen bilgi, belge, doküman ve verilere ulaşımında zaman kazanılmış, maliyet azalmış ayrıca çevreyi koruma açısından önemli bir adım atılmıştır.

Günümüzde kurumlar bilgilerinin büyük bir kısmını elektronik ortamda bulundurmakta ve bu bilgileri bilişim sistemleri altyapısı kullanarak işlemektedir. İş ve işlemlerin elektronik ortama taşınması, kamu hizmetlerinin etkinleştirilmesi, yasa dışı faaliyetlerin tespit edilebilmesi ve önlenmesine yönelik olarak kişisel bilgilerin de elektronik ortamda bulunması ve işlenmesi yoğun bir şekilde artmıştır. Ancak bu durum, kişisel bilgilerin sahiplerinin isteği dışında ilgisiz ve yetkisiz tarafların eline geçmesi, kişisel bilgi sahibini rahatsız edecek veya onlara zarar verecek şekilde yasa dışı olarak kullanılması ve kişi mahremiyetinin ihlali tehlikesini de doğurmaktadır. Dolayısı ile gelişen bilişim teknolojileri bilgi güvenliği olgusunu da beraberinde önce ihtiyaç sonra zorunluluk haline getirmiştir.

Sağlık sektöründe güncel teknolojinin hissedilir şekilde kullanılmasıyla birlikte teknolojinin taşıdığı bazı risklerle de yüz yüze gelinmiştir. Elektronik ortamdaki tüm veriler gibi, kişisel sağlık bilgilerini tehdit eden riskler için güvenlik önlemlerinin alınması zorunlu hale gelmiştir. Kişisel sağlık bilgileri, kişinin doğum öncesinden ölüm sonrasına kadar geçen süreyi kapsayan sağlık bilgilerinin tümüdür. Sağlık kayıtlarının sayısallaştırılması etkin sağlık hizmeti için yadsınamayan ciddi bir hamledir. Güncel teknolojilerin kişisel sağlık bilgilerinin gizlilik, bütünlük ve erişilebilirlik risklerini artırmasından dolayı sağlık bilgilerinin güvenliği zedelenmektedir. Kişisel sağlık bilgilerinin mahremiyeti esastır. Bu nedenle önlemlerin alınması, risklerin saptanıp indirgenmesi zorunlu hale gelmiştir.

Sağlık Bakanlığı olarak hazırlamış olduğumuz bu kılavuz sizlere yapılması gereken bilgi güvenliği çalışmalarında önderlik yapacaktır. Bir program dâhilinde ilerlemenizi sağlayacak, tüm yönetici ve son kullanıcıların bu kapsamda yapmaları gereken işler çerçevesinde bir rehber olarak hazırlanmıştır.

BİLGİ GÜVENLİĞİ POLİTİKALARI YÖNERGESİ VE KILAVUZA DAİR GENEL AÇIKLAMALAR

Bakanlığımız bilgi güvenliği çalışmaları; iki ana eksen üzerine oturtulmaya çalışılmıştır. Bunlardan Bilgi Güvenliği Politikaları Yönergesi ile hukuki ve idari alt yapı oluşturulmuş, yönergeden alınan yetki ile ise bilgi güvenliği teknik, sistemsal unsurlarının yer aldığı Bilgi Güvenliği Politikaları Kılavuzu hazırlanarak kullanıma sunulmuştur.

Kılavuzda yer alan teknik terminolojinin herkesçe anlaşılabilmesi için kılavuzun sonunda “Bilgi Güvenliği Terimleri Sözlüğü” ne yer verilmiştir.

Bu kılavuz Bakanlık Makamının 28/02/14 tarih ve 5181.1272 sayılı, onayı eki ile yürürlüğe konulan “Bilgi Güvenliği Politikaları Yönergesinin” ilgili hükümleri çerçevesinde Sağlık Bilgi Sistemleri Genel Müdürlüğünce hazırlanmak sureti ile yönergenin kapsam maddesinde belirtilen tüm ilgili taraflara resmi yazı ekinde ve bilgiguvenligi.saglik.gov.tr/ adresinde yayınlanmak sureti ile iletilmektedir.

Kılavuzda temel amaç; Sağlık Bakanlığının görevleri kapsamında bilginin toplanması, değerlendirilmesi, raporlanması ve paylaşılması süreçlerinde güvenliğin sağlanmasına yönelik tedbir almak, bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek içerden veya dışardan kasıtlı ya da kazayla oluşabilecek tüm tehditlerden korunmasını sağlamak, son kullanıcı, idareci, sistem ve veri tabanı yöneticileri ve teknik personelin bilgi sistem ve ağları üzerinde yapacakları çalışmalarda bilgi güvenliği farkındalık, duyarlılık ve teknik bilgi düzeylerinin artırılması ile sistemsal güvenlik açıklarının ortadan kaldırılmasını sağlayarak, insan kaynaklı zafiyetlerin önlenmesi ve gizliliği, bütünlüğü ve erişilebilirliği sağlanmış bilişim alt yapısının kullanılması ve sürdürülebilirliğinin temin edilmesi sureti ile;

veri ve bilgi kayıplarının önlenmesi bu yolla ekonomik zarara uğranılmaması ve kurumsal prestij kaybı yaşanmaması ana ilke ve amaçlar olarak öngörülmektedir.

Güvenlik Açıkları



Şekil 1- Güvenlik Açıkları

Kılavuzun 1.versiyonu içerisindeki bazı başlıklar çalışmaları devam ettiğinden 2.versiyonda tamamlanacaktır.

Bu çalışmada, Bakanlık merkez ve bağlı kuruluşların görüş ve önerileri dikkate alınmış olmakla beraber, kılavuza ilişkin yapılacak çalışmalarda dikkate alınmak üzere tüm kullanıcılar ile kurum ve kuruluşlar, olabilecek görüş ve önerilerini bgkilavuzu@saglik.gov.tr mail adresine gönderebilirler.

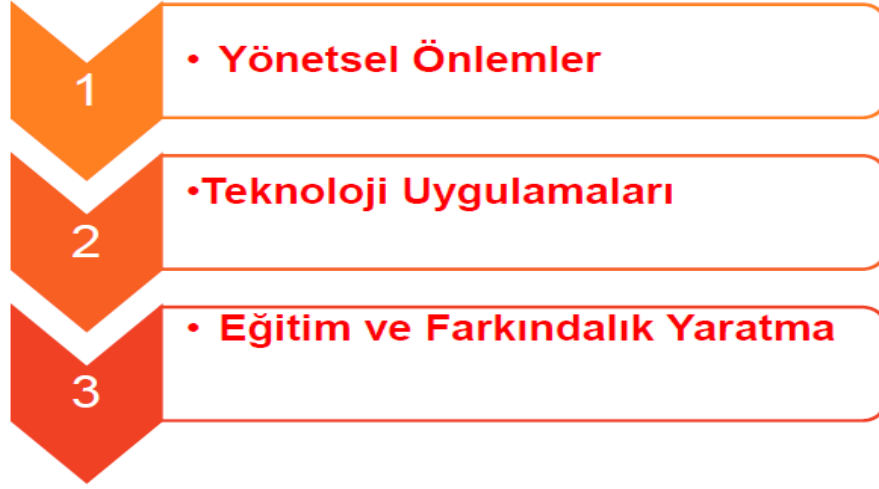
Bu kılavuzda esasen bilgi sistemleri güvenliğine yönelik yaklaşım benimsenmiş olup; “kişisel veri ve bilgilerin ” kullanımı ve mahremiyet ilkelerine ilişkin hususlar; 663 sayılı KHK’da ön görüldüğü üzere Sağlık Hizmetleri Genel Müdürlüğü görevleri arasında yer alan “8. Maddesinin j fıkrasında” ifade edilen “İlgili mevzuat çerçevesinde kişisel verilerin korunmasına ve veri mahremiyetinin sağlanmasına yönelik düzenleme yapmak” hükmü çerçevesinde hazırlanacak olan düzenlemeye bırakılmıştır

Bilgi güvenliği konusunda bilgi kaynaklarına erişim sağlanması amacı ile kılavuzun sonunda “yararlı kaynaklar “ başlığı altında bazı ulusal ve uluslar arası bağlantılar belirtilmiş olup; bunlardan bilgiguvenligi.gov.tr ve Bakanlığımız bilgiguvenligi.saglik.gov.tr/ sayfası takip edilmek suretiyle en güncel ve yararlı bilgi güvenliği belgelerine erişim sağlanmış olacaktır.

Bilgi güvenliği yetkilisinin görevlendirilmesinde; yönerge üst yönetimleri yetkili kılmış olmakla kurumların mevcut personel yapısının ortak amaçlar için kullanılmasına imkan sağlamıştır. Bu çerçevede üst idarelerin kararları doğrultusunda birkaç veya grup alt düzey kurumların “koordinatör bilgi güvenliği yetkilisi” görevlendirme noktasında esnek bir yaklaşım benimsemelerine imkan tanınmıştır. Bilgi güvenliği yetkilisi öncelikle bilişim alt yapısı yeterli personel içerisinden seçilmiş olabileceği gibi mevcut personeller içerisinden en uygun olanında seçilmesi şeklinde görevlendirilmesi mümkün olacaktır.

Bilgi Güvenliğinin sağlanmasında yönetsel, teknik, idari, hukuki araçlar sistematik olarak kullanılmalıdır. Bilgi güvenliğinin sağlanmasında standart bir yaklaşımın tesis edilmesi çerçevesinde yönetsel bir araç olarak, bilgi güvenliği yönetim sistemi yaklaşımı kurumsal düzeyde kullanılmakta olup, bu yaklaşımın temeli TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardıdır. Bu standart kurumlara bilgi güvenliğinin sağlanmasında sistematik ve dokümantasyon tabanlı bir anlayışın entegre edilmesinde önemli bir araç olarak kullanılmaktadır. Kurumlar, TS ISO 27001 Standardı uyumlaşma çalışmaları neticesinde, TSE başta olmak üzere akredite edilmiş kurum ve kuruluşlar tarafından sertifikalandırılmaktadır. Ancak, bilgi güvenliğinin sağlanmasında alınmış bir Bilgi Güvenliği Yönetim Sistemi sertifikasyonundan ziyade, içselleştirilmiş bir kurumsal farkındalık, duyarlılık ve bilgi düzeyinin kurumun bilgi güvenliği alt yapısı itibari ile çok daha önemli olduğu gerçeği göz ardı edilmemelidir.

Bilgi Güvenliđi Nasıl Sađlanır?



Şekil 2- Bilgi Güvenliđi Nasıl Sađlanır

TS ISO 27001 uyumlaşma çalışmaları her kurumun kendi çabaları ve kurumsal kapasiteleri ile gerçekleştirilebilecek bir alan olup, bu konuda üçüncü taraflar yerine Bakanlığımız Sağlık Bilgi Sistemleri Genel Müdürlüğü tüm kurum ve kuruluşlarımıza rehberlik ve danışmanlık desteđi sağlama noktasında alt yapısını geliştirme çalışmalarını yürütmektedir.

TS ISO/IEC 27001 BGYS standart şablon dokümanları bilgiguvenligi.saglik.gov.tr/ adresinde yayınlanacak, bilgi güvenliđi ve BGYS konularında uzaktan eğitim modülü yayına alınmak sureti ile aynı anda çok sayıda personelin bilgi güvenliđi farkındalık, duyarlılık ve bilgi düzeylerinin geliştirilmesi sağlanmış olacaktır. Bilgi Güvenliđi Politikaları Yönergesi ilgili maddeleri geređince bilgi güvenliđi eğitimleri ile ilgili eğitim planlamaları Sağlık Bilgi Sistemleri Genel Müdürlüğüne yapılacak olup, konu yıllık hizmet içi eğitim planlamalarında da yer alacaktır.

Kılavuzda ifade edilen hususlarda; tüm kullanıcıları kapsayan madde başlıkları olabildiđi gibi sadece sistem ve veri tabanı yöneticilerini, hizmet sağlayıcıları, yöneticileri ilgilendiren müstakil konu başlıkları da yer almaktadır.

Sorumluluk düzeylerinin belirlenmesinde ilgililik ve yetki düzeyleri temel kriterler olarak ön görülmeli, hazırlanacak olan bilgi güvenliđi planlarında yönetimsel, teknik ve son kullanıcı düzeyinde sorumluluk ve yetki alanları belirtilmelidir.

A. BİLGİ GÜVENLİĞİ

Günümüzde devlet kurumları ve ticari şirketler işlerini sürdürebilmek için yoğun bir şekilde bilgi kullanımına yönelmişlerdir. Zaman geçtikçe bilginin önemi artmış, sadece güvenli bir şekilde saklanması ve depolanması gelişen ihtiyaçlara cevap verememiş aynı zamanda bir yerden bir yere nakil edilmesi de kaçınılmaz bir ihtiyaç haline gelmiştir. Bilgiye olan bu bağımlılık bilginin korunması ihtiyacını gündeme getirmiştir. Bu anlamda bilgi, kurumun sahip olduğu varlıklar arasında çok önemli bir yere sahiptir. Bilgiye yönelik olası saldırılar, tahrip edilmesi, silinmesi, bütünlüğünün ve/veya gizliliğinin zarar görmesi, bilgi altyapısının bozulmasına ve bu da beraberinde işlerin aksamasına neden olmaktadır. Bu çerçevede bilgi ve bilgi güvenliği kavramları karşımıza çıkmaktadır.

Bilgi güvenliği, “bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak” tanımlanır. Bilgisayar teknolojilerinde güvenliğin amacı ise “kişi ve kurumların bu teknolojilerini kullanırken karşılaşılabilecekleri tehdit ve tehlikelerin analizlerinin yapılarak gerekli önlemlerin önceden alınmasıdır.

Bilgi, kurumdaki diğer varlıklar gibi, kurum için önem taşıyan ve bu nedenle de en iyi şekilde korunması gereken bir varlıktır. Bilgi güvenliği; kurumdaki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve yatırımlardan gelecek faydanın artırılması için bilginin geniş çaplı tehditlerden korunmasını sağlar.

Bilgi birçok biçimde bulunabilir. Bilgi, kâğıt üzerinde yazılı olabilir, elektronik olarak saklanıyor olabilir, posta ya da elektronik posta yoluyla bir yerden bir yere iletilir ya da kişiler arasında sözlü olarak ifade edilebilir. Bilgi hangi formda olursa olsun, mutlaka uygun bir şekilde korunmalıdır. Bilgi güvenliğinin sağlanabilmesi bilginin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin yeterli düzeylerde sağlanabilmesi ile mümkündür.

Bilgi güvenliği temelde aşağıdaki üç unsuru hedefler:



Şekil 3- Gizlilik, Bütünlük, Süreklilik



- Gizlilik
- Bütünlük
- Süreklilik

Bu kavramları biraz daha açacak olursak gizlilik, bilginin yetkisiz kişilerin erişimine kapalı olması şeklinde tanımlanabilir. Bir diğer tarif ile gizlilik bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir. Bütünlük, bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır. Bütünlük için kısaca kazara veya kasıtlı olarak bilginin bozulmaması diyebiliriz. Kullanılabilirlik, bilginin her ihtiyaç duyulduğunda kullanıma hazır durumda olması demektir. Herhangi bir sorun ya da problem çıkması durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Bu erişim kullanıcının hakları çerçevesinde olmalıdır. Kullanılabilirlik ilkesince her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir.

A.1. TEMEL İLKELER

- Tüm yöneticiler, yönetim alanları ve yerine getirmekle yükümlü oldukları tüm iş ve işlemlerin yürütülmesinde kullandıkları bilgi sistemleri ile ilgili olarak; bilgi güvenliği duyarlılığı çerçevesinde hareket etmekle, yönetim alanları ve işleri ile ilgili olarak bilgi güvenliği iş planı hazırlamakla ve yürürlüğe koymakla yükümlüdürler.
- Her kullanıcı Kılavuzda yer alan kişisel veya çalışma alanı ile ilgili hususlara uymakla yükümlüdür.
- Kullanıcı, bilgi sistemleri ve ağlarının güvenliğinin gerekliliği ve güvenliği artırmak için neler yapabileceği konularında bilinçli olmalıdır.
- Tüm yöneticiler kendi sorumluluk alanlarındaki bilgi sistemleri ve ağlarının güvenliğinden sorumludurlar.
- Kullanıcı, güvenlik tehditlerini önlemek, saptamak ve bunlara tepki verebilmek için işbirliği içinde ve zamanında eyleme geçmekten sorumludur.
- Kullanıcılar, bilgi sistem ve ekipmanlarının kullanımında birbirlerinin haklarına saygı göstermekle yükümlüdürler.
- Kullanıcı, idarece yapılmış olan risk değerlendirmelerinde kendileriyle ya da çalışma alanlarıyla ilgili öngörülen tedbirlere uymak zorundadır.
- Kullanıcı, güvenliği, bilgi sistem ve ağlarının önemli bir unsuru olarak değerlendirmelidir.
- Kurumlar hedeflenmek sureti ile içerden ya da dışarıdan yapılacak siber saldırılara karşı kurumsal sorumluluk ve yetkiler çerçevesinde gerekli tedbirler alınmalıdır.
- Yönetimler, bilgi güvenliği yönetimi ile ilgili kapsamlı bir yaklaşım benimsemelidir.
- Yönetimler, bilgi sistem ve ağlarının güvenliklerini incelemeli ve yeniden değerlendirmelidir. İnceleme ve yeniden değerlendirme neticesinde, güvenlik ile ilgili politika, uygulama, önlem ve prosedürlerde gerekli değişiklikleri zamanında yapmakla yükümlüdür.

A.1.1. Bilgi Güvenliği Politikası

Bakanlığımız, T.C. Anayasası ve kanunlar çerçevesinde yürütmekte olduğu iş ve işlemlerin işleyen süreçlerinde ülke nüfusunun tamamı ile ilgili olan sağlık ve tüm alt unsurları ile ilgili olarak doğum öncesinden ölüme kadar olan tüm süreçlerde çalışmakla yükümlendirilmiş bir kurum olma hüviyeti ile ülkedeki her bir vatandaşa karşı sorumlulukları olan kuruluşlardan birisidir. Her bir vatandaşın sağlık kuruluşuna müracaat ettiğinde en gizli ve mahrem sayılabilecek bilgilerine dair erişebilen kaydedebilen yegâne kuruluştur.

T.C. Sağlık Bakanlığı hasta sıfatı ile bir bireyle muhatap olduğunda ve bireyin herhangi bir verisini ve bilgisini kayıt altına aldığı anda, kayıt altına alınan bireye ait her türlü veri ve bilginin kendisine emanet edilmiş bir değer olduğu düşüncesiyle kendisini bu sorumluluğun yerine getirilmesinde mükellef olarak görmektedir.

T.C. Sağlık Bakanlığı kişi verilerinin ve bilgilerinin korunması ve güvenliği ile alakalı her türlü “**teknik idari ve hukuki yöntemi**” kullanmak sureti ile emanetinde bulunan tüm bilgi sistemleri kaynaklarını “bilgi güvenliği ana politikası çerçevesinde” korumakla ve bu hususta tüm tedbirleri almakla yükümlü olduğunun bilincindedir.

Tüm teşkilatımızda üretilen bilginin de en üst seviyelerde güvenlik anlayışı içerisinde korunması gerektiği bilinci ile hareket eden T.C. Sağlık Bakanlığı misyon ve vizyonuna bağlı kalarak Bilgi Güvenliği konseptinin esasını oluşturan basılı ve elektronik ortamdaki bilgilerin yasal mevzuat ışığında ve risk metotları kullanılarak **“gizlilik, bütünlük ve erişilebilirlik”** ilkelerine göre yönetilmesi amacıyla;

- Bilgi Güvenliği Standartlarının gerekliliklerini yerine getirmek,
 - Bilgi Güvenliği ile ilgili tüm yasal mevzuata uyum sağlamak,
 - Bilgi varlıklarına yönelik riskleri tespit etmek ve sistematik bir şekilde riskleri yönetmek,
 - Bilgi Güvenliği Yönetim Sistemini sürekli gözden geçirmek ve iyileştirmek,
 - Bilgi Güvenliği farkındalığını artırmak için, teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler gerçekleştirmek,
- ana politikalar olarak öngörülmektedir.

Bilgi güvenliği sadece bilgi teknolojileri çalışanlarının sorumluluğunda değil eksiksiz tüm çalışanların katılımı ile başarılabilecek bir iştir. Ayrıca bilgi güvenliği sadece bilgi teknolojileri ile ilgili teknik önlemlerden oluşmaz. Fiziksel ve çevresel güvenlik, insan kaynakları güvenliğine, iletişim ve haberleşme güvenliğinden, bilgi teknolojileri güvenliğine birçok konuyu da kapsar.

Bilgi güvenliği bilinçlendirme süreci kurum içinde en üst seviyeden en alt seviyeye kadar çalışanların katılımını gerektirmektedir. Kurum çalışanları, yüklenici firma personeli, yarı zamanlı personel, stajyerler, diğer kurum çalışanları, ziyaretçiler, iş ortaklarının çalışanları, destek alınan firmaların personeli, kısaca kurumun bilgi varlıklarına erişim gereksinimi olan herkes kullanıcı kategorisine girmektedir. Kullanıcılar, bilgi güvenliği bilinçlendirme sürecindeki en büyük ve önemli hedef kitledir. Kurum içindeki işler yürütülürken istemeden yapılan hataları ve bilgi sisteminde oluşabilecek açıklıkları en aza indirmek onların elindedir. Yöneticiler, bilgi güvenliği bilinçlendirme ve eğitimi sürecinin gereklerine personelinin uymasını sağlamakla sorumludurlar.

Başarılı ve etkin işleyen bir bilgi güvenliği bilinçlendirme süreci oluşturulabilmesi için bu alandaki görev ve sorumlulukların açık ve net bir biçimde belirlenmesi gerekmektedir. Olgunlaşmış bir bilinçlendirme süreci, bu görev ve sorumlulukların sahipleri tarafından doğru anlaşılması, bilinmesi ve uygulanması ile mümkündür.

Sonuç olarak Bilgi Güvenliği Politikasının amacı bilgi varlıklarını korumak, bilginin ve verinin gizliliğini sağlamak, bütünlüğünü bozmaya çalışacak yetkisiz kişilerin erişimine karşı korumak ve böylece Bakanlığımızın güvenliğini ve itibarını sarsacak durumları bertaraf etmektir.

A.1.2. Bilgi Güvenliği Organizasyonu

A.1.2.1. Genel Müdürlük tarafından, bilgi güvenliğinin iç organizasyonunun sağlanması için bilgi güvenliği konusunda uzmanlaşmış, bilgi sistemlerinin kapsamı göz önüne alınarak yeterli sayıda personelden oluşan, teknik, idari ve hukuki süreçlerde çalışmalarda bulunmak üzere “Bilgi Güvenliği Yönetim Komisyonu” oluşturulur.

A.1.2.2. Komisyona bağlı olarak çalışmak üzere bilgi güvenliğinin farklı alt alanlarında “çalışma grupları” teşkil edilir. Çalışma gruplarının oluşturulurken teknik, hukuki ve idari disiplinlerden personel bulunmalıdır.

A.1.2.3. Komisyonun görevleri;

- Bilgi güvenliği politika ve stratejilerini belirler, gerektiğinde Bilgi Güvenliği Politikaları Yönergesine bağlı olarak çalışma grupları tarafından hazırlanacak olan kılavuzlarla ilgili revizyon kararlarını verir,
- Bilgi güvenliği politikalarının uygulamasının etkinliğini gözden geçirir,
- Bilgi güvenliği faaliyetlerinin yürütülmesini yönlendirir,
- Bilgi güvenliği eğitimi ve farkındalığını sağlamak için plan ve programları hazırlar,
- Bilgi güvenliği faaliyetleri ve kontrollerinin tüm kurum ve kuruluşlarda koordine edilmesini sağlar.

A.1.2.4. Bakanlık Merkez, bağlı kuruluşlar ve taşra teşkilatları kurumları bünyesinde, bilgi güvenliği faaliyetlerini yürütmek ve koordine etmek üzere “Bilgi Güvenliği Yetkilisi ” görevlendirilir. Bakanlık Merkez, bağlı kuruluşlar ve taşra teşkilatları üst yönetimleri hangi seviyede ve hangi alt kuruluşlarında “Bilgi Güvenliği Yetkilisi” görevlendireceklerine kurum bilgi sistemleri kapsamı, etki alanı, personel sayısı gibi kriterleri göz önüne alarak, ölçek yaklaşımı çerçevesinde karar verirler ve görevlendirecekleri Bilgi Güvenliği Yetkilisinin sorumluluk kapsamını belirlerler.

A.1.2.5. Bilgi Güvenliği Yetkilisinin ana işlevi; bulunduğu kurumdaki bilgi güvenliği faaliyetlerini Genel Müdürlük ile koordineli bir şekilde yürütmektir. Bilgi Güvenliği Yetkilisi olarak görevlendirilen personel Genel Müdürlük tarafından ana ilke ve politikalar konusunda eğitilir ve yönlendirilir.

A.1.2.6. Bilgi güvenliği ihlal bildirimleri anında Bilgi Güvenliği Yetkilisine bildirilir. Bilgi Güvenliği Yetkilisi, Kurumu için Kılavuz çerçevesinde “Bilgi Güvenliği Planı” yapar ve bu Plan görev yaptığı kurum idaresince onaylanır.

A.1.3. Bilgi Güvenliği İhlâl Yönetimi**A.1.3.1. Bilgi güvenliği olaylarının rapor edilmesi;**

- Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan idari uygulama planı oluşturulur.
- Bilgi güvenliği ihlâli oluşması durumunda kişilerin tüm gerekli faaliyetleri hatırlamasını sağlamak amacıyla bilgi güvenliği olayı rapor formatı hazırlanır.
- Güvenlik ihlal olayının oluşması durumunda olay anında raporlanır.
- Güvenlik ihlaline neden olanlar hakkında, hukuki süreç başlatılır.

A.1.3.2. Tüm çalışanlar, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği olayını önlemek amacıyla güvenlik zayıflıklarını doğrudan kendi yönetimlerine veya hizmet sağlayıcılarına mümkün olan en kısa sürede rapor ederler.

A.1.4. Bilgi Güvenliği Denetimleri

- Genel Müdürlük Yönergenin kapsam maddesinde belirtilen tüm unsurlarla ilgili Kılavuzda belirtilen hususlarda bilgi güvenliği denetimleri yapar.
- Bilgi güvenliği denetimlerini yapacak personelin nitelikleri Genel Müdürlükçe belirlenir.
- Senaryoları idarece önceden onaylanmak kaydıyla “bilgi güvenliği ve sosyal mühendislik testleri” yapılabilir.
- Genel Müdürlük, bilgi güvenliği denetimlerinde yer almak üzere yeteri kadar personelin eğitimi ile ilgili çalışmaları yapar.

A.1.5. Bilgi Güvenliği Politikaları Kılavuzu

- Kılavuz; Genel Müdürlük tarafından Yönergenin kapsam maddesinde tanımlanan tüm unsurlarla ilgili olarak; bilgi güvenliğinin sağlanması ile ilgili; yönetsel, teknik, idari, hukuki süreçlerin tüm detaylarının yer alacağı bir doküman olarak hazırlanır.
- Kılavuzun ilk versiyonu Bakanın onayı ile yürürlüğe girer, daha sonraki versiyonlar Genel Müdürlük onayı ile yürürlüğe konulur.
- Kılavuz; periyodik olarak, teknolojik gelişmeler paralelinde gözden geçirilerek revize edilir ve elektronik ortamda yayınlanacak bir rehber doküman olarak hazırlanır.
- Kapsam maddesinde belirtilen tüm Bakanlık ve bağlı kuruluşları unsurları Kılavuzda yer alan hususlara uymakla yükümlüdürler. Gerekli hallerde Genel Müdürlükçe teknik destek talepleri karşılanır. Genel Müdürlük, Bakanlık internet ana sayfası üzerinde bilgi güvenliği alanı oluşturur. Bu alan üzerinde bilgi güvenliği konularında üretilen ulusal ve uluslararası kılavuz, rapor, bilgi notu, tez vb. dokümanlara erişim sağlar.
- Genel Müdürlük, Bilgi Güvenliği Terimleri Sözlüğü hazırlar ve internet üzerinden yayına sunar.

A.1.6. Kılavuzun Uygulanması

- Kılavuzun uygulanması ile ilgili olarak; yöneticiler hazırlayacakları bilgi güvenliği planları içerisinde “Kılavuza Uyumlaşma Takvimi ” hazırlar ve kılavuzun uygulanması ile ilgili gerekli idari tedbirleri alır.

A.1.7. Bilgi Güvenliği Eğitimleri

- Genel Müdürlük, bilgi güvenliği eğitim planlamasını tüm Bakanlık ve bağlı kuruluşları için yapmak suretiyle her seviyedeki personelin bilgi güvenliği farkındalık düzeylerini artırmak yönünde eğitim faaliyetlerinde bulunur. Yıllık hizmet içi eğitim planlamalarında bilgi güvenliği başlığı planlara dahil edilir. Teknik seviyedeki personelin bilgi düzeyinin artırılması yönünde ileri seviyede bilgi güvenliği eğitim planlamalarını yapar.
- Ulusal düzeyde siber güvenlik ile ilgili kurum ve kuruluşlarla ortak eğitim, seminer, konferans, sempozyum gibi faaliyetler gerçekleştirilmesine yönelik yıllık planlar yapar.
- Bilgi güvenliği ile ilgili uzaktan eğitim modülünü devreye sokarak, teknik ve farkındalık eğitimlerini web tabanlı olarak sunar.

A.1.8. Bilgi Güvenliği Standartları

Genel Müdürlük bilgi güvenliği çalışmalarının standartlaştırılması ve çalışmalara sistematik bir anlayış entegre edilmesi yaklaşımı ile ulusal ve uluslararası bilgi güvenliği standartlarına uyumlaşma ve sertifikasyonun gerçekleştirilmesi yönünde çalışmalar yapar. Bu konuda ulusal ve uluslararası kuruluşlarla işbirliği gerçekleştirir.

B. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS)

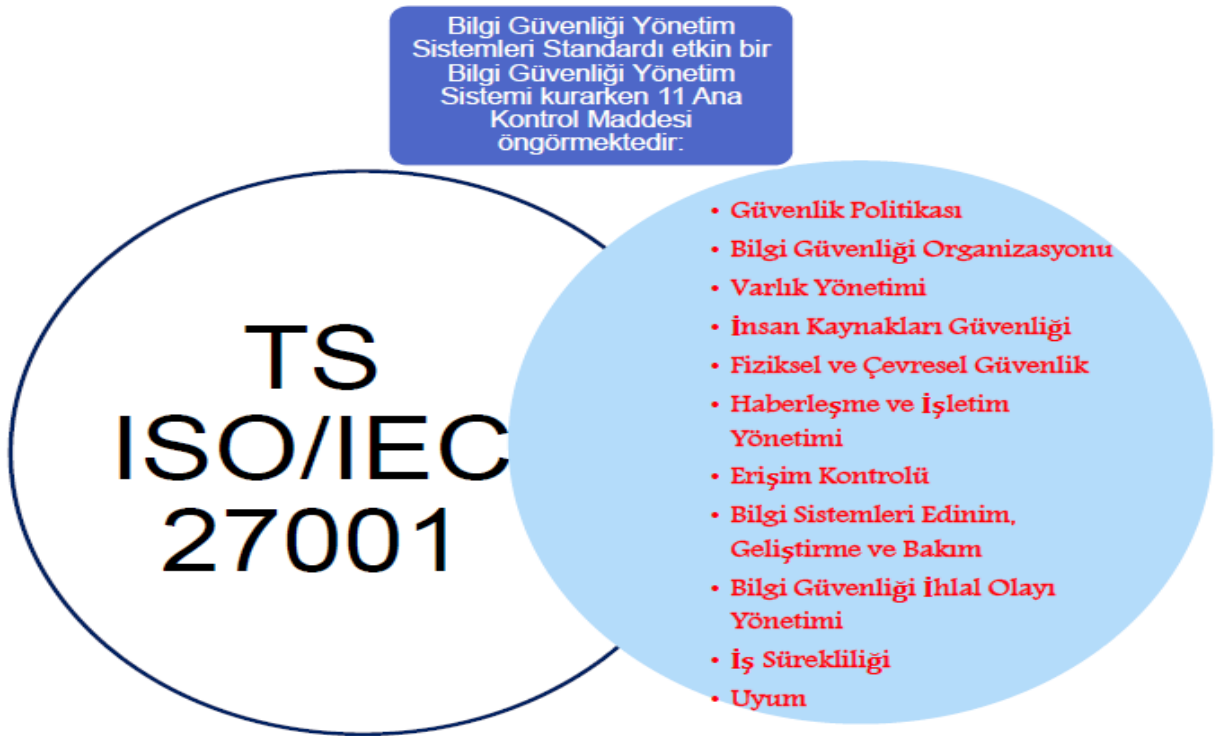
TS ISO/IEC 27001 Standardı bir Bilgi Güvenliği Yönetim Sistemi Standardı olup; bu standarda uyumlaşmak ve sertifikalandırılmak isteyen kurumlar kurumsal kapasiteleri çerçevesinde kuracakları Bilgi Güvenliği birimleri veya çalışma grupları ile uyumlaşma ve sertifikasyon sürecini, Sağlık Bilgi Sistemleri Genel Müdürlüğünün rehberliğinde ve dokümantasyon desteği ile kurup işletebilirler. Gerekli eğitim ve danışmanlık hizmeti Sağlık Bilgi Sistemleri Genel Müdürlüğü tarafından talepler çerçevesinde karşılanacaktır.

Bilgi Güvenliği Yönetim Sistemi BGYS, kurumun hassas bilgilerini yönetebilmek amacıyla benimsenen sistematik bir yaklaşımdır. Bu sistemin temel amacı hassas bilginin

korunmasıdır. Bu sistem çalışanları, iş süreçlerini ve bilgi teknolojileri (BT) sistemlerini kapsar.

Bilgi Güvenliği Yönetim Sistemi deyimi ilk kez 1998 yılında BSI (British Standards Institute) tarafından yayınlanan BS 7799-2 standardında kullanılmıştır. Daha sonra bu standart Uluslararası Standartlar Kurumu ISO tarafından kabul edilmiş ve ISO/IEC 27001:2005 olarak yayınlanmıştır. BSI tarafından yayınlanan bir diğer standart BS 7799-1 ise bilgi güvenliğinin sağlanmasında kullanılacak kontrollerden bahsetmektedir. Bu da yine ISO tarafından kabul edilmiş ve ISO/IEC 27002:2005 olarak yayınlanmıştır. ISO/IEC 27002:2005 bu standardın Temmuz 2007’den itibaren kullanılan ismidir, bu tarihe kadar standart ISO/IEC 17799:2005 olarak adlandırılıyordu.

Bilgi güvenliği yönetimi konusunda en yaygın olarak kullanılan standart, “ISO/IEC 27002:2005 Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri” standardıdır. Bu standart, işletmeler içerisinde bilgi güvenliği yönetimini başlatmak, gerçekleştirmek, sürdürmek ve iyileştirmek için genel prensipleri ve yönlendirici bilgileri ortaya koyar. ISO/IEC 27002:2005 rehber edinilerek kurulan BGYS’nin belgelendirmesi için “ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler” standardı kullanılmaktadır. Bu standart, dokümente edilmiş bir BGYS’ni kurumun tüm iş riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için gereksinimleri kapsamaktadır. İş risklerini karşılamak amacıyla ISO/IEC 27002:2005’te ortaya konan kontrol hedeflerinin kurum içerisinde nasıl uygulanacağı ve denetleneceği ISO/IEC 27001:2005’te belirlenmektedir.

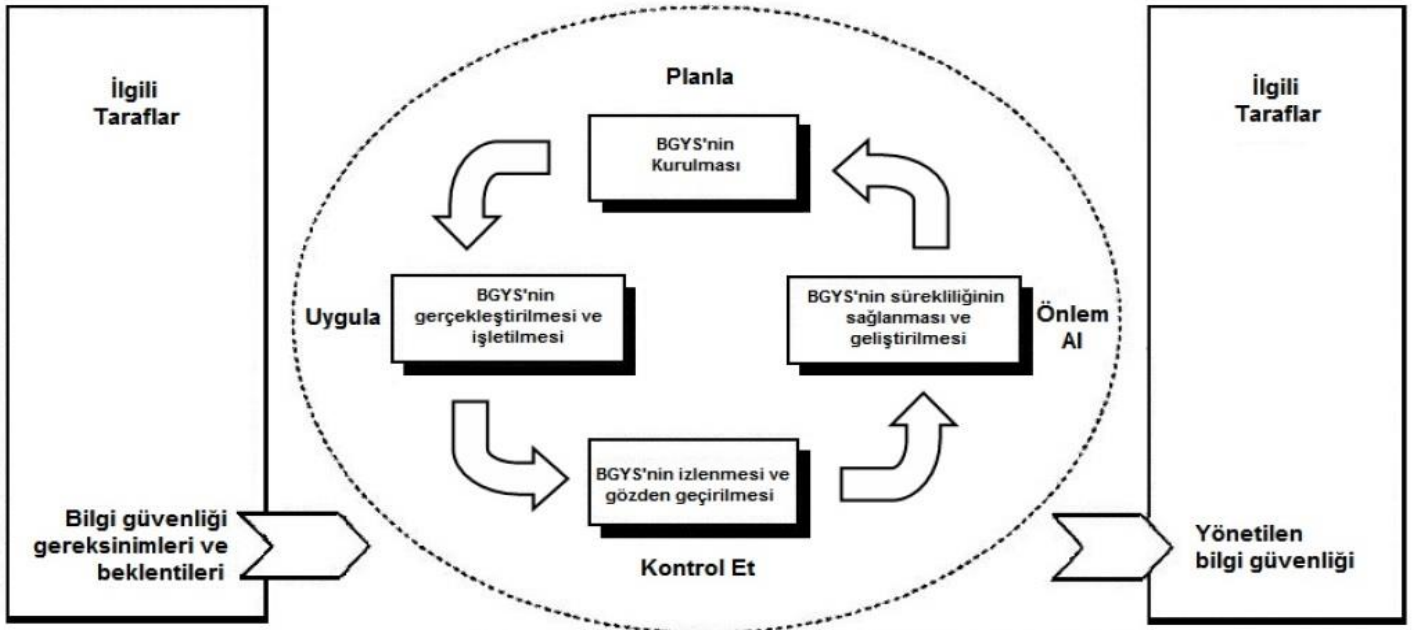


Şekil 4- TS ISO/IEC 27001

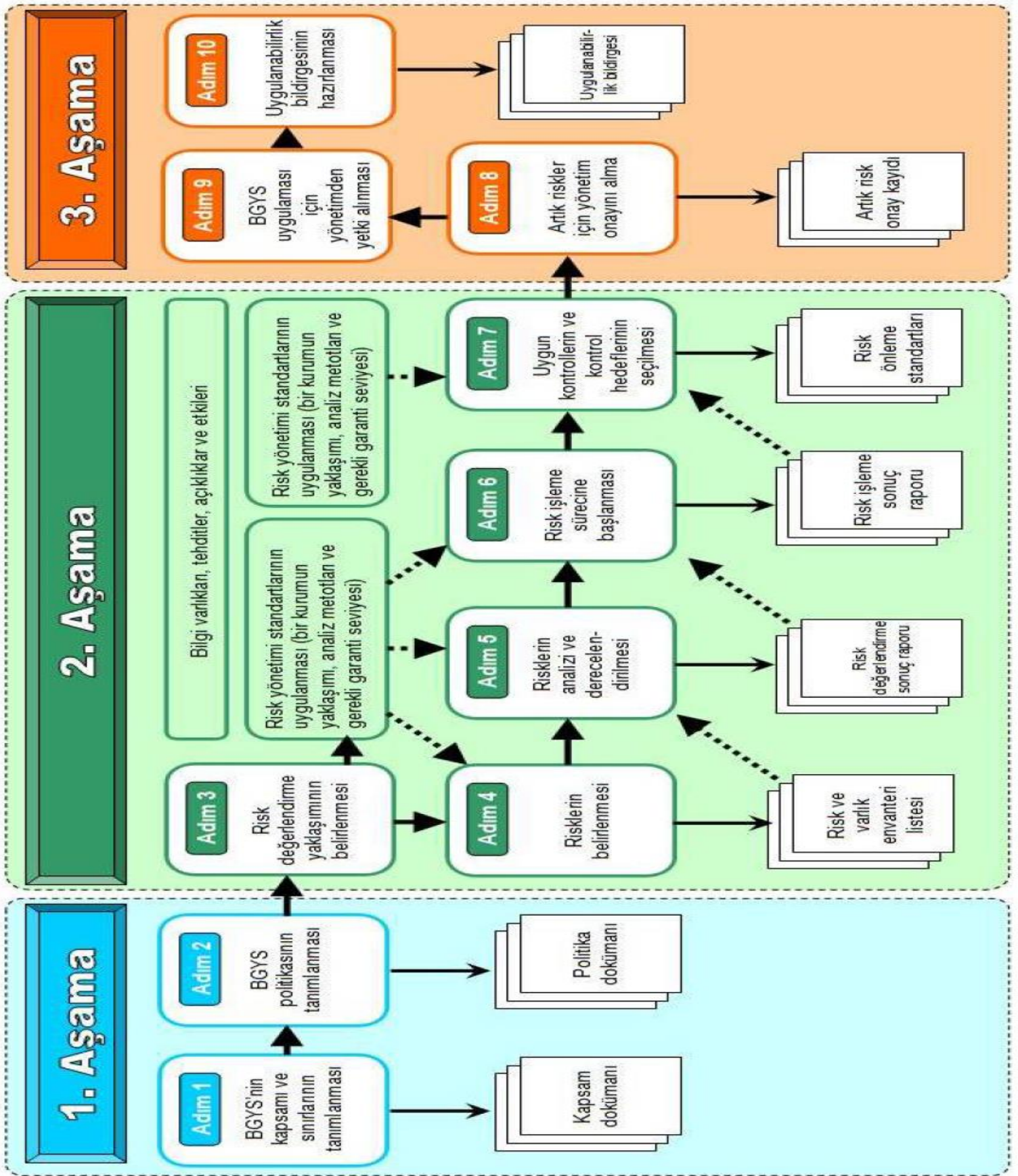
Her iki standardın Türkçe hali TSE tarafından sırasıyla TS ISO/IEC 17799:2005 ve TS ISO/IEC 27001:2005 isimleri ile yayınlanmıştır. Söz konusu standardın belgelendirmesi konusunda TSE tarafından TS 13268-1 BGYS Belgelendirmesi İçin Gereksinimler ve Hazırlık Kılavuzu standardı yayınlanmıştır.

ISO/IEC 27001 ve ISO/IEC 27002 standartları BGYS konusunda en temel başvuru kaynaklarıdır. Bu iki standart da doğrudan bilgi güvenliği konusunu ele alırlar. Teknik ve teknoloji bağımlı standartlar değildirler. Belli bir ürün veya bilgi teknolojisi ile ilgilenmezler. Hatta bilgi teknolojileri güvenliği dahi bu standartların içerisinde yer almaz. Tek ilgi alanı vardır, o da bilgi güvenliğidir. BGYS standartları kapsamında BGYS'in kurulumu, gerçekleştirilmesi, işletilmesi, izlenmesi, gözden geçirilmesi, sürdürülmesi ve tekrar gözden geçirilmesi için PUKÖ (Planla – Uygula – Kontrol et – Önlem al) modeli kullanılmaktadır. PUKÖ modelini görsel olarak anlatan Şekil 5, bir BGYS'nin bilgi güvenliği gereksinimlerini ve ilgili tarafların beklentilerini girdi olarak nasıl aldığını ve gerekli eylem ve prosesler aracılığıyla, bu gereksinimleri ve beklentileri karşılayacak bilgi güvenliği sonuçlarını nasıl ürettiğini gösterir.

Bilgi güvenliği yönetimi, başlangıç ve bitiş tarihleri olan bir proje gibi görülmemelidir. Sürekli devam eden bir gelişim süreci olarak düşünülmelidir. PUKÖ modelinde gösterildiği gibi (Planla – Uygula – Kontrol et – Önlem al) faaliyetleri bir döngü içinde durmaksızın sürekli devam etmelidir. PUKÖ modeli özet olarak ne yapılacağına karar verilmesi, kararların gerçekleştirilmesi, çalıştığının kontrol edilmesi hedefine uygun çalışmayan kontroller için önlemlerin alınmasıdır. BGYS kurulumu PUKÖ modelinin ilk adımını (Planla) teşkil etmektedir. Yerleşik bir sistemden bahsedebilmek için diğer adımların da uygulanması ve bunların bir döngü içinde yaşaması gerekir.



Şekil 5- PUKÖ Modeli



Şekil 6- BGYS Aşamaları

B.1. Risk Yönetimi

Risk, Fransızca *risque* olarak dilimize geçmiş olup sözlük anlamı “Riziko, zarara uğrama tehlikesi” şeklindedir. *Risk (riziko)*, bir olayın gerçekleşme olasılığı ve olaydan etkilenme olanağı olarak tanımlanmaktadır. Genellikle risk olumsuz bir durum yani tehlike olarak değerlendirilir. Bu nedenle risklerin olumsuz etkilerinden zarar görmemek için olasılıklar göz önüne alınarak, önlemler almaya yönelik, çalışma ve planlama faaliyetlerini içeren ve risk yönetimi olarak anılan bir disiplin ortaya çıkmıştır. Risk, gelecekte oluşabilecek potansiyel problemlere, tehdit ve tehlikelere işaret eden, belirli bir zaman aralığında, hedeflenen bir sonuca ulaşamama, kayba ya da zarara uğrama olasılığı olarak da tanımlanabilir.

Risk Yönetimi ise bir kurumun ya da kuruluşun çalışabilirliği, ticari kuruluşlar içinse öncelikle kârlılığını olumsuz yönde etkileyebilecek risk faktörlerinin belirlenmesi, ölçülmesi ve en alt düzeye indirilmesi sürecidir. Risk yönetiminde, riskin tamamıyla ortadan kaldırılması mümkün değildir. Sorunlara sistematik ve dikkatli bir şekilde yaklaşılması ve almaya karar verilen risklerin dikkatli yönetimi yoluyla gereksiz kayıpların engellenmesi amaçlanmaktadır. Başarılı bir risk yönetimi için, kuruluşların bilgi varlıklarına ve hedeflerine yönelik risklerin belirlenerek, analiz edilmesi, tanımlanan risklerin denetim altında tutularak izlenmesi gereklidir. Riski yönetmenin en doğru yolu, gerçekleşme olasılığı ve gerçekleştiğinde vereceği zarar en yüksek olan riskleri azaltacak bilgi teknolojisi risk yönetim sürecinin oluşturulmasıdır.

B.1.1.Varlıkların Belirlenmesi

Varlık, sistemin bir parçası olan ve kurum için değeri olan her şeydir. Varlık kurum için değer taşıdığından korunması gerekir. Bir BT sisteminde sadece yazılım ve donanımlar varlık olarak düşünülmemelidir. Aşağıdaki örnekler varlık olarak nitelendirilebilecek değerlerdir.

- Bilgi,
- Donanım (kişisel bilgisayarlar, yazıcılar, sunucular),
- yazılım (işletim sistemleri, geliştirilen uygulamalar, ofis programları),
- haberleşme cihazları (telefonlar, hatlar, kablolar, modemler, anahtarlama cihazları),
- dokümanlar(stratejik toplantıların tutanakları, sözleşmeler vb.),
- üretilen mallar,
- servisler,
- personel,
- kurumun prestiji / imajı.

Varlıkların belirlenmesinde kullanılabilecek bazı bilgi toplama teknikleri mevcuttur.

B.1.2.Tehditlerin Belirlenmesi

Tehdit, herhangi bir tehdit kaynağının kasıtlı olarak veya kazayla bir açıklığı kullanarak varlıklara zarar verme potansiyelidir. Tehdit kaynağı ise varlıklara zarar verme olasılığı olan olaylar ve durumlar olarak tanımlanabilir. En bilinen tehdit kaynakları şunlardır:

Doğal tehditler: Deprem, sel, toprak kayması, yıldırım düşmesi, fırtına gibi tehditler.

Çevresel tehditler: Uzun süreli elektrik kesintileri, hava kirliliği, sızıntılar vs.

İnsan kaynaklı Tehditler: İnsanlar tarafından yapılan veya yol açılan bilinçli veya bilinçsiz olaylar. Örneğin yanlış veri girişi, ağ saldırıları, zararlı yazılımların yüklenmesi, yetkisiz erişimler vs.

Tehdit değerlendirmesi sırasında hiçbir tehdidin küçümsenerek göz ardı edilmesi doğru değildir. Göz ardı edilen tehdit kurum güvenliğinde zayıflık yaratabilir.

Tehdit değerlendirmesi için gerekli girdi varlık sahiplerinden, kullanıcılardan, BT uzmanlarından, kurumun korunmasından sorumlu kişilerden elde edilebilir. Ayrıca tehditlerin belirlenmesinde tehdit katalogları da kullanılabilir.

Aşağıdaki tablo BT sistemlerinde sıklıkla karşılaşılan tehditleri ve bunların kaynaklarını içermektedir (tehdidin kaynağı bölümünde kullanılan kısaltmalar B: İnsan kaynaklı ve bilerek, K: İnsan kaynaklı ve kazayla, D: Doğal, Ç:Çevresel).

Tehdit	Tehdidin Kaynağı
Deprem	D
Sel	D
Fırtına	D
Yıldırım	D
Endüstriyel bilgi sızması	B,K
Bombalama ve silahlı saldırı	B
Yangın	B,K
Güç kesintisi	B,K,Ç
Su kesintisi	B,K,Ç
Havalandırma sisteminin arızalanması	B,K,Ç
Donanım arızaları	K
Güç dalgalanmaları	K,Ç
Tozlanma	Ç
Elektrostatik boşalma	Ç
Hırsızlık	B
Saklama ortamlarının izinsiz kullanılması	B,K
Saklama ortamlarının eskiyip kullanılmaz duruma gelmesi	K
Personel hataları	K
Bakım hataları/eksiklikleri	K
Yazılım hataları	B,K
Lisanssız yazılım kullanımı	B,K
Yazılımların yetkisiz kullanılması	B,K
Kullanıcı kimlik bilgilerinin çalınması	B,K
Zararlı yazılımlar	B,K
Yetkisiz kişilerin ağa erişimi	B
Ağ cihazlarının arızalanması	K
Hat kapasitelerinin yetersiz kalması	B,K
Ağ trafiğinin dinlenmesi	B
İletim hatlarının hasar görmesi	B,K
İletişimin dinlenmesi	B
Mesajların yanlış yönlendirilmesi	K
Mesajların yetkisiz kişilere yönlendirilmesi	B
İnkâr etme	B

Kaynakların yanlış kullanımı	K
Kullanıcı hataları	K
Personel yetersizliği	K

Tablo 1.BT sistemlerinde karşılaşılan tehditler ve kaynakları

B.1.3.Açıklıkların Belirlenmesi

Açıklık, sistem güvenlik prosedürlerinde, tasarımda, uygulamada veya iç kontrollerde bulunan ve bilgi güvenliği ihlal olayına sebep olabilecek zayıflık, hata veya kusurlardır. Açıklıklar tek başlarına tehlike oluşturmazlar ve gerçekleştirmeleri için bir tehdidin mevcut olması gerekir. Açıklık değerlendirmesi, tehditler tarafından gerçekleştirilebilecek açıklıkları ve bu açıklıkların ne kadar kolay gerçekleştirilebileceğini ele alır. Açıklıkların belirlenmesinde anket, birebir görüşme, dokümantasyon ve otomatik tarama araçları gibi yöntemler kullanılabilir.

B.1.4.Olasılık Değerlendirmesi

Risk analizinde bir açıklığın gerçekleşme olasılığının belirlenmesi büyük önem taşır ve tespit edilen tüm açıklıklar için olasılık değerlendirmesi yapılmalıdır. Olasılığın belirlenmesi için tehdit kaynağının motivasyonu ve becerisi, açıklığın cinsi, mevcut kontrollerin varlığı ve etkinliği göz önünde bulundurulmalıdır.

Olasılık değerlendirmesi için kurum kaç kademeli bir değerlendirme yapacağını ve kademelerin nasıl belirleneceğini tanımlamalıdır. Üç seviyeli bir olasılık değerlendirmesi için aşağıdaki örnek tablo kullanılabilir.

OLASILIK SEVİYESİ	OLASILIK SEVİYESİ
Yüksek	Tehdit kaynağı çok kabiliyetli ve motivasyonu yüksektir, açıklığın gerçekleşmesini engelleyecek kontroller bulunmamaktadır veya etkisizdir.
Orta	Tehdit kaynağı kabiliyetli ve motivasyonu yüksektir, açıklığın gerçekleşmesine engel olacak kontroller mevcuttur.
Düşük	Tehdit kaynağı daha az kabiliyetli ve motivasyonu daha düşüktür, açıklığın gerçekleşmesini engelleyecek veya çok zorlaştıracak kontroller mevcuttur.

Tablo 2.Üç seviyeli bir olasılık değerlendirmesi için olasılık tanımları

B.1.5.Etki Analizi

Risk derecelendirmesi yapabilmek için olasılık değerlendirmesinden sonra gelen adım etki analizidir. Etki analizinde herhangi bir açıklığın gerçekleşmesi halinde yaşanacak olası olumsuz etki seviyesi belirlenir. Bunun için varlığın görevi, kritikliği, varlığın etkilediği verinin hassasiyeti ve varlığın mali değeri göz önüne alınmalıdır. Bu bilgiler daha önceden yapılmış iş etki analizi raporlarından alınabilir. Eğer daha önce yapılmış böyle bir çalışma yoksa sistemin kritiklik seviyesi sistemin (ve sakladığı veya işlediği verinin) bütünlüğünü, gizliliğini ve erişilebilirliğini korumak için gerekli koruma göz önüne alınarak niceliksel olarak çıkarılabilir. Ayrıca sistemin yenilenme maliyeti, çalışmaması durumunda oluşabilecek gelir kaybı gibi bazı niteliksel etkiler de etki analizinde göz önüne alınabilir.

Niceliksel bir etki analizinde olasılık değerlendirmesinde olduğu gibi kurum kaç kademeli bir değerlendirme yapacağını ve kademelerin nasıl belirleneceğini tanımlamalıdır. Üç seviyeli bir etki değerlendirmesi için aşağıdaki örnek tablo kullanılabilir.

Etki Derecesi	Etki tanımı
YÜKSEK	Açıklığın gerçekleşmesi durumunda: Kurumun en önemli varlıkları çok fazla etkilenir veya kaybedilir ve mali zarar çok büyük olur. Kurumun çıkarları, misyonu ve prestiji büyük zarar görebilir veya etkilenebilir. İnsan hayatı kaybı veya ciddi yaralanmalar gerçekleşebilir.
ORTA	Açıklığın gerçekleşmesi durumunda: Kurumun önemli varlıkları etkilenir ve kurum mali zarara uğrar. Kurumun çıkarları, misyonu ve prestiji zarar görebilir veya etkilenebilir. Yaralanmalar gerçekleşebilir.
DÜŞÜK	Açıklığın gerçekleşmesi durumunda: Kurumun bazı varlıkları etkilenir Kurumun çıkarları, misyonu ve prestiji etkilenebilir.

Tablo 3. Üç seviyeli bir etki değerlendirmesi için etki tanımları

B.1.6.Risk Derecelendirmesi

Bu adımın amacı, varlıkları tehdit eden risklere değerler atayıp onları derecelendirmektir. Uygun kontrollerin seçilmesi burada belirlenen risklere ve seviyelere göre yapılır. Risk bir tehdidin bir açıklığı gerçekleştirme olasılığının, açıklığın ne kadar kolay gerçekleştirilebildiğinin ve mevcut veya planlanan kontrollerin yeterliliğinin bir fonksiyonudur. Yani kısaca olasılık değerlendirmesinde ve etki analizinde belirlenen değerlere bağlıdır. Risklerin ölçülebilmesi için risk sınıflandırma matrisi oluşturulmalıdır ve bu sınıflandırma için tanımlamalar yapılmalıdır.

B.1.7.Risk Derecelendirme Matrisi

Yukarıda örnek olarak verilen üç seviyeli olasılık değerlendirmesi ve etki analizi için şu şekilde bir risk derecelendirme matrisi oluşturulabilir.

		Etki Seviyesi		
		Düşük	Orta	Yüksek
Olma Olasılığı	Düşük	Düşük	Düşük	Düşük
	Orta	Düşük	Orta	Orta
	Yüksek	Düşük	Orta	Yüksek

Tablo 4.Örnek risk derecelendirme matrisi

Bu matristeki değerleri kurum kendisi belirlemelidir. Bunun için istenirse sayısal değerler kullanılabilir. Örneğin olma olasılıklarına 0 ile 1 arasında, etki seviyesine ise 0 ile 100 arasında değerler atanır. Risk dereceleri için aralıklar belirlenir. Olma olasılığı ve etki seviyesi çarpımının düştüğü aralık risk derecesini belirler. Örneğin bu matrise göre olma olasılığı “Orta” ve etki seviyesi “Yüksek” olan bir açıklığın risk derecesi “Orta” olarak sınıflandırılmıştır.

B.1.8.Risk Derecelerinin Tanımı

Risk derecelendirme matrisinde belirlenen risk dereceleri bir açıklığın gerçekleşmesi halinde karşı karşıya olunan riski belirlemektedir. Bu risk derecelerinin tanımlanması yönetimin risklerle ilgili alacağı kararlar açısından önemlidir. Ayrıca bu aşamada kurumun kabul edebileceği risk seviyesi de belirlenmelidir. Belirlenen bu seviyeye göre kurum bazı riskleri kabul ederek karşı önlem almamayı tercih edebilir.

Yukarıdaki risk seviye matrisine uygun olarak aşağıdaki tanımlamalar örnek olarak gösterilebilir.

Risk Derecesi	Risk Açıklaması ve yapılması gerekenler
Yüksek	Düzeltilici önlemlerin alınması şarttır. Mevcut sistem çalışmaya devam edebilir ama hangi önlemlerin alınacağı ve nasıl uygulanacağı olabildiğince çabuk belirlenmelidir ve önlemler uygulanmalıdır.
Orta	Düzeltilici önlemlerin alınması gerekmektedir. Hangi önlemlerin alınacağı ve nasıl uygulanacağına dair plan makul bir süre içerisinde hazırlanmalı ve uygulanmaya başlanmalıdır.
Düşük	Önlem alınıp alınmayacağı sistem sahibi/sorumlusu tarafından belirlenmelidir. Eğer yeni önlemler alınmayacaksa risk kabul edilmelidir.

Tablo 5. Risk dereceleri ve tanımları

B.1.9.Uygun Kontrollerin Belirlenmesi

Yapılan risk derecelendirme çalışmalarının sonucunda risklerin azaltılmasını veya ortadan kaldırılmasını sağlayacak kontrol önerileri belirlenmelidir. Önerilecek kontrollerin amacı riski kurumun kabul edebileceği bir değere düşürmek olmalıdır. Önerilecek kontrollerde kontrollerin etkinliği, yasalar ve düzenlemeler, iş yapma biçimine getireceği değişiklikler, kurum politikaları ve güvenlik konuları dikkate alınması gereken başlıca konulardır.

Uygulanabilecek olası kontroller belirlenirken başvurabilecek kaynaklardan biri “TS ISO/IEC 27001:2005 Bilgi Teknolojisi – Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler” standardıdır. Bu standart, güvenlik politikası, bilgi güvenliği organizasyonu, varlık yönetimi, insan kaynakları güvenliği, fiziksel ve çevresel güvenlik, haberleşme ve işletim yönetimi, erişim kontrolü, bilgi sistemleri edinim, geliştirme ve bakımı, bilgi güvenliği ihlal olayı yönetimi, iş sürekliliği yönetimi ve uyum ana başlıkları altında pek çok kontrol önerisi içermektedir. Ayrıca bu kontrollerin gerçekleştirilmesine ait öneriler ve en iyi uygulamalar için TS ISO/IEC 27002:2005 standardına başvurulmalıdır.

B.1.10.Sonuçların Dokümantasyonu

Sonuçların dokümantasyonu risk analizi sürecinde en önemli adımlardan biridir. Bu dokümanlar mevcut risk ve kontrollerin herkes tarafından bilinmesini sağlarlar. Ayrıca bu dokümanlar daha sonraki risk analizlerine girdi teşkil ederler.

Risk analizi süreci tamamlandığında sonuçlar bir rapor olarak dokümanite edilmelidir. Bu rapor yönetimin ve süreç sahiplerinin politikalarda, prosedürlerde, bütçede ve sistemin kullanımında veya yönetiminde yapılacak değişikliklerde karar verirken kullanacağı yönetsel bir rapordur.

Yönetimin riskleri rahat bir şekilde anlayabilmesi için rapor açık ve sistematik olmalıdır. Belirlenen riskler için yapılması gerekenlere, bu rapor göz önünde bulundurularak karar verilecektir.



BİLGİ GÜVENLİĞİ POLİTİKALARI



BOĞİTİKAĞAKI
BİLGİ GÜVENLİĞİ





C. POLİTİKALAR

C.1. İnsan Kaynakları ve Zafiyetleri Yönetimi

- C.1.1.** Çalışan personele ait şahsi dosyalar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde olmamalıdır.
- C.1.2.** Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmelidir.
- C.1.3.** ÇKYS üzerinden kişiyle ilgili bir işlem yapıldığında(izin kağıdı gibi) ekranda bulunan kişisel bilgilerin diğer kişi veya kişilerce görülmesi engellenmelidir.
- C.1.4.** Diğer kişi, birim veya kuruluşlardan telefonla ya da sözlü olarak çalışanlarla ilgili bilgi istenilmesi halinde hiçbir suretle bilgi verilmemelidir.
- C.1.5.** İmha edilmesi gereken (müsvedde halini almış ya da iptal edilmiş yazılar vb.) kağıt kesme makinasında imha edilmelidir.
- C.1.6.** Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmamalıdır.
- C.1.7.** Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.
- C.1.8.** Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.
- C.1.9.** Görevden ayrılan personelin kimlik kartı alınmalı ve yazıyla idareye iade edilmelidir.

C.2. Fiziksel ve Çevresel Güvenlik

Fiziksel ve çevresel güvenlik, işyerine yetkisiz erişimlerin engellenmesi ve bilgi varlıklarının hırsızlığa veya tehlikeye karşı korunmasıdır.

Geçmiş zamanlarda önemli bilgiler, taşlara kazınarak daha sonra da kâğıtlara yazılarak fiziksel ortamlarda saklanmış, duvarlarla, kale hendekleriyle ve başlarına dikilen nöbetçilerle koruma altına alınmıştır. Çoğu zaman fiziksel koruma yeterli kalmamış ve bilgilerin çalınması ve başka kişilerin eline geçmesi engellenememiştir. Bu durum, verileri korumak için fiziksel güvenliğin tek başına yeterli olmadığını göstermektedir.

Günümüzde de fiziksel güvenlik önemini korumakta ve bu konuyla ilgili gerekli çalışmalar yapılmaktadır. Örneğin, bina etrafına yüksek duvarlar ya da demirler yapılması, bina girişinde özel güvenlik ekiplerinin bulundurulması, önemli verilerin tutulduğu odaların kilitlenmesi ya da bu odalara şifreli güvenlik sistemleri ile girilmesi gibi önlemler kullanılmaktadır.

C.2.1. Fiziksel Güvenlik Sınırı;

C.2.2.1 Bilgi işleme servisini korumak amacıyla herhangi bir fiziksel sınır güvenliği tesisi kurulmuş olmalıdır. (Kart kontrollü giriş, duvarlar, insanlı nizamiye)

C.2.2.1 Fiziksel sınır güvenliği, içindeki bilgi varlıklarının güvenlik ihtiyaçları ve risk değerlendirme sürecinin sonucuna göre oluşturulmalıdır.

C.2.2. Fiziksel Giriş Kontrolleri;

C.2.2.1 Kurum içerisinde belli yerlere sadece yetkili personelin girişine izin verecek şekilde kontrol mekanizmaları kurulmalıdır.

C.2.2.2 Kapsam ve prosedürü idarelerce belirlenmek suretiyle ziyaretçilerin giriş ve çıkış zamanları kaydedilmelidir.

C.2.2.3 Hassas bilgilerin bulunduğu alanlar (kimlik doğrulama kartı ve PIN koruması gibi yöntemlerle) yetkisiz erişime kapatılmalıdır.

C.2.2.4 Kapsam ve prosedürü idarelerce belirlenmek suretiyle tüm personel ve ziyaretçiler güvenlik elemanları tarafından rahatça teşhis edilmelerini sağlayacak kimlik kartlarını devamlı takmalıdır.

C.2.2.5 Güvenli alanlara erişim hakları düzenli olarak gözden geçiriliyor olmalıdır.

C.2.3. Ofislerin ve Odaların Güvenliğinin Sağlanması;

C.2.3.1 Ofisler ve odalarla ilgili fiziksel güvenlik önlemleri alınmalıdır.

C.2.3.2 Personel güvenliği ve sağlığı ile ilgili yönetmelikler uygulanmalıdır.

C.2.3.3 Kritik tesisler kolayca ulaşılamayacak yerlere kurulmuş olmalıdır.

C.2.3.4 Binada bilgi işlem faaliyetlerinin yürütüldüğüne dair işaret, tabela vb. bulunmamasına dikkat edilmelidir.

C.2.3.5 Bilgi işlem merkezlerinin konumunu içeren dâhili/harici telefon rehberleri halka kapalı olmalıdır.

C.2.4. Harici ve Çevresel Tehditlerden Korunma;

C.2.4.1 Yangın, sel, deprem, patlama ve diğer tabii afetler veya toplumsal kargaşa sonucu oluşabilecek hasara karşı fiziksel koruma tedbirleri alınmalı ve uygulanmalıdır.

C.2.4.2 Komşu tesislerden kaynaklanan potansiyel tehditler göz önünde bulundurulmalıdır.

C.2.4.3 Yedeklenmiş materyal ve yedek sistemler ana tesisten yeterince uzak bir yerde konuşlandırılmış olmalıdır.

C.2.5. Güvenli Alanlarda Çalışma;

C.2.5.1 Güvenli çalışma alanlarındaki personel veya bu alanda yürütülmekte olan çeşitli faaliyetlerde bulunan personel ve üçüncü parti çalışanları için "ihtiyacı kadar bilme" prensibi uygulanmalıdır.

C.2.5.2 Kayıt cihazlarının güvenli alanlara sokulmasına engel olunmalıdır.

C.2.5.3 Kullanılmayan güvenli alanlar kilitleniyor ve düzenli olarak kontrol ediliyor olmalıdır.

C.2.5.4 Kötü niyetli girişimlere engel olmak için güvenli bölgelerde yapılan çalışmalara nezaret edilmelidir.

C.2.5.5 Güvenli bölgelere örneğin sistem odasına yapılan girişler kayıt altına alınmalıdır.

C.2.6. Bilgi işlem servisleri ile dağıtım ve yükleme alanları ve yetkisiz kişilerin tesislere girebileceği noktalar birbirinden izole edilmiş olmalıdır.

C.3. Ekipman Güvenliği

C.3.1. Masalarda ya da çalışma ortamlarında korumasız bırakılmış bilgiler yetkisiz kişilerin erişimleriyle gizlilik ilkesinin ihlaline, yangın, sel, deprem gibi felaketlerle bütünlüğünün bozulmalarına ya da yok olmalarına sebep olabilir. Tüm bu veya daha fazla tehditleri yok edebilmek için aşağıda yer alan belli başlı temiz masa kurallarına ilişkin politikalar geliştirilmeli ve bu politikaların çalışanlar tarafından haberdar olunması sağlanmalıdır.

C.3.2. Belli başlı temiz masa kuralları;

C.3.2.1 Hassas bilgiler içeren evraklar, bilgi ve belgelerin masa üzerinde kolayca ulaşılabilir yerlerde ve açıkta bulunmaması gereklidir. Bu bilgi ve belgelerin kilitli yerlerde muhafaza edilmesi gerekmektedir.

C.3.2.2 Personelin kullandığı masaüstü veya dizüstü bilgisayarlar iş sonunda ya da masa terkedilecekse ekran kilitlenmelidir. Bu işlem Windows + L tuşuna basılarak yapılabilir.

C.3.2.3 Sistemlerde kullanılan şifre, telefon numarası ve T.C kimlik numarası gibi bilgiler ekran üstlerinde veya masa üstünde bulunmamalıdır.

C.3.2.4 Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler kâğıt öğütücü, disk/disket kıyıcı, yakma vb. metotlarla imha edilmeli, bilginin geri dönüşümü ya da yeniden kullanılabilir hale geçmesinin önüne geçilmelidir.

C.3.2.5 Faks makinelerinde gelen giden yazılar sürekli kontrol edilmeli ve makinede yazı bırakılmamalıdır.

C.3.2.6 Her türlü bilgiler, şifreler, anahtarlar ve bilginin sunulduğu sistemler, ana makineler (sunucu), PCler vb. cihazlar yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde başıboş bırakılmamalıdır.

C.3.3. Ekipman Yerleşimi ve Koruması;

C.3.3.1 Ekipman yerleşimi yapılırken çevresel tehditler ve yetkisiz erişimden kaynaklanabilecek zararların asgari düzeye indirilmesine çalışılmalıdır.

C.3.3.2 Ekipman, gereksiz erişim asgari düzeye indirilecek şekilde yerleştirilmelidir.

C.3.3.3 Kritik veri içeren araçlar yetkisiz kişiler tarafından gözlenemeyecek şekilde yerleştirilmelidir.

C.3.3.4 Özel koruma gerektiren ekipman izole edilmiş olmalıdır.

C.3.3.5 Nem ve sıcaklık gibi parametreler izlenmelidir.

C.3.3.6 Hırsızlık, yangın, duman, patlayıcılar, su, toz, sarsıntı, kimyasallar, elektromanyetik radyasyon, sel gibi potansiyel tehditlerden kaynaklanan riskleri düşürücü kontroller uygulanmalıdır.

C.3.3.7 Paratoner kullanılmalıdır.

C.3.3.8 Bilgi işlem araçlarının yakınında yeme, içme ve sigara içme konularını düzenleyen kurallar olmalıdır.

C.3.4. Destek Hizmetleri;

C.3.4.1 Elektrik, su, kanalizasyon ve iklimlendirme sistemleri destekledikleri bilgi işlem dairesi için yeterli düzeyde olmalıdır.

C.3.4.2 Elektrik şebekesine yedekli bağlantı, kesintisiz güç kaynağı gibi önlemler ile ekipmanları elektrik arızalarından koruyacak tedbirler alınmış olmalıdır.

C.3.4.3 Yedek jeneratör ve jeneratör için yeterli düzeyde yakıt bulundurulmalıdır.

C.3.4.4 Su bağlantısı iklimlendirme ve yangın söndürme sistemlerini destekleyecek düzeyde olmalıdır.

C.3.4.5 Acil durumlarda iletişimin kesilmemesi için servis sağlayıcıdan iki bağımsız hat alınmalıdır.

C.3.4.6 Kurum bu konuda yasal yükümlülüklerini yerine getirmelidir.

C.3.5. Kablolama Güvenliği;

C.3.5.1 Güç ve iletişim kablolarının fiziksel etkilere ve dinleme faaliyetlerine karşı korunması için önlemler alınmış olmalıdır.

C.3.5.2 Kablolar yeraltında olmalıdır.

C.3.5.3 Karışmanın ("interference") olmaması için güç kabloları ile iletişim kabloları ayrılmış olmalıdır.

C.3.5.4 Hatalı bağlantıların olmaması için ekipman ve kablolar açıkça etiketlenmiş ve işaretlenmiş olmalıdır.

C.3.5.5 Hassas ve kritik bilgiler için ekstra güvenlik önlemleri alınmalıdır.

C.3.5.6 Alternatif yol ve iletişim kanalları mevcut olmalıdır.

C.3.5.7 Fiber optik altyapı yapılandırılmalıdır.

C.3.5.8 Bağlantı panelleri ve odalara kontrollü erişim altyapısı kurulmuş olmalıdır.

C.3.6. Ekipman Bakımı;

C.3.6.1 Ekipmanın bakımı doğru şekilde yapılmalıdır.

C.3.6.2 Ekipmanın bakımı, üreticinin tavsiye ettiği zaman aralıklarında ve üreticinin tavsiye ettiği şekilde yapılmalıdır.

C.3.6.3 Bakım sadece yetkili personel tarafından yapılıyor olmalıdır.

C.3.6.4 Tüm şüpheli ve mevcut arızalar ve bakım çalışmaları için kayıt tutulmalıdır.

C.3.6.5 Ekipman bakım için kurum dışına çıkarılırken kontrolden geçirilmelidir.

C.3.6.6 İçindeki hassas bilgiler silinmelidir.

C.3.6.7 Ekipman sigortalıysa, gerekli sigorta şartları sağlanıyor olmalıdır.

C.3.6.8 Üretici garantisi kapsamındaki ürünler için garanti süreleri kayıt altına alınmalı ve takip edilmelidir.

C.3.7. Kurum Dışındaki Ekipmanın Güvenliği;

C.3.7.1 Kurum alanı dışında bilgi işleme için kullanılacak ekipman için yönetim tarafından yetkilendirme yapılıyor olmalıdır.

C.3.7.2 Tesis dışına çıkarılan ekipmanın başıboş bırakılmamasına, seyahat halinde dizüstü bilgisayarların el bagajı olarak taşınmasına dikkat edilmelidir.

C.3.7.3 Cihazın muhafaza edilmesi ile ilgili olarak üretici firmanın talimatlarına uyulmalıdır.

C.3.7.4 Evden çalışma ile ilgili tedbirler alınmalıdır. Cihazların sigortaları, tesis dışında korumayı da kapsamalıdır.

C.3.7.5 Kurum alanı dışında kullanılacak ekipmanlar için uygulanacak güvenlik önlemleri, tesis dışında çalışmaktan kaynaklanacak farklı riskler değerlendirilerek belirlenmelidir.

C.3.8. Ekipmanın Güvenli İmhası ya da Tekrar Kullanımı;

C.3.8.1 Ekipman imha edilmeden önce gizli bilginin bulunduğu depolama cihazı fiziksel olarak imha edilmelidir.

C.3.8.2 Depolama cihazının içerdiği bilginin bir daha okunamaması için klasik silme veya format işlemlerinin ötesinde yeterli düzeyde işlem yapılmalıdır.

C.3.9. Varlıkların Kurumdan Çıkarılması;

C.3.9.1 Ekipman, bilgi veya yazılımın yetkilendirme olmadan tesis dışına çıkarılmamasını sağlayan kontrol mekanizması oluşturulmalıdır.

C.3.9.2 Kurum varlıklarının yetkisiz olarak kurum dışına çıkarılıp çıkarılmadığını saptamak için denetleme yapılmalıdır.

C.3.9.3 Kurum çalışanları bu tip denetlemelerden haberdar olmalıdır.

C.4. İşletim Sistemleri ve Son Kullanıcı Güvenliği

C.4.1. İşletim Sistemleri Güvenliği

C.4.1.1 Kurum son kullanıcı düzeyinde hangi işletim sistemini kullanacağına karar verir ve bu işletim sistemine uygun yazılım donanım sistemlerinin kurulumunu temin eder.

C.4.1.2 Kurum, işletim sistemlerinin güncel ve güvenli olması için yama yönetimi yapmalıdır.

C.4.1.3 Kurum, bilgisayar başındaki kullanıcının doğru kullanıcı olup olmadığını tespit etmek için her bilgisayarda etki alanı kimlik doğrulamasını sağlamalıdır.

C.4.1.4 Kurum, mevcut envanteri haricindeki donanımların kurum bilgisayarlarında kullanımını engellemelidir.

C.4.1.5 İşletim sistemlerinde kurulumda gelen yönetici hesaplarının (Administrator, root) kaba kuvvet saldırılarına karşı, Microsoft ürünlerinde pasif hale getirilmesi, Linux tabanlı ürünlerde root hesabına ssh erişiminin engellenmesi gerekir.

C.4.2. Son Kullanıcı Güvenliği

C.4.2.1. Son kullanıcılar sistemlere, etki alanları dâhilinde kendilerine verilmiş kullanıcı adı ve şifreleri ile bağlanmalıdır.

C.4.2.2. Son kullanıcılar, yetkileri dâhilinde sistem kaynaklarına ulaşabilmeli ve internete çıkabilmelidir.

C.4.2.3. Son kullanıcıların yetkileri, içinde bulundukları grup politikasına göre belirlenmelidir.

C.4.2.4. Son kullanıcıların aktiviteleri, güvenlik zafiyetlerine ve bilgi sızdırmalarına karşı loglanarak kayıt altına alınmalıdır.

C.4.2.5. Güvenlik zafiyetlerine karşı, son kullanıcılar kendi hesaplarının ve/veya sorumlusu oldukları cihazlara ait kullanıcı adı ve şifre gibi kendilerine ait bilgilerin gizliliğini korumalı ve başkaları ile paylaşmamalıdır.

C.4.2.6. Son kullanıcılar bilgisayarlarında ki ve sorumlusu oldukları cihazlarda ki bilgilerin düzenli olarak yedeklerini almalıdır.

C.4.2.7. Son kullanıcılar, güvenlik zafiyetlerine sebep olmamak için, bilgisayar başından ayrılırken mutlaka ekranlarını kilitlemelidir.

C.4.2.8. Son kullanıcılar, bilgisayarlarında ya da sorumlusu oldukları sistemler üzerinde USB flash bellek ve/veya harici hard disk gibi removable media (taşınabilir medya) bırakmamalıdır.

C.4.2.9. Son kullanıcılar, mesai bitiminde bilgisayarlarını kapatmalıdır.

C.4.2.10. Kullanıcı bilgisayarlarında, güncel anti virüs bulunmalıdır.

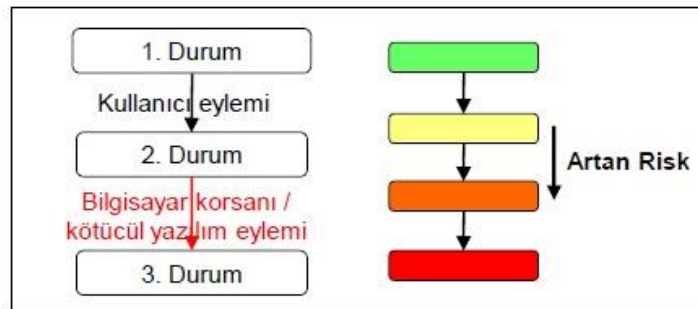
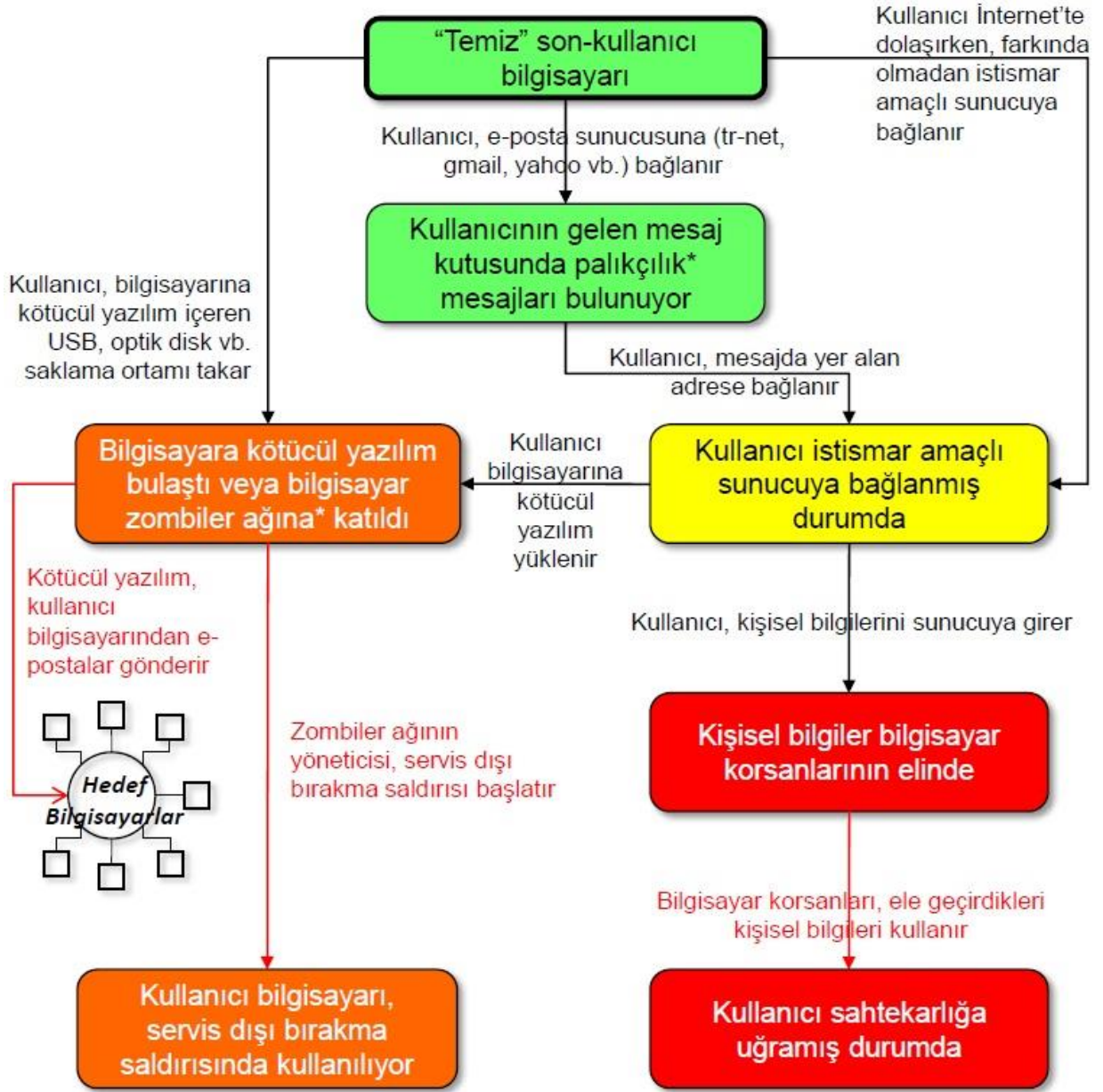
C.4.2.11. Kurum, son kullanıcı güvenliğine dair oluşturulmuş grup politikalarını, etki alanı üzerinden kullanıcı onayı olmaksızın uygulamalıdır.

C.4.2.12. Kurum, son kullanıcıların farkında olmadan yapabilecekleri ve sonunda zafiyet yaratabilecek değişiklikleri merkezi grup politikalarıyla engellemelidir.

C.4.2.13. Kullanıcılarına yeni parolaları bildirilirken sms gibi daha güvenli yöntemler kullanılmalıdır.

C.4.2.14. Temiz masa, temiz ekran ilkesi benimsenmeli ve hayata geçirilmelidir.

Son kullanıcılar, sahtekarlık ve servis dışı bırakma* saldırıları



Şekil 7- Son Kullanıcı Güvenliği

C.5. Parola Güvenliği

C.5.1. Güvenliğin oluşturulacağı birim için kullanılan programlarda uygulanan parola standardı belirlenmeli, bu parola sistemi aşağıdaki unsurları içerecek standarda getirilmelidir.

C.5.2. Bilgi Güvenliği Yetkilisinin devreye girmesi ile parola standardı belirlenerek uygulanmaya başlanmalı, geliştirilerek aşağıdaki yapıya çekilmesi konusunda plan yapılmalıdır.

C.5.2.1 Parola en az 8 karakterden oluşmalıdır.

C.5.2.2 Harflerin yanı sıra, rakam ve "? , @ , ! , # , % , + , - , * , %" gibi özel karakterler içermelidir.

C.5.2.3 Büyük ve küçük harfler bir arada kullanılmalıdır.

C.5.3. Bu kurallara uygun parola oluştururken genelde yapılan hatalardan dolayı saldırganların ilk olarak denedikleri parolalar vardır. Bu nedenle parola oluştururken aşağıdaki önerileri de dikkate almak gerekir.

C.5.3.1 Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır.

(Örneğin 12345678, qwerty, doğum tarihiniz, çocuğunuzun adı, soyadınız gibi)

C.5.3.2 Sözlükte bulunabilen kelimeler parola olarak kullanılmamalıdır.

C.5.3.3 Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş parolalar kullanılmamalıdır.

C.5.4. Basit bir kelimenin içerisindeki harf veya rakamları benzerleri ile değiştirilerek güçlü bir parola elde edilebilir.

'B' yerine 8	'Z' yerine 2	Örneğin
'l', 'i', 'L', 'I' yerine 1	'O' harfi yerine 0	Balıkçıl-Kazak 8a11kç11-Ka2ak
'S' yerine 5 'G' yerine 6	'g' yerine 9	Solaryum! 501aryum!

Tablo 6. Güçlü parola yöntemleri

C.5.5. Basit bir cümle ya da ifade içerisindeki belirli kelimeler özel karakter veya rakamlarla değiştirilerek güçlü bir parola elde edilebilir.

'T', 't' yerine '+'	'Ş', 'ş' yerine '\$'	Örneğin
"kar", "yıldız" yerine '*'	"dolar", "para" yerine '\$'	"Dün Kar Yağmı" : Dün*Yağm1\$
"Soru" yerine '?'	"gibi" yerine '~'	"Şeker gibi bir soru sordu" : Şeker~1?Sordu
"gül" yerine ':')	"eksi" yerine '-'	"Tek eksikim bir güldü" : 1-ğim1:)dü
"bir", "tek" yerine 1	"yüz", "yüzde" yerine '%'	"Yüzeysel bir soru eşittir eksi puan": %eysel1?=-Puan

Tablo 7. Güçlü parola yöntemleri

C.6. Kriptolama Yönetimi

C.6.1. Kriptografik kontroller aşağıdaki maksatlarla kullanılır;

C.6.1.1 Gizlilik: Saklanan veya iletilen hassas veya kritik bilgiyi korumak için şifrelemenin kullanılması,

C.6.1.2 Bütünlük/Güvenilirlik: Saklanan veya iletilen hassas veya kritik bilginin güvenilirlik veya bütünlüğünü korumak için sayısal imzaların veya mesaj doğrulama kodlarının kullanılması,

C.6.1.3 İnkâr edilemezlik: Bir olay veya faaliyetin oluşumu veya oluşmadığının kanıtını elde etmek için kriptografik tekniklerin kullanılması.

C.6.2. Personelin gönderdiği maillerde, hiçbir şekilde yönetici, kullanıcı gibi hesap şifreleri bulundurulmamalıdır.

C.6.3. İşletim sistemi üzerinde saklanan kullanıcı ve yönetici hesabı şifrelerinin kriptolu olarak saklandığı belirli zaman aralıklarında kontrol edilmelidir.

C.6.4. Sunuculara kriptolu bağlantı ile bağlanılmalı, kripto kullanmayan yöntemler tercih edilmemelidir. Düz metin kullanarak veri alışverişi yapan yöntemlerin kullandığı portlar gerekirse kapatılmalıdır.

C.6.5. Kripto kullanımı ile hangi iş bilgisinin korunacağı ile ilgili genel prensipler belirlenmelidir.

C.6.6. Risk belirleme esasına dayalı olarak gereksinim duyulan koruma seviyesi ile şifreleme algoritmasının türü, gücü ve niteliği ortaya konulmalıdır.

C.6.7. Taşınabilir ortam, cihaz ve iletişim hatlarında iletilen hassas bilginin korunması için şifreleme mekanizmalarının kullanımı belirlenmelidir.

C.6.8. Organizasyon çapında etkin bir uygulama için uyarlanması gereken standartlar ortaya konulmalıdır.

C.6.9. İçerik denetimi üzerinden yapılan kontrollerde şifrelenmiş bilgi kullanımının etkileri değerlendirilmelidir.

C.6.10. Kriptografik anahtarların korunması, şifrelenmiş bilginin kaybolması, tehlikeye düşmesi veya hasar görmesi durumunda tekrar geri alınması ile ilgili metotları içeren anahtar yönetimi uygulanmalıdır.

C.6.11. Politikanın uygulanması, anahtar üretimini de içeren anahtar yönetimi ile ilgili görevler ve sorumluluklar belirlenmelidir.

C.6.12. Anahtar yönetiminde göz önüne alınacak hususlar aşağıda belirtilmiştir;

- Farklı kriptografik sistemler ve farklı uygulamalar için anahtar üretimi,
- Açık anahtar sertifikası üretimi ve elde edilmesi,
- Anahtarın alınmasını müteakip nasıl faaliyete geçirileceği dâhil kullanıcılara anahtar dağıtımı,
- Yetkili kullanıcıların anahtar erişiminin sağlanmasını da kapsayan anahtarların saklanması,
- Anahtarların ne zaman ve nasıl değiştirileceğinin kurallarını da kapsayan anahtarların değişimi ve güncellenmesi,
- Güvenliği tehlikeli bir duruma düşmüş anahtarlar,
- Anahtarların geri alımı ve kullanılmaz hale getirilmesini kapsayan anahtarın yürürlükten kaldırılması (Ör. Anahtarın güvenliğinin tehlikeli bir duruma düşmüş olması veya kullanıcının kuruluştan ayrılması durumları),
- İş süreklilik yönetiminin bir parçası olarak kaybolan veya bozulan anahtarların kurtarılması (Örn: Kriptolanmış bilginin kurtarılması),
- Anahtarların arşivlenmesi,
- Anahtarların imhası,
- Anahtar yönetimi ile ilgili faaliyetlerin izleme kayıtlarının (log) tutulması.

C.7. İnternet ve Elektronik Posta Güvenliği

C.7.1. Kullanıcıya resmi olarak tahsis edilen e-posta adresi, kötü amaçlı ve kişisel çıkar amaçlı kullanılamaz.

C.7.2. İş dışı konulardaki haber grupları kurumun e-posta adres defterine eklenemez.

C.7.3. Kurumun e-posta sunucusu, kurum içi ve dışı başka kullanıcılara SPAM, phishing mesajlar göndermek için kullanılamaz.

C.7.4. Kurum içi ve dışı herhangi bir kullanıcı ve gruba; küçük düşürücü, hakaret edici ve zarar verici nitelikte e-posta mesajları gönderilemez.

C.7.5. İnternet haber gruplarına mesaj yayımlanacak ise, kurumun sağladığı resmi e-posta adresi bu mesajlarda kullanılamaz. Ancak iş gereği üye olunması yararlı internet haber grupları için yöneticisinin onayı alınarak Kurumun sağladığı resmi e-posta adresi kullanılabilir.

C.7.6. Hiçbir kullanıcı, gönderdiği e-posta adresinin kimden bölümüne yetkisi dışında başka bir kullanıcıya ait e-posta adresini yazamaz.

C.7.7. E-posta gönderiminde konu alanı boş bir e-posta mesajı göndermemelidir.

C.7.8. Konu alanı boş ve kimliği belirsiz hiçbir e-posta açılmamalı ve silinmelidir.

C.7.9. E-postaya eklenecek dosya uzantıları “.exe”, “.vbs” veya yasaklanan diğer uzantılar olamaz. Zorunlu olarak bu tür dosyaların iletilmesi gerektiği durumlarda, dosyalar sıkıştırılarak (zip veya rar formatında) mesaja eklenmelidir.

C.7.10. Bakanlık ile ilgili olan gizli bilgi, gönderilen mesajlarda yer almamalıdır. Bunun kapsamı içerisine iliştirilen öğeler de dâhildir. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir.

C.7.11. Kullanıcı, kurumun e-posta sistemi üzerinden taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında Sistem Yönetimine haber verilmelidir.

C.7.12. Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçla e-posta gönderilmemelidir.

C.7.13. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletmeyip, Sistem Yönetimine haber verilmelidir.

C.7.14. Spam, zincir, sahte vb. zararlı olduğu düşünülen e-postalara yanıt verilmemelidir.

C.7.15. Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.

C.7.16. Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul etmektedir. Suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların içeriğinden kullanıcı sorumludur.

C.7.17. Kullanıcı, gelen ve/veya giden mesajlarının kurum içi veya dışındaki yetkisiz kişiler tarafından okunmasını engellemelidir.

C.7.18. Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e-postalara herhangi bir işlem yapmaksızın Sistem Yönetimine haber vermelidir.

C.7.19. Kullanıcı, kurumsal mesajlarına, kurum iş akışının aksamaması için zamanında yanıt vermelidir.

C.7.20. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar Sistem Yönetimine haber verilmelidir.

C.7.21. Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolasının kırıldığını fark ettiği anda Sistem Yönetimine haber vermelidir.

C.8. Sunucu ve Sistem Güvenliği

C.8.1. Sunucu Güvenlik Politikaları;

C.8.1.1 Bakanlığa hizmet veren tüm uygulama, veri tabanı sunucuları ve disk üniteleri Bakanlık veri merkezlerinde veya idarece uygun görülen güvenli fiziksel alanlarda konumlandırılmalıdır.

C.8.1.2 Farklı lokasyonlarda konumlandırılmış yerel sunucuların Sağlık Özel Ağına bağlanması engellenmelidir.

C.8.1.3 Servislere erişimler kaydedilmeli ve servis erişimleri, erişim kontrol yöntemleri ile sağlanmalıdır.

C.8.1.4 Sunucu üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları, anti virüs vb. koruma amaçlı yazılımlar sürekli güncellenmelidir.

C.8.1.5 Güncellemelerde değişiklik yapılacak ise bu değişiklikler, önce değişiklik yönetimi kuralları çerçevesinde, uygulama sahipleri tarafından test mekanizmasından geçirilmeli, onaylanmalı sonra uygulanmalıdır. Test sürecinden başarılı bir şekilde geçen değişiklikler Sistem Yönetimi onayı ile uygulamaya alınır.

C.8.1.6 Sistem yöneticileri 'Administrator' ve 'root' gibi genel sistem hesapları kullanmamalıdır.

C.8.1.7 Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSL, IPsec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.

C.8.1.8 Kurumda bulunan sunucuların yönetiminden, ilgili sunucu yönetimi için yetkilendirilmiş personel sorumludur. Yetkilendirme Sistem Yönetimi tasarrufunda yapılmalıdır. Görevinden ayrılan personelin tüm erişim yetkileri anında iptal edilmelidir.

C.8.1.9 Sunucu kurulumları, konfigürasyonları, işletim sistemi yedeklemeleri, yamaları, güncellemeleri Sistem Yönetimi tarafından yapılmalıdır.

C.8.1.10 Sunuculara ait bilgilerin yer aldığı envanter veri tabanı oluşturulmalıdır. Bu veri tabanında, sunucuların isimleri, IP adresleri, yeri, ana görevi, üzerinde çalışan uygulamalar, işletim sistemi sürümleri ve yamaları, donanım, kurulum, yedek, yama yönetimi işlemlerinden sorumlu personelin isimleri ve telefon numaraları yer almalıdır. Bu tablo bir portal üzerinde bulundurulmalıdır.

C.8.1.11 Sunucuların yazılım ve donanım bakımları, üretici firma tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılmalıdır.

C.8.2. Sahip olma ve sorumluluklar ile ilgili kurallar;

C.8.2.1 Kurum'da bulunan sunucuların yönetiminden, ilgili sunucuyla yetkilendirilmiş personel sorumludur.

C.8.2.2 Sunucu kurulumları, konfigürasyonları, işletim sistemi yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personel tarafından yapılmalıdır.

C.8.2.3 Tüm bilgiler, sistem yöneticisinin belirlediği kişi(ler) tarafından güncel tutulmalıdır.

C.8.2.4 Sunucular ile ilgili, üçüncü parti firmalar ile yapılacak çalışmalarda, ilgili sunucuyla yetkilendirilmiş personel eşlik etmelidir.

C.8.3. Genel yapılandırma kuralları;

C.8.3.1 Sunucu kurulumları, yapılandırmaları, yedeklemeleri, yamaları, güncellemeleri Genel Müdürlük talimatlarına göre yapılmalıdır.

C.8.3.2 Kullanılmayan servisler ve uygulamalar kapatılmalıdır.

C.8.3.3 Servislere erişimler, kaydedilerek ve erişim kontrol yöntemleri ile koruma sağlanmalıdır.

C.8.3.4 Sunucu üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları ve anti virüs vb. koruma amaçlı yazılımlar sürekli güncellenmelidir. Anti virüs ve yama güncellemeleri otomatik olarak yazılımlar tarafından yapılmalıdır. Güncellemelerde değişiklik yapılacak ise bu değişiklikler, önce değişiklik yönetimi kuralları çerçevesinde, bir onay ve uygulama sahipleri tarafından test mekanizmasından geçirilmeli, sonra uygulanmalıdır. Bu çalışmalar için yetkilendirilmiş bir sistem biriminden, bir de uygulama biriminden personel olmalıdır.

C.8.3.5 Sistem yöneticileri 'Administrator' ve 'root' gibi genel sistem hesapları kullanmamalıdır. Sunuculardan sorumlu personelin istemciler ve sunuculara bağlanacakları kullanıcı adları ve parolaları farklı olmalıdır.

C.8.3.6 Sunuculara ait bağlantılar normal kullanıcı hatlarına takılmamalıdır. Sunucu VLAN'larının tanımlı olduğu portlardan bağlantı sağlanmalıdır.

C.8.3.7 Sunucular üzerinde lisanslı yazılımlar kurulmalıdır.

C.8.3.8 Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.

C.8.4. Sunucu gözlemlene kuraları;

C.8.4.1 Kritik sistemlerde, uygulamalar kaydedilmeli ve kayıtlar aşğıdaki gibi saklanmalıdır.

C.8.4.2 Kayıtlara çevrimiçi olarak en az 90(doksan) gün süreyle erişilmelidir.

C.8.4.3 Günlük tape backuplar en az 1(bir) ay saklanmalıdır.

C.8.4.4 Haftalık tape backuplar en az 1(bir) ay saklanmalıdır.

C.8.4.5 Aylık fiili backuplar en az 6(altı) ay saklanmalıdır.

C.8.4.6 Kayıtlar sunucu üzerinde tutulmalarının yanı sıra ayrı bir sunucuda da saklanmalıdır.

C.8.4.7 Sunucu üzerinde zararlı yazılım (malware, spyware, hack programları, warez programları, vb.) çalıştırılmamalıdır.

C.8.4.8 Kayıtlar sorumlu kişi tarafından değerlendirilmeli ve gerekli tedbirler alınmalıdır.

C.8.4.9 Port tarama atakları düzenli olarak yapılmalıdır.

C.8.4.10 Yetkisiz kişilerin ayrıcalıklı hesaplara erişip erişemeyeceğinin kontrolü periyodik yapılmalıdır.

C.8.4.11 Denetimler, Bilgi İşlem grubu tarafından yetkilendirilmiş kişilerce yönetilmeli ve belli aralıklarda yapılmalıdır.

C.8.4.12 Sunucuların bilgileri yetkilendirilmiş kişi tarafından tutulmalı ve güncellenmelidir.

C.8.5. Sunucu işletim kuralları;

C.8.5.1 Sunucular, sıcaklık ve nem değerleri düzenlenmiş; elektrik, ağ altyapısı kuvvetli; tavan ve taban güçlendirmeleri yapılmış ortamlarda bulundurulmalıdır.

C.8.5.2 Sunucuların yazılım ve donanım bakımları üretici firma tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılmalıdır.

C.8.5.3 Sistem odalarına giriş ve çıkışlar kontrol edilmelidir.

C.9. Ağ Cihazları Güvenliği**C.9.1. Ağ Cihazları Güvenlik Politikası**

C.9.1.1. Ağ cihazlarının IP ve MAC adres bilgileri envanter dosyasında yer almalıdır.

C.9.1.2. Cihazlar üzerinde yerel kullanıcı hesapları açılmamalıdır.

C.9.1.3. Yönlendirici ve anahtarlardaki tam yetkili şifre olan 'enable şifresi' kodlanmış formda saklanmalıdır. Bu şifrenin tanımlanması kurumun içerisinden yapılmalıdır.

C.9.1.4. Kurumun belirlemiş olduğu SNMP community string'leri kullanılmalıdır. Bu bilgi sadece yetkilendirilmiş kişiler tarafından bilinmelidir. Ayrıca SNMP v3 kullanılmasına dikkat edilmelidir.

C.9.1.5. İhtiyaç duyulduğu zaman erişim listeleri eklenmelidir.

C.9.1.6. Yönlendirici ve anahtarlar Ağ Yönetimi kontrolünde olmalıdır.

C.9.1.7. Yazılım ve firmware güncellemeleri önce test ortamlarında denenmeli, sonra çalışma günlerinin dışında üretim ortamına taşınmalıdır.

C.9.1.8. Cihazlar üzerinde kullanılmayan servisler kapatılmalıdır.

C.9.1.9. Cihazlara yetkili kişiler dışında cihazın başında olarak erişilmesini önlemek amacıyla Console(Konsol) portu için de “enable şifresi” gibi kodlanmış ayrı bir parola verilmelidir.

C.9.1.10. Cihazları yönetecek kurum içindeki kişiler için cihaz üzerinde “enable şifresinden” farklı olarak kullanıcı adı, parola ve yetki seviyesini belirleyen privilege numarası tanımlanmalıdır.

C.9.1.11. Cihazlar Sistem odası gibi yerlerde şifreli kabinlerde konumlandırılmalıdır. Sistem odası dışında kalan cihazlar yine uygun kabinlerde kapalı dolap ya da şifreli kabinlerde muhafaza edilmelidir.

C.9.2. Kablosuz Ağlar Güvenliği

C.9.2.1. Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmalıdır. Bunun için Wi-Fi Protected Access2 (WPA2-kurumsal) şifreleme kullanılmalıdır. IEEE 802.1x erişim kontrol protokolü ve TACACS+ ve RADIUS gibi güçlü kullanıcı kimlik doğrulama protokolleri kullanılmalıdır.

C.9.2.2. Erişim cihazlarındaki firmwareler düzenli olarak güncellenmelidir. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlamaktadır.

C.9.2.3. Cihaza erişim için güçlü bir parola kullanılmalıdır. Erişim parolaları varsayılan ayarda bırakılmamalıdır.

C.9.2.4. Varsayılan SSID isimleri kullanılmamalıdır. SSID ayar bilgisi içerisinde kurumla ilgili bilgi olmamalıdır, mesela kurum ismi, ilgili bölüm, çalışanın ismi vb.

C.9.2.5. Radyo dalgalarının binanın dışına taşmamasına özen gösterilmelidir. Bunun için çift yönlü antenler kullanılarak radyo sinyallerinin çalışma alanında yoğunlaşması sağlanmalıdır.

C.9.2.6. Kullanıcıların erişim cihazları üzerinden ağa bağlanabilmeleri için, Kurum kullanıcı adı ve parolası bilgilerini etki alanı adı ile beraber girmeleri sağlanmalı ve Kurum kullanıcısı olmayan kişilerin, kablosuz ağa yetkisiz erişimi engellenmelidir.

C.9.2.7. Erişim cihazları üzerinden gelen kullanıcılar Firewall üzerinden ağa dâhil olmalıdırlar.

C.9.2.8. Erişim cihazları üzerinden gelen kullanıcıların internete çıkış bant genişliğine sınırlama getirilmeli ve kullanıcılar tarafından kurumun tüm internet bant genişliğinin tüketilmesi engellenmelidir.

C.9.2.9. Erişim cihazları üzerinden gelen kullanıcıların ağ kaynaklarına erişim yetkileri, internet üzerinden gelen kullanıcıların yetkileri ile sınırlı olmalıdır.

C.9.2.10. Kullanıcı bilgisayarlarında kişisel anti-virüs ve güvenlik duvarı yazılımları yüklü olmalıdır.

C.9.2.11. Erişim cihazları bir yönetim yazılımı ile devamlı olarak gözlemlenmelidir.

C.9.2.12. Kablosuz erişim noktalarının aktif cihazlara giden kablolamasında fiziksel güvenliğe dikkat edilmelidir.

C.9.2.13. Kurum çalışanlarının kullandığı ile misafirler için olan SSID'ler farklı olmalıdır.

C.9.2.14. Kablosuz ağa dahil olan kurum çalışanları için bile erişimler sınırlandırılmalıdır. Sadece internete çıkacak olan kullanıcıların kablosuz ağ üzerinden diğer uygulamaların (ses, güvenlik, mobilite vb) çalıştığı networklere erişimi engellenmeli gerekirse networkler farklı IP aralıkları üzerinde ayarlanmalı, cihaz üzerinde Access Control Listler (Yetki kuralları) oluşturulmalıdır.

C.9.2.15. Kablosuz ağ cihazlarına erişim sadece yetkili kişiler tarafından SSH ile ya da cihaz başında console (konsol) ile yapılmalı, http ve telnet kapatılmalıdır. Ayrıca kablosuz cihazlara erişim için de “enable ve console (konsol) şifresi” oluşturulmalıdır.

C.10. Mal ve Hizmet Alımları Güvenliği

C.10.1. Mal ve hizmet alımlarında ilgili kanun, genelge, tebliğ ve yönetmeliklere aykırı olmayacak ve rekabete engel teşkil etmeyecek şekilde gerekli güvenlik düzenlemeleri Teknik Şartnameler de belirtilmelidir.

C.10.2. Belirlenen güvenlik gereklerinin karşılanması için aşağıdaki maddelerin anlaşmaya eklenmesi hususu dikkate alınmalıdır:

- Bilgi güvenliği politikası,
- Bilgi, yazılım ve donanımı içeren kuruluşun bilgi varlıklarının korunması prosedürleri,
- Gerekli fiziki koruma için kontrol ve mekanizmalar,

- Kötü niyetli yazılımlara karşı koruma sağlamak için kontroller,
- Varlıklarda oluşan herhangi bir değişimin tespiti için prosedürler; örneğin, bilgi, yazılım ve donanımda oluşan kayıp veya modifikasyon,
- Anlaşma sırasında, sonrasında ya da zaman içinde kabul edilen bir noktada, bilgi ve varlıkların iade veya imha edildiğinin kontrolü,
- Varlıklarla ilgili gizlilik, bütünlük, elverişlilik ve başka özellikleri,
- Bilgilerin kopyalama ve ifşa kısıtlamaları ve gizlilik anlaşmalarının kullanımı,
- Kullanıcı ve yönetici eğitimlerinin methodu, prosedürü ve güvenliği,
- Bilgi güvenliği sorumluluğu ve sorunları için kullanıcı bilinci sağlama,
- Uygun olduğu yerde personel transferi için hüküm,
- Donanım ve yazılım kurulumu ve bakımı ile ilgili sorumluluklar,
- Açık bir raporlama yapısı ve anlaşılabilir raporlama formatı,
- Değişim yönetimi sürecinin açıkça belirlenmesi,
- Erişim yapması gereken üçüncü tarafın erişiminin nedenleri, gerekleri ve faydaları,
- İzin verilen erişim yöntemleri, kullanıcı kimliği ve şifresi gibi tek ve benzersiz tanımlayıcı kullanımı ve kontrolü,
- Kullanıcı erişimi ve ayrıcalıkları için bir yetkilendirme süreci,
- Korumanın bir gerekliliği olarak mevcut hizmetleri kullanmaya yetkili kişilerin ve hakları ile ayrıcalıkları gibi kullanımları ile ilgili olan bir bilgilerin bir listesi,
- Erişim haklarının iptal edilmesi veya sistemler arası bağlantı kesilmesi için süreç,
- Sözleşme de belirtilen şartların ihlali olarak meydana gelen bilgi güvenliği ihlal olaylarının ve güvenlik ihlallerinin raporlanması, bildirimi ve incelenmesi için bir anlaşma,
- Sağlanacak ürün veya hizmetin bir açıklaması ve güvenlik sınıflandırması ile kullanılabilir hale getirilmesini tanımlayan bir bilgi,
- Hedef hizmet seviyesi ve kabul edilemez hizmet seviyesi,
- Doğrulanabilir performans kriterlerinin tanımı, kriterlerin izlenmesi ve raporlanması,
- Kuruluşun varlıkları ile ilgili herhangi bir faaliyetin izlenmesi ve geri alınması hakkı,
- Üçüncü bir taraf tarafından yürütülen denetimler için sözleşmede belirtilen denetleme sorumlulukları hakkı ve denetçilerin yasal haklarının sıralanması,
- Sorun çözümü için bir yükseltme sürecinin kurulması,
- Bir kuruluşun iş öncelikleri ile uygun elverişlilik ve güvenilirlik de dahil olmak üzere hizmet sürekliliği gerekleri,
- Anlaşmayla ilgili tarafların yükümlülükleri,
- Hukuki konularla ilgili sorumlulukları ve yasal gereklerin nasıl karşılanması gerektiğinden emin olunmalıdır, (örneğin, veri koruma mevzuatı, anlaşma diğer ülkelerle ile işbirliği içeriyorsa özellikle farklı ulusal yargı sistemleri dikkate alınarak)
- Fikri mülkiyet hakları (IPRs), telif hakkı ve herhangi bir ortak çalışmanın korunması,
- Üçüncü tarafların alt yüklenicileri ile birlikte bağlılığı ve altyüklenicilere uygulanması gereken güvenlik kontrolleri,
- Anlaşmaların yeniden müzakeresi ya da feshi için şartlar,

- Taraflardan birinin anlaşmayı planlanan tarihten önce bitirmesi durumunda bir acil durum planı olmalıdır.
- Kuruluş güvenlik gereklerinin değişmesi durumunda anlaşmaların yeniden müzakere edilmesi,
- Varlık listeleri, lisanslar, anlaşmalar ve hakların geçerli belgeleri ve onlarla ilişkisi.

C.10.3. Farklı kuruluşlar ve farklı türdeki üçüncü taraflar arasında yapılan anlaşmalar önemli ölçüde değişebilir. Bu nedenle; anlaşmalar, belirlenen tüm riskleri ve güvenlik gereklerini içerecek şekilde yapılmalıdır. Gerektiğinde güvenlik yönetim planındaki gerekli kontroller ve prosedürler genişletilebilir.

C.10.4. Bilgi güvenliği yönetimi dış kaynaklı ise anlaşmalarda üçüncü tarafın güvenlik garantisinin yeterliliğini nasıl ele alındığı anlaşmada belirtilmelidir. Risk değerlendirmede tanımlandığı gibi, risklerdeki değişiklikleri belirlemek ve başa çıkmak için güvenliğin nasıl adapte edileceği ve sürdürüleceği ele alınmalıdır.

C.10.5. Dış kaynak kullanımı ve üçüncü taraf hizmet sunumunun diğer formları arasındaki farklılıkların bazıları; sorumluluk, geçiş durumu planlama ve işlemler süresince potansiyel kesinti süresi, acil durum planlaması yönetmelikleri ve durum tespitinin gözden geçirilmesi, güvenlik olayları hakkında bilgi toplanması ve yönetimi konularında sorular içerecektir. Bu nedenle, dış kaynaklı bir yönetmelik geçişinde; kuruluş değişiklikleri yönetmek için uygun süreçlere ve anlaşmaların yeniden müzakere edilmesi ya da fesh edilmesi hakkına sahip olduğu için kuruluşun planlaması ve yönetimi önemlidir.

C.10.6. Üçüncü taraflarla yapılan anlaşmalar diğer tarafları içerebilir. Üçüncü taraflara erişim hakkı verilmeden önce, erişim hakkı ve katılım için diğer tarafların ve koşulların belirlenmesi amacıyla anlaşmaya varılması gerekir.

C.10.7. Genellikle anlaşmaların esasları kuruluşlar tarafından geliştirilmiştir. Bazı durumlarda anlaşmaların üçüncü taraflarca geliştirilmesi ve kuruluşa empoze edilmesi durumu olabilir. Kuruluşlar, kendi yapılarına üçüncü taraflarca empoze edilecek anlaşmalarda kendi güvenliklerinin gereksiz yere etkilenmesini engeller.

10.8. Gizlilik Sözleşmeleri

C.10.8.1 Gizlilik veya ifşa etmeme anlaşmaları yasal olarak uygulanabilir terimleri kullanarak gizli bilgileri korumanın gerekliliğini ele almalıdır. Gizlilik veya ifşa etmeme anlaşmaları için aşağıdaki unsurlar dikkate alınmalıdır:

- Korunacak bilginin bir tanımı (örneğin; gizli bilgileri),
- Gizliliğin süresiz muhafaza edilmesi gereken durumlar da dahil olmak üzere anlaşma süresi,
- Anlaşma sona erdiğinde yapılması gereken eylemler,
- Yetkisiz bilginin açığa çıkmasını önlemek için sorumluluklar ve imza eylemlerinin belirlenmesi ('bilmesi gereken' gibi),
- Bilginin sahibinin, ticari sırların ve fikri mülkiyet haklarının ve bu gizli bilgilerin nasıl korunması gerektiği,
- Gizli bilgilerin kullanım izni ve bilgileri kullanmak için imza hakları,
- Gizli bilgileri içeren faaliyetleri izleme ve denetleme hakkı,

- Yetkisiz açıklama ya da gizli bilgilerin ihlal edilmesinin bildirimi ve raporlama prosesi,
- İade veya imha anlaşmasına bırakılacak bilgi için terimler,
- Bu anlaşmanın ihlali durumunda yapılması beklenen eylemler.

C.10.8.2 Bir kuruluşun güvenlik gereksinimlerine dayalı olarak, diğer unsurlarla bir gizlilik veya ifşa etmeme anlaşması gereklidir.

C.10.8.3 Gizlilik ve ifşa etmeme anlaşmaları uygulandığı yerin geçerli tüm yasa ve yönetmeliklerine uygun olmalıdır.

C.10.8.4 Gizlilik ve ifşa etmeme anlaşmaları için gerekler periyodik olarak veya gerekleri etkileyecek bir değişiklik olduğunda gözden geçirilmelidir.

C.10.8.5 Gizlilik ve ifşa etmeme anlaşmaları kurumsal bilgileri korumalı ve imzalayanın, bilginin korunmasından, kullanılmasından ve ifşa edilmesinden yetkili ve sorumlu olduğunu belirtmelidir.

C.10.8.6 Farklı koşullarda gizlilik ve ifşa etmeme anlaşmaları kuruluşun ihtiyaçları doğrultusunda farklı şekillerde kullanılmalıdır.

C.11. Uygulama Yazılımları Güvenlik Yönetimi

C.11.1. Yazılım Geliştirme Politikası

C.11.1.1. Mevcut sistem yazılımları üzerine kurulacak, kullanılacak yeni bir yazılım veya mevcut sisteme yapılacak olan güncellemeler ile etkisiz hale getirilmemelidir.

C.11.1.2. Yönetim sadece uygun yazılım projelerinin başlatıldığından ve proje altyapısının uygun olduğundan emin olmalıdır.

C.11.1.3. Uygulama yazılımlarının kurum içerisinde mi hazırlanacağı yoksa satın mı alınacağını belirlenmesi, uygun bir şekilde tanımlanmalıdır.

C.11.1.4. Sistem geliştirmede, ihtiyaç analizi, fizibilite çalışması, tasarım, geliştirme, deneme ve onaylama safhalarını içeren sağlıklı bir iş planı kullanılmalıdır.

C.11.1.5. Kurum içinde geliştirilmiş yazılımlar ve seçilen paket sistemler ihtiyaçları karşılamalıdır.

C.11.1.6. Yazılım geliştirme ve temin politikalarına uygun olmayan, ulusal ve uluslararası yazılım geliştirme standartları çerçevesinde geliştirilmemiş ve kurum talebi olmaksızın üretilmiş olan yazılımların kurumsal sistemler üzerine entegre edilmesine izin verilmemelidir.

C.11.1.7. Hazırlanan sistemler mevcut prosedürler dâhilinde, işin gerekliliklerini yerine getirdiklerinden ve iç kontrol yapıldığından emin olunması açısından test edilmeli, yapılan testler ve test sonuçları belgelenecek onaylanmalıdır.

C.11.1.8. Yeni alınmış veya revize edilmiş bütün yazılımlar test edilmeli ve onaylanmalıdır.

C.11.1.9. Eski sistemlerdeki veriler tamamen, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılmalıdır.

C.11.1.10. Uygulama ortamına aktarılma kararı uygun bilgilere dayalı olarak, ilgili yönetim tarafından verilmelidir.

C.11.1.11. Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.

C.11.1.12. Yazılımlar sınıflandırılmalı/etiketlenmeli ve envanterleri çıkarılarak bir yazılım kütüğünde muhafaza edilmelidir.

C.11.1.13. İlgili yazılım denetim süreçlerine göre yazılım geliştirme süreci politikasının gözden geçirilmesini önerilmektedir.

C.11.1.14. 3. Taraflarca geliştirilen yazılımın proje yönetimi, yazılım geliştirme, test ve kabul esasları tanımlanmalıdır.

C.11.1.15. Kurumsal yazılım geliştirme esasları yayınlanmışsa ona uygun geliştirme talep edilmelidir. Fonksiyon isimlendirme, yorum kullanımı, kullanılan yazılım dili vb.

C.11.1.16. Sistem yazılımında mevcut olan kontroller, kullanılacak yeni bir yazılım veya mevcut sistem yazılımına yapılacak olan güncellemeler ile etkisiz hale getirilmemelidir.

C.11.1.17. Sistem geliştirmede, ihtiyaç analizi, fizibilite çalışması, tasarım, geliştirme, deneme ve onaylama safhalarını içeren sağlıklı bir iş planı kullanılmalıdır.

C.11.1.18. Kurum içinde geliştirilmiş yazılımlar ve seçilen paket sistemler ihtiyaçları karşılamalıdır.

C.11.1.19. Kurumda kişisel olarak geliştirilmiş yazılımların kullanılması engellenmelidir.

C.11.1.20. Hazırlanan sistemler mevcut prosedürler dâhilinde, işin gerekliliklerini yerine getirdiklerinden ve iç kontrol yapıldığından emin olunması açısından test edilmeli, yapılan testler ve test sonuçları belgelenerek onaylanmalıdır.

C.11.1.21. Yeni alınmış veya revize edilmiş bütün yazılımlar test edilmeli ve onaylanmalıdır.

C.11.1.22. Eski sistemlerdeki veriler tamamen, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılmalıdır.

C.11.1.23. Uygulama ortamına aktarılma kararı uygun bilgilere dayalı olarak, ilgili yönetim tarafından verilmelidir.

C.11.1.24. Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.

C.11.1.25. Yazılımlar sınıflandırılmalı/etiketlenmeli ve envanterleri çıkarılarak bir yazılım kütüğünde muhafaza edilmelidir.

C.11.2. Belgelendirme Politikası

C.11.2.1. Bilişim sisteminin yapısı ile bütün iş ve işlemler açıkça belgelenmeli ve bu belgeleme inceleme amacıyla kolaylıkla ulaşılabilir durumda olmalıdır.

C.11.2.2. İş akışları uygun şekilde belgelenmelidir.

C.11.2.3. Belgeleme, tarih belirtilerek yapılmalı ve yedek kopyaları güvenli bir yerde muhafaza edilmelidir.

- C.11.2.4.** Girdi türleri ve girdi form örnekleri belgelenmelidir.
- C.11.2.5.** Ana dosyalar ile diğer dosyaların içerik ve şekilleri belgelenmelidir.
- C.11.2.6.** Çıktı form örnekleri ve çıktıların kimlere dağıtılacağı belgelenmelidir.
- C.11.2.7.** Programların nasıl test edildiği ve test sonuçları belgelenmelidir.
- C.11.2.8.** Bütün program değişikliklerinin detayları belgelenmelidir.

C.12. Güvenlik Yazılım ve Donanımları Yönetimi

- C.12.1.** Bu sunuculara 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.
- C.12.2.** Kuruma ait sunucular üzerinde bulunan, tüm kullanıcı hesapları (administrator ve root hesaplarında dahil olmak üzere) güçlü şifreler ile korunmalıdır.
- C.12.3.** Yapılacak tüm işlemler düzgün bir şekilde dokümente edilmeli ve ilgili birim sorumlularına iletilmelidir.
- C.12.4.** Güvenlik yazılım ve donanımlarının erişim logları, merkezi log sisteminde tutulmalı ve izlenmelidir.
- C.12.5.** Güvenlik yazılım ve donanımlarının logları, her bir yazılım ve donanım için belirlenen disk alanlarında tutulmalı ve ilgili birim tarafından yönetilmelidir.
- C.12.6.** Güvenlik donanımları, yetkisiz kişiler tarafından erişilememesi için gerekli güvenlik tedbirleri alınmış sistem odalarında tutulmalıdır.
- C.12.7.** Güvenlik donanımlarının konfigürasyon yedekleri düzenli olarak alınmalı ve bir back-up sunucusunda tutulmalıdır.
- C.12.8.** Kurumda kullanılan güvenlik yazılım ve donanımları en güncel ve stabil yamaya (patch) sahip olmalıdır.
- C.12.9.** 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.
- C.12.10.** Kurumun tüm istemcileri ve sunucuları anti-virüs yazılımına sahip olmalıdır. Ancak sistem yöneticilerinin gerekli gördüğü sunucular üzerine istisna olarak anti-virüs yazılımı yüklenmeyebilir.
- C.12.11.** İstemcilere ve sunuculara virüs bulaştığı fark edildiğinde etki alanından çıkartılmalıdır.
- C.12.12.** Sistem yöneticileri, anti-virüs yazılımının sürekli ve düzenli çalışmasından ve istemcilerin ve sunucuların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur.
- C.12.13.** Kullanıcı hiç bir sebepten dolayı anti-virüs yazılımını bilgisayarından kaldırmamalıdır.

C.12.14. Anti-virüs güncellemeleri anti-virüs sunucusu ile yapılmalıdır. Sunucular internete sürekli bağlı olmalı, sunucuların veri tabanları otomatik olarak güncellenmelidir. Etki alanına bağlı istemcilerin, anti-virüs sunucusu tarafından anti-virüs güncellemeleri otomatik olarak yapılmalıdır.

C.12.15. 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.

C.12.16. Bilinmeyen veya şüpheli kaynaklardan dosya indirilmemelidir.

C.12.17. Kurumun ihtiyacı haricinde okuma/yazma hakkı veya disk erişim hakkı tanımlamaktan kaçınılmalıdır. İhtiyaca binaen yapılan bu tanımlamalar, ihtiyacın ortadan kalkması durumunda iptal edilmelidir.

C.12.18. Optik Media ve harici veri depolama cihazları anti-virüs kontrolünden geçirilmelidir.

C.13. Bilgi Güvenliği Teknolojileri Güvenliği

Bilgi güvenliği ile ilgili görev ve sorumluluklar belirlenmelidir.

C.13.1. Yazılım Güvenliği

C.13.1.1. Kurum içerisinde kullanılan tüm bilgisayarların zararlı yazılımlara karşı en güncel anti virüs yazılımına sahip olmalıdır.

C.13.1.2. Bilgisayarlarda kullanılan anti virüs yazılımları düzenli olarak güncellenmelidir.

C.13.1.3. Bilgisayarların üzerinde kullanılan işletim sistemleri düzenli olarak güncelleştirilmelidir.

C.13.1.4. Bilgisayarlar üzerinde korsan yazılımlar bulundurulmamalıdır.

C.13.1.5. Kurum için hazırlanacak uygulamalar güvenlik zafiyetlerini en aza indirmek için güvenli yazılım yaşam döngüsüne uygun olarak tasarlanmalıdır.

C.13.1.6. Geliştirilen yazılımlar gizlilik, bütünlük ve erişebilirlik şartlarına uygun olmalıdır.

C.13.1.7. Yazılım geliştirme sürecinde, giriş doğrulama, yetkilendirme, kimlik doğrulama, konfigürasyon yönetimi, hassas bilgi, kriptografi, parametre manipülasyonu, hata yönetimi ve kayıt tutma ve denetimi kriterleri dikkate alınmalıdır.

C.13.1.8. Yazılım geliştirme süreci boyunca, gerekli bütün testler eksiksiz şekilde yapılmalıdır.

C.13.1.9. Kurum için geliştirilen uygulamalar ve satın alınan yazılımlar, güvenlik zafiyetlerine neden olmamak için en son stabil yamalara ve güncelleştirmelere sahip olmalıdır.

C.13.1.10. Uygulamalar geliştirilme süreçlerinde gerçek ortamda uygulanmadan önce test sunucularında test edilmelidir. Uygulamalar gerçek ortamda kurumun uygun bulunduğu mesai saatleri dışında bir zaman diliminde devreye alınmalıdır.

C.13.1.11. Kurum için geliştirilen uygulamalar, uluslararası kabul görmüş standartlara bağlı dokümanite edilmelidir. Uygulama için yazılmış olan dokümanlar uygulama ile beraber kuruma teslim edilmelidir.

C.13.2. Donanım Güvenliği

C.13.2.1. Kuruma ait sistemler ve sunucular dışarıdan gelebilecek saldırılara karşı, güncel teknolojilere sahip donanımsal firewall cihazları ile korunmalıdır.

C.13.2.2. Kurum çalışanlarının internete çıkışlarının kontrol edilerek, zararlı ve kurum politikasına uymayan sitelere erişimlerinin engellenmesi için proxy cihazları ile korunmalıdır.

C.13.2.3. Kuruma ait uygulamaların güvenli bir şekilde çalışması ve uygulamalara gelebilecek saldırıların engellenmesi için Web Application Firewall (Web Uygulama Güvenlik Duvarı) ile korunmalıdır.

C.13.2.4. Kurum ile dış dünya arasında ki yazışmalar bir eposta güvenlik cihazı ile kontrol edilmelidir. SPAM, virüs, kurum politikalarına uygun olmayan içerikler engellenmelidir.

C.13.2.5. Kurumda ki güvenlik cihazları sürekliliğin sağlanması için cluster (yedekli yapıda) bulunmalıdır.

C.13.2.6. Kurumda kullanılan güvenlik cihazlarının loglarının düzenli olarak alınması ve encrypt (şifreli) olarak saklanması gerekmektedir.

C.13.2.7. Kurumda kullanılan bütün güvenlik cihazlarının konfigürasyon yedekleri periyodik olarak alınmalı, doğru şekilde etiketlenerek saklanmalıdır.

C.13.2.8. Kurumda kullanılan bütün sistem ve güvenlik donanımları, kurumun ihtiyaçlarına bağlı olarak sadece izin verilen erişimlere göre konfigüre edilmelidir.

C.14. Bulut Teknolojileri Güvenliği

Bulut bilişim popülerliğini artırdıkça, bu yeni modelle ortaya çıkan güvenlik sorunları endişeleri artırmıştır. Geleneksel koruma mekanizmalarının etkinliği ve verimliliği yeniden değerlendirilmektedir, bu yeni yerleştirme modelinin özellikleri büyük ölçüde geleneksel mimarilerden farklılık arz etmektedir.

Özel bulut ekipmanlarının fiziksel kontrolünün yapılabilirliği ekipmanların tesis dışında ve başkalarının kontrolünde olmasından daha güvenlidir. Veri bağlantılarının güvenliği için fiziksel kontrol ve veri bağlantılarını görsel olarak incelemek ve portlara erişebilmek gereklidir. Bulut bilişimin benimsenmesi yolundaki engellerin sebebi çoğunlukla kamu ve özel sektörünün güvenlik tabanlı hizmetlerinin harici yönetiminin korku ve endişeye sebep olmasıdır. Bulut bilişim tabanlı hizmetlerin dışarıdan sağlanması ise en temel özelliğidir. Bu durum bulut bilişim hizmet sağlayıcılarına güvenli hizmetlerin yönetimini kurma ve sürdürmeye öncelik verilmesi hususunda iticidir.

C.14.1. Fiziksel Güvenlik Sunuculara erişimlerinin fiziksel olarak güvenliğinin en az TIER-3 seviyesinde sağlanmalıdır.

C.14.2. Network Güvenliği Network ekibi tarafından sağlanacak güvenlik tedbirleri refere edilmelidir.

C.14.3. Data Güvenliği;

Kriptografi: Veriyi korumanın yollarından biri de şifrelemedir. Bugün şifreleme çalışmaları oldukça ilerlemiş, bilgisayarlar oldukça gelişmiştir. Fakat bu durum saldırganlar için de geçerlidir. Hassas bilgiler bilinen ve test edilmiş şifreleme yöntemleri ile saklanmalıdır. Ayrıca daha önce kırılması uzun zaman alan algoritmalar günümüzde daha kısa zamanda çözülebilmektedir. Dolayısıyla uygulama içindeki algoritmalar zamanla gözden geçirilmeli ve güncellenmelidir.

C.14.4. Kimlik Erişim Yönetimi; yetkisiz erişimlerin tespiti ve ağ sistemlerinin korunması için gerekli kontrol faaliyetleri sağlanmalıdır.

C.14.5. Uygulama Güvenliği;

C.14.5.1 Konfigürasyon Yönetimi; Konfigürasyon, uygulama ile ilgili hassas bilgileri içermektedir. Örnek vermek gerekirse veri tabanına erişim için gerekli bağlantı bilgilerini içeren dosyalar bu kapsamdadır. Konfigürasyona müdahale uygulamanın işleyişini değiştirebilir veya çalışmamasına sebep olabilir. Konfigürasyon dosyalarının sunucularda saklanması yeterli güvenlik önlemlerinin alındığı anlamına gelmemektedir. Konfigürasyon dosyaları hassas bilgi olarak nitelendirilmeli, şifrelenmiş bir şekilde tutulmalı ve bu dosyalara erişim kayıt altında tutulmalıdır.

C.14.5.2 Hassas Bilgi (Sensitive Information); Hassas bilginin ne olduğunun belirlenebilmesi için uygulamanın ve işin bir arada ele alınması gereklidir. Uygulama geliştirici işin niteliğini tam olarak bilemediğinden, diğer yandan işin sahibi de uygulamanın teknik altyapısı hakkında sınırlı bilgiye sahip olacağından bu iki taraf tek başlarına hassas bilgi için yeterli tanımlama yapamayacaklardır. İki tarafın bir araya gelmesiyle hassas bilgileri içeren bir liste oluşturulmalı ve bu listeyi koruyacak bir politika oluşturulmalıdır.

C.14.5.3 Kayıt Tutma ve Denetim; Uygulama veya uygulamanın yöneticileri saldırı altında olduklarını anlamalıdır. Bu durum aslında neyin normal neyin anormal olduğunun belirlenmesi ile sağlanır. Bir uygulamaya ilişkin normal süreç ve şablon tanımlanmalı ve bunu dışında bir olay olduğunda saldırı ihtimali ele alınmalıdır. Örneğin, normal senaryoda bir uygulamaya dakikada ortalama beş kişinin erişmesi beklenirken bu sayı bine ulaşıyorsa muhtemelen bir "Servis Dışı" bırakma atağı söz konusudur.

C.15. Mobil Cihazlar Güvenliği

Bilgiyi taşımanın kolay bir yolu laptop ve akıllı telefonlar gibi mobil cihazlardır. Bu cihazlarda bulunan hassas bilgiler ve erişim yetkileri de düşünüldüğünde mobil cihazlarda güvenliğin dikkat edilmesi gereken bir konu olduğu anlaşılmaktadır.

C.15.1. Mobil cihazlara erişimde mutlaka parola kullanılmalıdır.

C.15.2. Mobil cihazınızda ne tür bilgiler sakladığınızı farkında olun, hassas ve gizli bilgileri mümkün olduğunca mobil cihazınızda bulundurmayınız.

C.15.3. Verilerinizin yedeklerini alın ve güncel bir kopyasını farklı bir yerde saklayınız.

C.15.4. Kaybolması ve çalınması kolay olduğundan mobil cihazlar başıboş bırakılmamalıdır.

C.16. İletişim ve İşletim Güvenliği

C.16.1. Bilgi sistemlerinin iletişim ve işletim görev ve sorumlulukları kuruluşun varlıklarının yetkisiz veya kasıtsız olarak değiştirilmesi ve yanlış kullanılmasını engellemek amacıyla ayrılmalıdır. Hiçbir personel denetimsiz veya yetkisiz olarak sistemlere erişemez ve sistemleri değiştiremez.

C.16.2. Bilgi İşleme ve İşletim yönetimi aşağıda belirtilen konuları kapsar;

- Bilgi işleme ve bulundurma gereksinimlerinin belirlenmesi,
- Bilginin yedeklenmesi,
- En erken işe başlama ve en geç işi tamamlama zamanlarının belirlenmesi,
- Sistem kullanım kısıtları hata mesajlarını yöneten talimatların oluşturulması,
- Beklenmeyen işletim ve teknik sorunlar karşısında destek irtibatları belirlenmesi,
- Güvenli çıktı alma talimatlarının hazırlanması,
- Sistem hatası durumunda yeniden başlatma ve kurtarma süreçlerinin belirlenmesi,
- Sistem izleme kayıtlarının yönetiminin planlanması ve uygulanması.

C.16.3. Uygulama geliştirme, test ve operasyonel sistemlerinin ayrılması;

C.16.3.1 Yazılımın geliştirme sistemlerinden uygulama sistemlerine aktarımı kuralları belirlenmeli ve dokümente edilmelidir.

C.16.3.2 Geliştirme ve uygulama yazılımları ayrı işlemcilerde, ayrı sistemlerde, ayrı etki alanlarında veya kütüphanelerde çalıştırılmalıdır.

C.16.3.3 İhtiyaç olmadığı durumlarda operasyonel sistemlerde derleyici, editör, ve diğer geliştirme araçları bulundurulmaz.

C.16.3.4 Test sistemi operasyonel sistemle mümkün olduğunca aynı sistem olmamalıdır.

C.16.3.5 Kullanıcılar test ve uygulama sistemlerinde farklı kullanıcı tanımları kullanılmalıdır.

C.16.4. Üçüncü taraflardan hizmet alımı esnasında gereken aktarımlar (bilgi, bilgi işleme imkânları ve taşınan diğer unsurlar) planlanmalı ve güvenlik daima göz önünde bulundurulmalıdır. Üçüncü taraf hizmetlerinin izlenmesi ve gözden geçirilmesi kapsamında;

C.16.4.1 Hizmet performans seviyesinin anlaşmaya uyumlu olduğu izlenmelidir.

C.16.4.2 Üçüncü tarafça hazırlanan hizmet raporları gözden geçirilmeli, anlaşmada belirtildiği şekilde geliştirme toplantıları yapılmalıdır.

C.16.4.3 Alınan hizmete ilişkin üçüncü taraf tarafından tutulan güvenlik olayları kayıtları, operasyonel sorunlar, hatalar, hizmet kesintileri gözden geçirilmelidir.

C.16.4.4 Varsa tespit edilen sorunlar yönetilmeli ve çözülmelidir.

C.16.5. Üçüncü taraf hizmetlerinde yapılan değişikliklerde;

- Ağdaki değişimler,
- Yeni teknolojilerin kullanımı,
- Yeni ürünlerin daha yeni sürüm ve baskılara uyumu,
- Yeni geliştirme araç ve ortamları,
- Hizmetlerin verildiği fiziksel yerin değişimi göz önüne alınmalıdır.

C.16.6. Üçüncü taraflardan hizmet alımlarında değişiklik olması durumunda; kuruluş tarafından yapılan değişikliklerde;

- Sunulan hizmetteki gelişmeler,
- Yeni uygulama ve sistemlerin geliştirilmesi,
- Kurumun politikalarındaki değişiklik ve güncellemeler,
- Güvenliği geliştirmek ve bilgi güvenliği olaylarını çözmek için geliştirilen yeni kontroller göz önüne alınmalıdır.

C.16.7. Bilgi işlem teçhizatının kapasite yönetimine ilişkin olarak anahtar konumundaki sistem kaynaklarının kullanım durumu sistem yöneticileri tarafından sürekli izlenir, her yeni veya devam eden faaliyetin kapasite gereksinimi belirlenir. Sistemden en uygun şartlarda verim almak için sistem ayarları sürekli kontrol edilir. Gelecekteki sistem ihtiyaçları, ileriye yönelik planlanan yeni iş uygulamaları ve mevcut kapasite göz önüne alınarak değerlendirilir.

C.16.8. Ağ güvenliği;

C.16.8.1 Mümkün olduğu takdirde ağdan sorumlu personel bilgisayar işletiminden sorumlu personelden ayrı görevlendirilmelidir.

C.16.8.2 Uzak cihazların yönetimiyle ilgili sorumluluklar belirlenmelidir.

C.16.8.3 Halka açık ağ veya kablosuz ağlardan iletilen verinin bütünlüğünü sağlayacak tedbirler alınmalıdır.

C.16.8.4 Güvenlikle ilgili olayların kaydedilmesini sağlayıcı uygun izleme yöntemleri kullanılmalıdır.

C.16.8.5 Hizmet kalitesini artırmak ve bilgi işleme altyapısının sürekli kontrolünü sağlamak için yönetim faaliyetleri yakından koordine edilmelidir.

C.16.8.6 Ağ hizmetlerinin güvenli bir şekilde verildiği düzenli olarak izlenmelidir.

C.16.8.7 Ağ güvenliği için yetkilendirme, kriptolama, bağlantı kontrolü vb. güvenlik tedbirleri uygulanmalıdır.

C.16.8.8 Gerekli görüldüğünde ağ kullanımına sınırlar getirilmelidir.

C.16.8.9 Özellikle sağlık bilgisinin iletildiği ağların kesintiye uğraması durumundaki riskler ayrıca değerlendirilmelidir.

C.16.9. Taşınabilir ortamların yönetimi;

C.16.9.1 İhtiyaç kalmadığında tekrar kullanılabilir ortamların içeriği tekrar düzeltilemeyecek hale getirilmelidir.

C.16.9.2 Gerek görüldüğünde kurumdan taşınan ortam için yetkilendirme yapılır ve kayıt altına alınmalıdır.

C.16.9.3 Tüm ortamlar üretici talimatında belirtildiği şekilde emniyetli ve güvenli ortamda saklanmalıdır.

C.16.9.4 Ortamın saklama kapasitesinden daha uzun bir süre saklanmasına ihtiyaç duyulan bilgi, aynı zamanda farklı bir ortam üzerinde de saklanmalıdır.

C.16.9.5 Veri kayıplarını engellemek amacıyla taşınabilir ortamları kayıt altına alınmalıdır.

C.16.9.6 Çıkarılabilir ortam sürücüleri sadece iş ihtiyaçları için kullanılabilir hale getirilmelidir.

C.16.9.7 Taşınan medya üzerinde kişisel sağlık bilgisi yer alıyorsa mutlaka kriptolanmalıdır.

C.16.10. Ortamın imha edilmesi;

C.16.10.1 Hassas bilgi içeren ortamlar yakılarak, silinerek, parçalanarak güvenli ve emniyetli bir şekilde yok edilmelidir.

C.16.10.2 Üzerindeki hassas bilgiyi ayırmaktan çok ortamları toplu olarak güvenli bir şekilde imha etmek daha kolay olabilmekte olup, bu durum imha aşamasında göz önüne alınmalıdır.

C.16.10.3 Birçok kurum atık toplama ve imha etme hizmeti vermekte olup, böyle bir kurumun seçimi durumunda güvenlik açısından uygun kontroller geliştirilmelidir.

C.16.10.4 Mümkün olduğu takdirde imha işlemi kayıt altına alınmalıdır.

C.16.11. Bilgi işleme süreci aşağıda belirtilen hususları kapsar;

C.16.11.1 Bilgi belirlenen sınıflandırma seviyesine işlenmeli ve etiketlenmelidir.

C.16.11.2 Yetkisiz personelin erişimini önlemek için erişim kısıtlamaları konulmalıdır.

C.16.11.3 Veriyi alan yetkililer kayıt altına alınmalıdır.

C.16.11.4 Girdi verisinin tamlığı, işlemenin uygun şekilde tamamlandığı ve çıktı doğrulamasının yapıldığı garanti edilmelidir.

C.16.11.5 Çıktı için havuzda bekleyen verinin hassasiyetine göre korunması sağlanmalıdır.

C.16.11.6 Üreticinin belirlediği özelliklere göre ortamların saklanması sağlanmalıdır.

C.16.11.7 Kopyalanan ortamların yetkili alıcının dikkatini çekmek için açık bir şekilde işaretlenmesi sağlanmalıdır.

C.16.11.8 Yetkili alıcı listeleri ile dağıtım listelerinin belirli aralıklarla gözden geçirilmesi sağlanmalıdır.

C.16.11.9 Özellikle sağlık bilgisi fiziksel olarak çok iyi korunmalı ya da şifrelenmelidir.

C.16.12. Sistem dokümantasyonunun güvenliği;

C.16.12.1 Sistem dokümantasyonu güvenli bir ortamda saklanmalıdır.

C.16.12.2 Sistem dokümantasyonuna erişim uygulama sahibi tarafından yetkilendirilmeli ve minimum seviyede tutulmalıdır.

C.16.12.3 Halka açık ağlarda tutulan veya bu ağlar üzerinden gönderilen sistem dokümantasyonu uygun bir biçimde korunmalıdır.

C.16.13. Bilgi değişim esasları;

C.16.13.1 Bilgi değişiminin kopyalanması, değiştirilmesi, yanlış yönlendirilmesi ve imhasından korunması sağlayıcı tedbirler alınmalıdır.

C.16.13.2 Elektronik iletişim kullanılarak iletilen bilginin zararlı kodlara karşı korunması için tedbir alınmalıdır.

C.16.13.3 İletilen elektronik bilginin eklentilerinin korunmasına yönelik tedbir alınmalıdır.

C.16.13.4 Elektronik iletişimin uygun kullanımına ilişkin politika ve prensipler geliştirilmeli ve yayınlanmalıdır.

C.16.13.5 Riskleri göz önüne alarak kablosuz iletişim kullanımı ile ilgili kurallar belirlenmelidir.

C.16.13.6 Çalışanlar, sözleşme tarafları ve diğer kullanıcıların kurumu karalayıcı, sıkıntıya sokucu, ardı ardına zincir posta, haksız kazanç sağlama gibi faaliyetlere katılmama sorumlulukları ortaya konulmalıdır.

C.16.13.7 Bilginin gizliliği, bütünlüğü ve güvenilirliğini korumak için kriptografik tekniklerin kullanımı değerlendirilmelidir.

C.16.13.8 Ulusal ve uluslararası mevzuat dâhilinde tüm mesajları kapsayan iş yazışmalarının saklanması ve imhası ile ilgili kurallar belirlenmelidir.

C.16.13.9 Kritik ve hassas bilgi, yazıcılar, kopyalayıcı cihazlar, faks makineleri vb. cihazlar üzerinde bırakılarak yetkisiz kişilerin erişmelerine imkân verilmemelidir.

C.16.13.10 Elektronik imkânlar kullanılarak mesajların dış adreslere otomatik iletilmesine kısıtlar getirilmeli ve kontrol edilmelidir.

C.16.13.11 Telefonla görüşürken hassas bilginin ifşa edilmemesi, bilginin dinlenmemesi için tedbir alınmasına dikkat edilmelidir.

C.16.13.12 Yetkisiz personel tarafından tekrar dinlenebileceğinden, yanlışlıkla numara çevrilebileceğinden hassas bilgi otomatik cevap kayıtlarına, iletişim sistemlerine konulmamalıdır.

C.16.13.13 Personel faks makinelerinin dikkatsiz kullanımının bilgi güvenliği açısından verebileceği zararlar konusunda bilinçli olmalıdır.

C.16.13.14 Personel, yetkisiz bilgi toplamayı engellemek için demografik veri, e-posta adresleri, kişisel bilgi vb. kayıt edilmemesi konusunda bilinçli olmalıdır.

C.16.13.15 Personel faks ve fotokopi makinelerinin arıza yapması halinde hafızalarında bilgi kaldığı, onarılmayı müteakip bu bilginin basıldığı veya iletildiği konusunda bilinçli olunmalıdır.

C.16.14. Dış taraflarla yapılacak bilgi değişim anlaşmalarında aşağıda belirtilen hususlar göz önüne alınır;

C.16.14.1 Bilgi gönderme ve alımının kontrolü için sorumluluklar belirlenmelidir.

C.16.14.2 Gönderenin, gönderim ve alımla ilgili bilgilendirilmesi sağlanmalıdır.

C.16.14.3 İnkâr edilemezlik ve izlenebilirlik garanti edilmelidir.

C.16.14.4 Paketleme ve transfer için asgari teknik standartlar belirlenmelidir.

C.16.14.5 Emanet anlaşmaları yapılmalıdır.

C.16.14.6 Kurye belirleme standartları belirlenmelidir.

C.16.14.7 Bilginin kaybolması gibi bilgi güvenliği olaylarındaki sorumluluklar tayin edilmelidir.

C.16.14.8 Bilginin uygun şekilde korunduğunu garanti etmek maksadıyla karşılıklı mutabık kalınmış bir etiketleme sisteminin hassas ve kritik bilgi üzerinde kullanılması sağlanmalıdır.

C.16.14.9 Veri koruma, telif hakları ve lisans uyumlulukları için sorumlulukların sahibi belirlenmelidir.

C.16.14.10 Kriptografik anahtarlar gibi hassas bilginin korunmasında ihtiyaç duyulacak özel kontroller belirlenmelidir.

C.16.15. Fiziksel ortamların taşınması;

C.16.15.1 Güvenilir taşıma şekli ve kuryeler kullanılmalıdır.

C.16.15.2 Yönetim tarafından yetkili bir kurye listesi belirlenmelidir.

C.16.15.3 Kuryelerin kimliğini kontrol eden süreçler geliştirilmelidir.

C.16.15.4 Paketleme, içeriğin fiziksel hasarlardan yeterince korunmasını sağlayacak şekilde yapılmalıdır.

C.16.15.5 Hassas bilgi, kilitli kapların kullanılması, elden teslim, kurcalanmaya karşı korunmalı, gerekirse farklı yollardan parçalı olarak gönderim yöntemleri kullanılarak açığa vurulması veya değiştirilmesi önlenmelidir.

C.16.16. Elektronik mesajlaşma;

C.16.16.1 Mesajların yetkisiz erişim, değiştirilme veya hizmet engelleme saldırısından koruma, mesajın doğru adreslemesi ve iletiminin sağlanması, servisin genel güvenilirliği ve kullanılabilirliği, elektronik imza vb. hukuki sebepler, anlık mesajlaşma veya dosya paylaşımı gibi halka açık dış servisleri kullanmadan önce onay elde etme, halka açık ağ erişimlerinde daha güçlü kimlik denetimi yapma konuları göz önüne alınır.

C.16.16.2 Uzmanlar arasında e-posta ile iletilen sağlık bilgisi mutlaka şifrelenmelidir.

C.16.16.3 VPN kullanıcılarına verilen şifreler e-posta yoluyla değil sms aracılığıyla gönderilmelidir.

C.16.17. Çevrimiçi işlemlerle ilgili güvenlik açısından aşağıdaki hususlar dikkate alınır;

- İşlem içerisinde yer alan her iki tarafın elektronik imzalarının kullanımı,
- Her iki tarafın kullanıcı yetkilendirmelerinin doğru olduğu ve doğrulandığı, işlemlerin güvenli olduğu, her iki tarafın gizliliğinin sağlandığı,
- Tüm tarafların iletişiminin şifrelenmesi,
- Tüm tarafların iletişim protokollerinin güvenli olması,
- İş detaylarının saklandığı yerin herkes tarafından erişilemeyen bir yerde bulunması,
- Uçtan uca elektronik imzanın kullanıldığı güvenli bir yetkilendirme,
- Sağlık bilgi sistemlerinde herkese açık bilginin değiştirilmeden arşivlenmesi.

C.16.18. Erişim kontrolüne ilişkin olarak sistem kayıtları asgari aşağıdaki hususları kapsar;

- Kullanıcı tanımları,
- Sisteme giriş-çıkış tarihi, zamanı gibi ana faaliyetler,
- Terminal kimliği ve mümkünse yeri,
- Başarılı ve ret edilen sisteme erişim girişimleri,
- Başarılı ve ret edilen veri ve diğer kaynaklara erişim girişimleri,
- Sistem konfigürasyonundaki değişiklikler,
- Ayrıcalıkların kullanımı,
- Sistem olanakları ve uygulamalarının kullanımı,
- Erişilen dosyalar ve erişim türü,
- Ağ adresleri ve protokoller,
- Erişim kontrol sisteminin verdiği uyarılar,
- Anti virüs ve saldırı önleme sistemleri gibi koruma sistemlerin başlatılması ve sonlandırılması.
- Sağlık bilgilerinde yapılan güncellemelerde kayıtların önceki durumları ayrıca log'lanır ve arşivlenir.

C.17. Kullanıcı Hesabı Açma, Kapatma Yönetimi

C.17.1. Kullanıcı hesabı tanımlanması için 2 yöntem uygulanır.

C.17.1.1 Bağlı bulunulan kurumdan resmi yazı yazılması şeklinde yapılmalıdır.

C.17.1.2 Bağlı bulunulan kurum yetkilisi tarafından @saglik.gov.tr uzantılı bir resmi e-posta adresi ile talep ettikleri yeni kullanıcılar için hazırlanan formu doldurarak eposta@saglik.gov.tr resmi e-posta adresine taleplerini göndermeleri şeklinde yapılmalıdır. Kullanıcı talebine göre yetki verilmesi durumunda ayrıca taahhütname istenilebilir.

C.17.2. Yeni kullanıcı oluşturulması taleplerinde, kişinin Başbakanlık DTVT sistemine uygun olarak konumlandırılacağı Kurum birimi, ekleneceği yetki grupları, görev tipine göre istenir. 657, 4A, 4B dışındaki personel için çalışma süre aralığının belirtilmesi gereklidir.

C.17.3. Kullanıcı hesabının dondurulması, kapatılması kullanıcının bağlı olduğu personel işleri veya bilgi işlem tarafından **C.17.1.1** ve **C.17.1.2** maddelerindeki erişim kanalları ile bildirilmelidir.

C.17.4. Kullanıcı hesabı kapatma talebi gelmesine istinaden dondurulur ve dondurulmuş hesaplar klasöründe bir sene süresince yasal takip ihtiyaçlarına binaen saklanır ve bir sene sonunda silinmelidir.

C.18. Erişim Yönetimi ve Erişim Kaydı Tutulması

Veri tabanlarına erişen kullanıcıların yapmış oldukları işlemler loglanmalı, gerektiğinde erişim yetkilisinin kayıt silme logları da listelenebilir olmalıdır.

C.18.1. Erişim Yönetimi

C.18.1.1. Kurumun erişim sağlanacak sunucularına admin/root yetkili yönetici kullanıcılar, sudo ve runas yetkili kısıtlı yönetici kullanıcılar ve dış dünyadan erişen, uygulamayı kullanan kullanıcılardan oluşmaktadır.

C.18.1.2. Bakanlık sunucularına erişim için IP/SEC ya da SSL VPN kullanılmalıdır. Mümkünse kullanıcıların erişimi için SSL ve VPN tercih edilmelidir. Güvenlik Birimi tarafından sağlanmalıdır.

C.18.1.3. Sunuculara kullanıcı erişimi için SSH, RDP gibi protokollerle sunucu yönetimi için belirli portlar erişim verilmelidir.

C.18.1.4. Sunucuların kendi aralarında servis ve yönetimleri için belirli portlarla erişim sağlanması gerekmektedir.

C.18.1.5. Kullanıcıların sunucu yönetim için sağlanan erişimde admin/root yetkisi sistem grubu dışında verilmemelidir. Parola yönetimi bakanlık bilgi güvenliği kılavuzundaki parola yönetim politikaları ile yürütülmelidir.

C.18.1.6. Kullanıcıların sunucu yönetim için sağlanan erişimde merkezi kullanıcı yönetimi (MS AD, LDAP, ssh-key) ile yapılmalıdır.

C.18.1.7. Kullanıcıların sunucu yönetim için sağlanan erişimde sudo, runas gibi erişim kısıtlı erişim yetkileri tanımlanmalıdır.

C.18.1.8. Dış dünyadan sunucular üzerindeki servislere erişim için 80, 443, 7001, 8080, 8443 gibi servis portları da özel durumlarda verilmelidir. Güvenlik Birimi tarafından bu işlem sağlanmalıdır.

C.18.1.9. Sunucu servislerinin yönetim işlemlerinde yetkili kullanıcı bilgileri, sistem gurubuna teslim edilmelidir. Sistem birimi nezaretinde ve tarafından yürütülmelidir.

C.18.1.10. Sunucu servislerinin yönetim işlemleri merkezi kullanıcı yönetimi ve kısıtlı erişim yetkileriyle kullanıcılara sağlanmalıdır.

C.18.1.11. Kurumun yedekleme sistemlerine sadece memur ya da danışman yetkili kişi erişim yapmaktadır. Firmaların yapacakları tüm işlemler sistem birimi nezaretinde yürütülmelidir.

C.18.2. Kayıt Tutulması (Log tutulması)

C.18.2.1. Kurumun güvenlik cihazlarına ait loglar güvenlik birimi tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde sistem birimiyle işbirliği içinde raporlar paylaşılmalıdır.

C.18.2.2. Kurumun veri tabanlarına ait loglar veri tabanları birimi tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde sistem birimiyle işbirliği içinde raporlar paylaşılmalıdır.

C.18.2.3. Kurumun network cihazlarına ait loglar network birimi tarafından yönetilmeli ve değerlendirilmelidir. İstendiğinde sistem birimiyle işbirliği içinde raporlar paylaşılmalıdır.

C.18.2.4. Tüm sunuculara ve servislere sağlanan tüm yönetici erişimleri uzak ve merkezi bir kayıt sunucusuna gönderilmelidir.

C.18.2.5. Merkezi kayıt sunucusu üzerinde yapılan analizler sonucunda başarısız erişimler raporlanmalıdır.

C.18.2.6. Merkezi kayıt sunucusu üzerinde alınan başarısız erişim istekleri uyarı olarak yetkili Birimlere gönderilmelidir.

C.18.2.7. Merkezi kayıt sunucusu üzerindeki başarılı girişler de istatistiksel veriler halinde raporlanabilmelidir.

C.18.2.8. Merkezi kayıt sunucusu üzerindeki kayıt verileri belirli tarih aralığında tutulmalı ve istenildiğinde raporlanabilir olmalıdır.

C.18.2.9. Merkezi kayıt sunucusu kayıtlar üzerinde yaptığı analizler doğrultusunda saldırı ve normal olmayan durumları tespit edip, uyarı gönderebilmelidir.

C.19. Uzaktan Erişim Yönetimi

C.19.1. Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahip olmalıdır.

C.19.2. İnternet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar VPN teknolojisini kullanmalıdırlar. Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlamalıdır. VPN teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vs. protokollerinden birini içermelidir.

C.19.3. Uzaktan erişim güvenliği sıkı şekilde denetlenmelidir. Kontrol tek yönlü şifreleme (one-time password authentication, örnek; Token Device) veya güçlü bir passphrase (uzun şifre) destekli public/private key sistemi kullanılması tavsiye edilmelidir. Daha fazlası için parola politikasına bakınız.

C.19.4. Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.

C.19.5. Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.

C.19.6. Mobile VPN ile uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile yapılmalıdır.

C.19.7. Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve anti virüs yazılımı güncellemeleri yapılmış olmalıdır.

C.19.8. Kurumdan ilişkisi kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.

C.19.9. Uzak erişimde yapılan tüm network hareketleri loglanmalıdır.

C.19.10. Uzak erişim için kullanılacak olan servisler ve protokoller ön tanımlı olmalıdır.

C.19.11. Uzak erişim verilecek olan kullanıcılara sözleşmesine göre günlük saatlik izinler verilmelidir. Sınırsız izin verilmekten kaçınılmalıdır.

C.19.12. VPN ile erişecek olan kullanıcı VPN Erişim formunu doldurmak zorundadır.

C.19.13. Uzak erişim bağlantısında boşa kalma süresi (Herhangi bir işlem yapılmadığı takdirde connection time out süresi) kurumun ihtiyacına göre limitlenmelidir.

C.20. Acil Erişim Yetkilendirme Yönetimi

C.20.1. Acil erişim yetkilendirme gerektiren durumlarda uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahip olmalıdır.

C.20.2. Kurum bünyesindeki bütün dahili sunucuların, ağ güvenliği ve şebeke cihazları ile veri tabanı yönetiminden yetkilendirilmiş sistem yöneticileri sorumludur.

C.20.3. Kurum bünyesindeki yazılım ve veri güvenliğini sağlarken yetkilendirilmiş sistem yöneticisi Güvenliği sağlamaktan sorumlu Ağ ve Sistem Güvenliği birimi ile birlikte uyumlu çalışarak sağlamak zorundadır.

C.20.4. Sunuculara ve cihazlara acil erişim yetkilendirilmesi gereken durumlarda; kurum içi kullanıcı, yetkilendirilmiş sistem yöneticisine başvurarak sistem üzerinde yetki istemelidir.

C.20.5. Veri tabanına acil erişim yetkilendirilmesi gereken durumda; kurum içi kullanıcı için erişim yetkilendirmesinde veri tabanı güvenlik politikası maddelerine bakılır.

C.20.6. Acil erişim yetkisi gereken durumlarda kurum dışı kullanıcılar için resmi taahhütname gelmeden uzak erişim yetkisi verme isteği acil erişim gereken birim yetkilisi tarafından verilmelidir.

C.20.7. Başka birimlerden alınması gereken erişim yetkisinin sorumluluğu, isteği yapan birimin yetkilendirilmiş yöneticisinin sorumluluğundadır.

C.20.8. Sistem üzerinde verilecek erişim yetkisi ve bunun doğuracağı sorumluluk sunucu/cihaz üzerinde yetki veren yetkilendirilmiş sistem yöneticisindir.

C.20.9. Kritik sistemlerde veri güvenliğini sağlamak için sistem yöneticisi gerekli güvenlik tedbirlerini almalıdır. Güvenliği sağlamak için gereken durumlarda başka birimler ile birlikte çalışmalıdır.

C.20.10. Veri tabanlarında bulunan bir veriye acil olarak erişilmesi gerektiğinde, verinin bulunduğu tablonun sahibinden eposta ortamında izin alındıktan sonra erişim izni veri tabanı birimi tarafından verilmelidir.

C.21. Veri Merkezi Standartları ve Yönetimi

C.21.1. Kurumun veri merkezinde yedek enerji ve soğutma sistemleri olmalıdır.

C.21.2. Kurumun veri merkezi (Sistem odaları) yangın söndürme sistemlerine sahip olmalıdır. Yangın söndürme çözümleri veri merkezinde bulunan elektronik cihazlara ve personel sağlığına zarar vermeyecek şekilde olmalıdır. Bu yüzden bu özelliğe sahip gazlar kullanılmaktadır. Yangın söndürmede FM200, FE25, Argon ve Novec 1230 gazları kullanılmalıdır.

C.21.3. Kurumun veri merkezi olarak kullanılacak odalarda dışarıya açılan pencere veya kapı (balkon kapısı) bulunmamalıdır. Girişler için sadece tek kapı bulunmalıdır ve bu kapıda da gerekli güvenlik tedbirleri (biometric giriş, card-reader, şifre paneli) alınmış olmalıdır. Veri Merkezine yetkisiz personelin girişi engellenmelidir.

C.21.4. Veri Merkezi 7/24 güvenlik kameraları ile gözetlenmeli ve kayıt altına alınmalıdır. Oluşabilecek istenmeyen bir durumda 7/24 izleme yapan personeller öneme göre sorumlu personelle irtibata geçmeli ya da kendisi veri merkezine müdahale edebilecek yakınlıkta olmalıdır. Veri Merkezinde bulunan iklimlendirme sistemlerinden sızan su sızıntıları, sıcaklık, yangın, voltaj değişimleri ve içeride bulunan havanın neminin izlenmesi amacıyla anlık bilgilendirme yapabilen sistemler ile takip edilmelidir. Bu bilgilendirmeler mail ve ya sms yoluyla sorumlu kişiye iletilebilmelidir.

C.21.5. Veri Merkezi için 7/24 güvenlik personeli bulunmalı ve tesisin fiziksel güvenliğini sağlamalıdır.

C.21.6. Veri Merkezine yapılacak tüm giriş ve çıkışlar kayıt altına alınmalıdır. İlgili personel tarafından, giriş yapan kişilerin bilgileri ayrıca log'lanmalıdır. (imzalı kayıt defteri gibi).

C.21.7. Veri merkezinde çalışacak personeller Veri Merkezi yönetimi konusunda yetkin olmalı ve gerekli durumlarda ilgili personele teknik ve farkındalık eğitimleri verilmelidir.

C.21.8. Veri merkezinde bulunan bütün güvenlik, acil durum ve iklim sistemlerinin periyodik bakımları yapılmalı ve bu bakımlar dokümanite edilmelidir.

C.21.9. Veri merkezi içerisinde, sunucu yönetimi uzak masaüstü veya SSH gibi protokoller kullanılarak yapılmalıdır.

C.21.10. Veri merkezi içerisinde, acil durumlarda ya da felaket anında ki görev ve sorumluluklar belirlenerek dokümanite edilmelidir.

C.21.11. Veri Merkezi Zemin Döşemesi kablo kanallarına ve soğuk hava akışına imkân verecek şekilde uygun bir yükseklikte (asgari 50 cm) yapılmalıdır.

Kullanılacak döşeme malzemeleri kabinlerdeki tam dolu olma durumu göz önünde tutularak 1000 kg kadar basınca dayanabilecek sağlamlıkta seçilmelidir. Günümüz kabinlerinin 1500 kg kadar yük taşıma kapasitelerine sahip olabildikleri göz önünde bulundurulmalıdır. Zemin altında karoları tutan destek ayakları mümkün olduğunca kabin ayaklarının basacağı noktaların altına veya yakınına konarak kabin yüklerinin taşınması kolaylaştırılmalıdır. Kabinlerin sallanması gibi ihtimallere karşı bu ayaklar yerlerinden kolayca oynamayacak ve birbirine destek olabilecek şekilde yerleştirilmelidir. Ayrıca kabinler için Deprem Ayağı da konulmalıdır.

C.21.12. Veri Merkezinde, sunucu kabinler ve kablolama işleri aşağıdaki standartlar çerçevesinde olmalıdır.

C.21.12.1. UTP, fiber ve enerji kablolarını birbirinden ayırmak için kanallar kullanılmalıdır. Kablolar birbirinin manyetiğinden etkilenmemelidir. Yanmaz kablolar tercih önceliğine sahip olmalıdır.

C.21.12.2. Kablo sonlandırmaları olabildiğince sağlıklı yapılmalı gerekirse sonlandırma yapıldıktan sonra kabloda performans ölçme cihazlarıyla test yapılmalıdır.

C.21.12.3. Manyetik alanın yüksek olacağı yerlerde mutlaka fiber kablo kullanılmalı, manyetik alandan etkilenmediği için böyle noktalarda verileri fiber ile taşınmalıdır.

C.21.12.4. Kablolar döşenirken kıvrımlara izin verilmemeli, 90 derecelik keskin dönüşler daha yumuşak şekilde yapılmalıdır. Kabloların kırılmalarını veya dışlarındaki muhafazasına zarar verecek keskin kenarlar üzerinden geçmelerini engelleyecek malzemeler kullanılmalıdır.

C.21.12.5. Kabinler yerde sabit ayaklarda durmaları küçük sarsıntılarda ileri geri hareket etmelerini engelleyecek bir yapı oluşturulmalıdır. Deprem gibi durumlarda devrilme yer değiştirme gibi ihtimaller düşünülerek yerleşim yapılmalı, kablo bağlantıları çok gergin tutulmamalıdır.

C.21.12.6. Kabin kapakları şifreli olmalı yetkisiz personel tarafından açılmamalıdır.

C.21.12.7. Gerek elektrik gerek data kablolarında mutlaka ana bağlantıların yedekli olarak çekilmesine önem verilmelidir. Kabloların yedekliliğinin yanında yedek kabloların sistem odasına farklı bir güzergâhtan girişlerinin sağlanmalıdır.

C.21.12.8. Sunucular doğru şekilde etiketlenmeli, sunucu kabinleri çalışma yapılmadığı zamanlarda kilitlenmelidir. Sunucu kabinlerinde kablolamalar düzgün ve kolayca ayırt edilecek şekilde yapılmalıdır. Bütün kablolar ayrı ayrı etiketlenmelidir.

C.21.12.9. Sunucular arası kablo bağlantıları yer altından yapılmalıdır.

C.22.13. Veri merkezi kurulumunda ve kurulum sonrasında periyodik olarak gerekli testler yapılmalı ve yapılan bu testler dokümante edilmelidir.

C.22. Veri Tabanı Güvenliği

- C.22.1.** Veri tabanı sistemleri envanteri dokümente edilmeli ve bu envanterden sorumlu personel tanımlanmalıdır.
- C.22.2.** Veri tabanı işletim kuralları belirlenmeli ve dokümente edilmelidir.
- C.22.3.** Veri tabanı sistem kayıtları tutulmalı ve gerektiğinde idare tarafından izlenmelidir.
- C.22.4.** Veri tabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilmelidir.
- C.22.5.** Veri tabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli olarak alınması kontrol altında tutulmalıdır. Belirli aralıklarla yedekten geri dönme senaryoları ile backupların güvenilirliği test edilmelidir.
- C.22.6.** Veri tabanı yedekleme planları dokümente edilmelidir. Hangi veri tabanının, hangi yöntem ile hangi gün ve saatte yedeğinin alındığını içermelidir.
- C.22.7.** Manyetik kartuş, DVD veya CD ortamlarında tutulan log kayıtları en az 2 (iki) yıl süre ile çelik kasa gibi güvenli ortamlarda encrypted olarak saklanmalıdır.
- C.22.8.** Veri tabanı erişim politikaları kimlik doğrulama ve yetkilendirme usulleri çerçevesinde oluşturulmalıdır.
- C.22.9.** Hatadan arındırma, bilgileri yedekten dönme kuralları "Acil Durum Yönetimi" politikalarına uygun olarak oluşturulmalı ve dokümente edilmelidir.
- C.22.10.** Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.
- C.22.11.** Veri tabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmalarında yetkili bir personel bilgilendirilmelidir.
- C.22.12.** Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulmalı ve sonrasında ilgili uygulama kontrolleri gerçekleştirilmelidir.
- C.22.13.** Bilgi saklama medyaları kurum dışına çıkartılmamalıdır.
- C.22.14.** Sistem dokümantasyonu güvenli şekilde saklanmalıdır.
- C.22.15.** İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için temas edilecek kişiler belirlenmelidir.
- C.22.16.** Veri tabanı sunucusu sadece ssh, rdp, ssl ve veri tabanının orijinal yönetim yazılımına açık olmalı; bunun dışında ftp, telnet vb. gibi açık metin şifreli bağlantılara kapalı olmalıdır.
- C.22.17.** Uygulama sunucularından veri tabanına rlogin vb. şekilde erişilememelidir.
- C.22.18.** Veri tabanı sunucularına erişim şifreleri kapalı bir zarfta imzalı olarak kurumun kasasında saklanmalı ve gereksiz yere açılmamalıdır. Zarfın açılması durumunda ilgili yetkililer bilgilendirilmelidir.

- C.22.19.** Ara yüzden gelen kullanıcılar bir tabloda saklanmalı, bu tablodaki kullanıcı adı ve şifreleri şifrelenmiş(encrypted) olmalıdır.
- C.22.20.** Veri tabanı sunucusuna ancak zorunlu hallerde "root" veya "admin" olarak bağlanılmalıdır. Root veya admin şifresi tanımlı kişi/kişilerde olmalıdır.
- C.22.21.** Bağlanacak kişilerin kendi adına kullanıcı adı verilmeli ve yetkilendirme yapılmalıdır.
- C.22.22.** Veri tabanlarında yönetici yetkisine sahip (sysdba, sysoper, admin vb.) kullanıcı haklarına hangi kullanıcıların sahip olduğu kontrol edilmelidir.
- C.22.23.** Veri tabanlarında kullanıcı oluşturulabilmesi için üst idare tarafından hazırlanacak bir taahhütname doldurulmalıdır. Üst idare'ye resmi yazı ile başvurulmalıdır. Veri tabanındaki herhangi bir nesne için yapılacak yetki talepleri, ilgili nesnenin sahibi olan birim sorumlusundan veya proje yöneticisinden yazılı olarak veya e-posta yoluyla yapılmalı ve telefon ile teyit edilmelidir.
- C.22.24.** Bütün kullanıcıların yaptıkları işlemler kaydedilmelidir.
- C.22.25.** En üst düzey veri tabanı yöneticiliği yetkisi sadece bir kullanıcıda olmalıdır.
- C.22.26.** Veri tabanında bulunan farklı şemalara, kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişmesi engellenmelidir.
- C.22.27.** Veri tabanı sunucularına internet üzerinden erişimlerde VPN gibi güvenli bağlantılar kullanılmalıdır.
- C.22.28.** Veri tabanı sunucularına ancak yetkili kullanıcılar erişmelidir.
- C.22.29.** Veri tabanı sunucularına kod geliştiren kullanıcı dışında diğer kullanıcılar bağlanıp sorgu yapmamalıdır. İstekler ara yüzden sağlanmalıdır. (Örnek; Kullanıcılar tablolardan "select" sorgu cümleciklerini yazarak sorgulama yapmamalıdır.
- C.22.30.** Veri tabanı kullanıcılarının mesai saatleri içerisinde deployment yapmaları engellenmelidir.
- C.22.31.** Veri tabanı sunucularına giden veri trafiği ağ trafiğini dinleyen casus yazılımların verilere ulaşamaması için mümkünse şifrelenmelidir.
- C.22.32.** Bütün şifreler düzenli aralıklarla değiştirilmelidir. Şifre belirleme konusunda "Parola Güvenliği Politikası" esas alınmalıdır.
- C.22.33.** Sisteme giriş denemelerinde maksimum yanlış şifre giriş değeri belirlenmeli, bu değerin aşılması durumunda belirli bir süre kullanıcı hesabı kapatılmalıdır.
- C.22.34.** Veri tabanı kullanıcıları belirli aralıklarla incelenmeli ve veri tabanının kendi oluşturduğu veya sonradan oluşturulan ama kullanılmayan kullanıcı hesapları belirlenmeli ve kilitlenmelidir.
- C.22.35.** Veri tabanı sunucuları için yukarıda bahsedilen ve uygulanabilen güvenlik kuralları uygulama sunucuları için de geçerlidir.

C.22.36. Alınan veri tabanı yedekleri disklerdeki doluluk oranına bağlı olarak en azından en son full yedek ve devamındaki incremental yedekleri olacak şekilde saklanmalıdır.

C.22.37. Veri tabanı yedeklerinin başarılı bir şekilde alınıp alınmadığı bilgisi, yedekleme işleminin sonunda otomatik olarak e-posta yoluyla veri tabanı yöneticilerine gönderilmelidir.

C.22.38. Veri tabanı tablo erişim hakları belli aralıklarla denetlenmelidir.

C.22.39. Uygulama kullanıcısı üzerinden gelen DB sorgularının sorguyu yapan uygulama kullanıcısı ile eşleştirilmesi için gerekli altyapı/kodlama sağlanmalıdır.

C.23. Kaydedilebilir Taşınır Materyaller Güvenliği

USB flash diskler ve harici hddler; yüksek veri kapasiteleri, boyutları, taşınabilirlikleri ve farklı sistemlerde sorunsuzca çalışabilmeleri ile yanımızdan hiçbir zaman ayırmadığımız temel ihtiyaçlarımızdandır. Hemen hemen her sistemde çalıştırılabilir olmaları nedeniyle de bilgisayarlar arası veri alışverişimizi USB diskler ve harici hddler yardımıyla yapıyoruz.

USB disklerimizi onlarca farklı bilgisayarda kullanıyor, yine bilgisayarımıza onlarca farklı diskin takılmasına izin veriyoruz. Aslında USB diskleri tehlikeli kılan da bu çok da denetimli olmayan taşınabilirlikleri. Taşınabilir medya üzerinden bilgisayara giren zararlı yazılımlar başta bilgi sızdırma, uzaktan komut koşturma ve servis dışı bırakma olmak üzere birçok güvenlik zafiyetine neden olabilmektedir.

C.23.1. Taşınacak veri eğer usb disk ile taşınacaksa bu usb diskin tehdit unsuru olan bir yazılım içermediğine emin olunmalıdır.

C.23.2. Usb disk biçimlendirdikten sonra veriyi kopyalanmalıdır. Aksi takdirde içerisinde tehdit unsuru olan casus yazılımlar usb disk içindeki verinin silinmesine veya başkalarını eline geçmesine neden olabilir.

C.23.3. Taşınacak verinin de tehdit unsuru içeren herhangi bir yazılım içermediğine emin olunmalıdır.

C.23.4. Veriyi ister usb disk isterse de cd, dvd ortamında taşısın kesinlikle şifrelemelidir.

C.23.5. Veriyi usb disk ile taşıyorsak; bunları bilgisayara takarken usblerin sağlıklı çalıştığından emin olmalıyız. Aksi takdirde aygıtımızın bozulmasına neden olabilir.

C.23.6. Usb diskleri bilgisayardan çıkartırken aygıtı düzenli şekilde çıkart dedikten sonra bilgisayardan çıkartmalıyız aksi takdirde aygıtımız bozulabilir.

C.23.7. Harici taşınabilir disklerin içi mekanik yapıya sahip olduğundan dolayı darbelere karşı çok hassastır. Bu nedenle kullanırken ve taşırken dikkat edilmelidir. Özellikle hard diskler taşınırken koruyucu kılıflar içerisinde taşınmalıdır.

C.23.8. Cd ve dvdlerde veri saklamak için ise kaliteli medyalar kullanılmalı, düşük hızla yazdırmalı, alt yüzeye mümkün olduğunca temas etmemeli, nemli, ışıık almayan ortamlarda cdleri çok fazla sıkıştırmadan saklamalıdır.

C.23.9. Kötü amaçlı kimselerin bilgilerimize ulaşmasını engellemek için taşınabilir materyallerimizi güvenilir şekilde muhafaza etmeliyiz. Gerekirse kilitli dolaplarda veya çelik kasalarda muhafaza edilmelidir.

C.23.10. Taşınır materyaller çalışma masasında veya bilgisayarda güvensiz şekilde bırakılmamalıdır. Yanımızda, kaybedebileceğimizden dolayı mümkün olduğunca taşınmamalıdır. Eğer taşıyorsa veri kesinlikle şifrelenmelidir.

C.24. Bilgi Sistemleri Edinim Geliştirme ve Bakımı

C.24.1. Bakanlık politikalarına uygun ihtiyaçlar hızlı ve güvenli bir şekilde sağlanmalıdır.

C.24.2. Yatırım yapılan teknolojilerde üretici bağımsız ve yaygın ürünler tercih edilmelidir.

C.24.3. Bilgi sistemleri ihtiyaçları tam, sorunsuz karşılayacak ürünler tercih edilmelidir.

C.24.4. Tüm bilgi sistemleri ihtiyaçları, kapasite planlaması yapılarak tespit edilmelidir. Gerekli ihtiyaçlar ivedilikle yönetime sunulmalıdır.

C.24.5. Üreticilerden sistemler ile ilgili bakım prosedürleri sağlanmalıdır.

C.24.6. Firma teknik destek elemanlarının bakım yaparken "Sağlık Bakanlığı Bilgi Güvenliği Politikaları" na uygun davranmaları sağlanmalı ve kontrol edilmelidir.

C.24.7. Sistem üzerinde yapılacak değişiklikler ile ilgili olarak "Değişim Yönetimi Politikası" uygulanmalıdır.

C.24.8. Bakım yapıldıktan sonra tüm sistem dokümantasyonu güncellenmelidir.

C.24.9. 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.

C.24.10. Sistem bakımlarından sonra bir güvenlik açığı olduğundan şüphelenilmesi durumunda "Bilgi Güvenliği Politikaları" uyarınca hareket edilmelidir.

C.24.11. Kurum sistemlerinin tamamı (donanım, uygulama yazılımları, paket yazılımlar, işletim sistemleri) periyodik bakım güvencesine alınmalıdır. Bunun için bütçe ayrılmalıdır.

C.24.12. Yüklenici teknik destek elemanlarının bakım yaparken bu kılavuza uygun davranmaları sağlanmalı ve kontrol edilmelidir.

C.24.13. Bilgi sistemleri edinimi ve sistem geliştirmede güvenlik gereksinimi analizi;

C.24.13.1 Kontrol gereksinimlerinin belirtimi bilgi sistemi içerisindeki otomatik kontrolleri ve manüel kontrolleri kapsar. Aynı kontroller iş ihtiyaçları için geliştirilen veya sipariş edilen yazılım paketleri için de dikkate alınmalıdır.

C.24.13.2 Güvenlik gereksinimleri ve kontroller bilgi varlıklarının iş değerini ve güvenlik kaybı veya güvenlik hatalarından kaynaklanan potansiyel iş kayıpları göz önüne alınarak düzenlenmelidir.

C.24.13.3 Bilgi güvenliği için sistem gereksinimleri ve güvenliği uygulama süreçleri bilgi sistemleri projelerinin ilk aşamalarında entegre edilmelidir. Tasarım aşamasında oluşturulan kontrollerin uygulanması ve geliştirilmesi sistemlerin kurulması veya kurulması aşamasından sonraki aşamalarındaki uygulanmasından daha az maliyetli olacaktır.

C.24.13.4 Eğer ürünler sipariş edilmiş ise bir test ve edinim süreci takip edilir. Üreticiler ile yapılan sözleşmeler belirlenmiş güvenlik gereksinimlerini karşılamalıdır. Güvenlik fonksiyonlarının gereksinimleri karşılamadığı noktada, satın almadan önce riskler belirlenmeli ve ilgili kontroller oluşturulmalıdır.

C.24.14. Uygulama yazılımlarında giriş verisinin geçerlemesi;

C.24.14.1 Sınır dışı değerler, veri alanlarındaki geçersiz karakterler, kayıp veya eksik veri, üst ve alt değer sınırlarının aşımı, yetkisiz veya tutarsız kontrol verisi gibi hataları gidermek için çift giriş, sınır kontrolü, gibi giriş değeri kontrolleri yapılmalıdır.

C.24.14.2 Anahtar alanların veya veri dosyalarının geçerliliğini ve bütünlüğünü korumak için içeriklerinin periyodik olarak gözden geçirilmesi sağlanmalıdır.

C.24.14.3 Geçerleme hatalarına karşılık olarak izlenecek süreçler belirlenmelidir.

C.24.14.4 Makul girdi verisinin test süreçleri uygulanmalıdır.

C.24.14.5 Veri girişi ile görevlendirilen personelin sorumlulukları belirlenmelidir.

C.24.14.6 Veri giriş prosesi için izleme (log) kayıtları tutulmalıdır.

C.24.15. Uygulama yazılımlarında iç işleyişin kontrolü;

C.24.15.1 Veri değişikliklerini işlemek için ekleme, değiştirme ve silme fonksiyonları kullanılmalıdır.

C.24.15.2 Programların yanlış sırada çalışmasını veya önceki programın hataya düşmesi durumunda sıradaki programın çalışmasını önlemek maksadıyla kontroller yapılmalıdır.

C.24.15.3 Tampon belleğin aşırı işlem/taşma durumunu kullanarak yapılan ataklara karşı koruma sağlanmalıdır.

C.24.16. İç işleyiş ile ilgili kontrol listeleri aşağıdaki hususları dikkate almalıdır;

- İşlem güncellemelerinden sonra veri kütüklerini dengeleyen ve düzenleyen oturum süresince veya toplu kipte yürütülen kontroller,
- Önceki kütük kapatmalarına karşı açma dengelemelerini kontrol etmek için programların çalışması esnasında, kütük güncellemeleri bazında ve programlar bazında yapılan dengeleme ayarları,
- Sistem tarafından üretilen girdi verisinin doğrulanması,
- Merkezi ve uzak sistemler arasında indirilen veya karşı tarafa yüklenen veri veya yazılımın bütünlüğü, yetki durumu ve diğer güvenlik seviyesinin kontrolü,
- Kayıtların ve kütüklerin özetleme algoritmalarının toplamları,
- Uygulama programlarının doğru zamanda çalıştığının kontrolü,
- Programların doğru sırada çalışması, hata durumunda çalışmanın kesilmesi ve sorun çözülünceye kadar çalışmanın durdurulduğunun kontrolü,
- İşlev kapsamındaki faaliyetlerin izleme kayıtlarının (log) yaratılması,

- Uygulamalarda yetkilendirme ve mesaj bütünlüğünün korunması, bu maksatla uygun kontrollerin belirlenmesi.

C.24.17. Uygulama yazılımlarında çıkış verisinin geçerlemesi;

C.24.17.1 Çıktı verisinin uygunluğu kontrol edilmelidir.

C.24.17.2 Tüm verinin işlenmesini sağlanmalıdır.

C.24.17.3 Bilginin doğruluğunu, tam olduğunu, hassasiyetini ve sınıflandırmasını belirtmek maksadıyla yeterli bilgi sağlanmalıdır.

C.24.17.4 Çıktı geçerleme testleri uygulanmalıdır.

C.24.17.5 Çıktı geçerleme testlerinin izleme kayıtları (log) tutulmalıdır.

C.24.17.6 Sağlık bilgi sistemlerindeki çıktıların doğruluğunun taşıdığı hayati önem daima göz önünde bulundurulmalıdır.

C.24.18. Operasyonel sistemlerdeki arızaları en aza indirmek ve güvenli işletim için aşağıdaki hususlara dikkat edilmelidir;

C.24.18.1 Yazılım uygulamaları ve program kütüphanelerinin güncellemesi eğitimli personel tarafından uygun yönetim yetkisi altında yapılmalıdır.

C.24.18.2 Operasyonel sistemler sadece onaylanmış çalıştırılabilir kodları tutar, bu sistemlerde geliştirme kodları veya derleyiciler bulunmamalıdır.

C.24.18.3 Uygulama ve operasyon sistem yazılımları geniş kapsamlı ve başarılı testlerden sonra sisteme yüklenmelidir. Bu testler kullanılabilirlik, güvenlik, diğer sistemler üzerindeki etkiler ve kullanım kolaylığı testlerini içerir ve ayrı sistemlerde uygulanmalıdır. Karşılık gelen program kaynak kütüphanelerinin güncellenmesi sağlanmalıdır.

C.24.18.4 Sistemin konfigürasyonu dokümente edilmeli, uygulanan yazılımların kontrolü için bir konfigürasyon kontrol sistemi oluşturulmalıdır.

C.24.18.5 Değişiklikler yürürlüğe girmeden önce bir geri kurtarma stratejisi belirlenmelidir.

C.24.18.6 Operasyonel program kütüphanelerinin güncellenmesinde izleme kayıtlarının (audit log) tutulması sağlanmalıdır.

C.24.18.7 Beklenmedik durumlar için uygulama yazılımlarının önceki versiyonlar saklanmalıdır.

C.24.18.8 Veri arşivlendiği sürece yazılımların eski versiyonları, gerekli bilgi, parametreler, prosedürler, konfigürasyon detayları ve destek yazılımları ile birlikte arşivlenmelidir.

C.24.19. Operasyonel verinin test verisi olarak kullanılırken güvenliğinin sağlanması;

C.24.19.1 Operasyon sistemi için kullanılan erişim kontrol usulleri test uygulama sistemlerinde de kullanılır.

C.24.19.2 Test sistemine operasyon bilgisinin her kopyalanışında ayrı bir yetkilendirme yapılmalıdır.

C.24.19.3 Test tamamlanmayı müteakip operasyonel bilgi test sisteminden hemen silinmelidir.

C.24.19.4 Operasyonel bilginin kopyalanması ve kullanımının izleme kayıtları (audit log) tutulmalıdır.

C.24.19.5 Sağlık bilgi sistemlerinde saklanan veriler asla test maksatlı olarak kullanılamaz.

C.24.20. Program kaynak kodlarına erişimin kontrolü;

C.24.20.1 Mümkün olduğu takdirde programların kaynak kütüphaneleri operasyonel sistemler üzerinde tutulmaz.

C.24.20.2 Programların kaynak kodları ve kaynak kodu kütüphaneleri kontrol altında bulundurulmalıdır.

C.24.20.3 Destek personeli program kaynak kodu kütüphanelerine sınırsız erişim yetkisine sahip olamaz.

C.24.20.4 Program kaynak kütüphanelerinin, ilgili öğelerin ve program kaynaklarının programcılara yayımı uygun yetkiler alındıktan sonra yapılmalıdır.

C.24.20.5 Program listeleri güvenli bir ortamda saklanmalıdır.

C.24.20.6 Program kaynak kütüphanelerine erişimlerin izleme kayıtları (log) tutulmalıdır.

C.24.20.7 Program kaynak kütüphanelerinin bakımı, kopyalanması sıkı değişim kontrolleri ile kontrol altında bulundurulmalıdır.

C.24.21. Değişim kontrolleri aşağıda belirtilen hususları içermelidir;

C.24.21.1 Kararlaştırılmış yetki seviyelerinin kaydı tutulmalıdır.

C.24.21.2 Değişikliklerin yetkili kullanıcılar tarafından yapılması sağlanmalıdır.

C.24.21.3 Değişikliklerin mevcut durumu tehlikeye atmaması için kontroller ve bütünlük süreçleri gözden geçirilmelidir.

C.24.21.4 İyileştirme gerektiren yazılımın tamamı, bilgi, veri tabanı varlıkları ve donanım belirlenmelidir.

C.24.21.5 İşin başlamasından önce resmi bir onay alınmalıdır.

C.24.21.6 Yetkili kullanıcıların uygulamadan önce değişiklikleri üstlenmeleri sağlanmalıdır.

C.24.21.7 Her değişiklikten sonra sistem dokümantasyonunun güncellenmesi, eski dokümantasyonun arşivlenmesi veya imha edilmesi sağlanmalıdır.

C.24.21.8 Tüm yazılım güncellemeleri için sürüm kontrolü sağlanmalıdır.

C.24.21.9 Tüm değişiklik gereksinimlerinin izleme kayıtları (log) tutulmalıdır.

C.24.21.10 Operasyon dokümanlarının uygun bir şekilde değiştirilmesi sağlanmalıdır.

C.24.21.11 Değişiklik uygulamalarının iş süreçlerini bozmayacak şekilde uygun zamanda yapılması sağlanmalıdır.

C.24.22. İşletim sistemindeki değişikliklerden sonra uygulamaların teknik olarak gözden geçirilmesi;

C.24.22.1 Uygulama kontrollerinin ve bütünlük prosedürlerinin işletim sistemi değişikliklerinden zarar görmediğini garanti etmek için gözden geçirilmesi sağlanmalıdır.

C.24.22.2 Yıllık destek planı ve bütçenin işletim sistemi değişikliğinden kaynaklanan gözden geçirme ve sistem testlerini karşılaması sağlanmalıdır.

C.24.22.3 İş süreklilik planlarında uygun değişikliklerin yapılması sağlanmalıdır.

C.24.23. Yazılım paketlerinde değişiklik yapıldığında aşağıdaki hususlar dikkate alınmalıdır;

C.24.23.1 Yazılım içindeki kontroller ve bütünlüğün tehlikeye düşme riski değerlendirilmelidir.

C.24.23.2 Satıcının izninin alınıp alınmayacağı belirlenmelidir.

C.24.23.3 İhtiyaç duyulan değişikliklerin satıcıdan standart program güncellemesi olarak alınma ihtimali değerlendirilmelidir.

C.24.23.4 Eğer kurum değişiklikler sonucunda ileriki bakımlar için sorumlu olacaksa bunun etkisi değerlendirilmelidir.

C.24.24. Bilgi sızma risklerini kısıtlamak amacıyla aşağıdaki hususlar dikkate alınmalıdır;

C.24.24.1 Saklı bilgi için gönderilen ortam ve iletişimin taranması sağlanmalıdır.

C.24.24.2 Üçüncü tarafların sistem ve iletişim durumlarından muhtemel bilgi çıkarmalarını azaltmak için bu durumlar maskelenir veya değiştirilmelidir.

C.24.24.3 Yüksek seviyede bütünlük sağlayan sistem ve yazılımlar kullanılmalıdır.

C.24.24.4 Mevcut mevzuat ve düzenlemeler çerçevesinde personel ve sistemin düzenli olarak gözlenmesi sağlanmalıdır.

C.24.24.5 Bilgisayar sistemlerindeki kaynak kullanımı izlenmelidir.

C.24.25. Dışarıdan (dış kaynaktan) sağlanan yazılım geliştirme ile ilgili olarak aşağıda belirtilen konular dikkate alınmalıdır;

- Lisans anlaşmaları, kod mülkiyeti, telif hakları,
- Yürütülen işin kalitesi ve doğruluğuna ait sertifikasyon,
- Üçüncü tarafın başarısız olması durumunda alınacak tedbirler,
- Yapılan işin kalite ve doğruluğunun izlenmesi için yetki,
- Kodun kalitesi ve güvenlik fonksiyonelliği için sözleşme gereksinimleri,
- Kurulumdan önce zararlı ve trojan kodları tespit etmek için test etme.

C.24.26. Teknik açıklıkların kontrolü;

C.24.26.1 Açıklıkları gözleme, açıklık risk belirlemesi, yamalar, varlıkların izlenmesi, gerekli koordinasyon sorumlulukları dâhil teknik açıklıkların yönetimiyle ilgili görevler ve sorumluluklar belirlenmelidir.

C.24.26.2 Teknik açıklıkları belirlemek ve bunlarla ilgili farkındalığı sağlamak için kullanılacak kaynaklar belirlenmelidir. Bu kaynaklar envanter değişikliklerinde veya yeni kaynaklar bulunduğunda güncellenmelidir.

C.24.26.3 Potansiyel teknik açıklık bildirimlerine reaksiyon göstermek için bir zaman çizelgesi oluşturulmalıdır.

C.24.26.4 Potansiyel bir teknik açıklık ortaya çıktığında ilgili riskler ve alınacak tedbirler belirlenmeli böyle bir tedbir açıklık olan sistemlerin yamalanması veya diğer kontrolleri içerebilmelidir.

C.24.26.5 Teknik açıklığın belirlenmesinin aciliyetine bağlı olarak alınan tedbir değişim yönetimiyle ilgili kontrollere göre veya güvenlik ihlali durumunda uygulanacak süreçlere göre devam ettirilmelidir.

C.24.26.6 Eğer yama mevcutsa yamanın oluşturabileceği riskler ile teknik açıklığın riskleri karşılaştırılmalıdır.

C.24.26.7 Yamalar yüklenmeden önce etkinliğini ve tolerans gösterilemeyecek yan etkilerini ortaya koymak amacıyla test edilmelidir. Eğer yama mevcut değil ise açıklıkla ilgili servisler ve imkânlar kapatılmalı, ağ sınırlarına güvenlik duvarı kurulması gibi erişim kontrolleri ilave ve adapte edilmeli, mevcut atakları önlemek ve tespit etmek için izleme artırılmalı ve açıklığın farkındalığı artırılmalıdır.

C.24.26.8 Uygulanan tüm prosedürler için izleme kaydı (log) tutulmalıdır.

C.24.26.9 Yüksek riskli sistemler öncelikle belirlenmelidir.

C.25. Yedekleme ve İş Sürekliliği Yönetimi

C.25.1. Veri Yedekleme

C.25.1.1. Veri yedeklemesi kurumun kritik BT işlemlerinden birisidir. Kurum politikasında yedekleme konusu mutlaka yer almalı ve veri yedeklemesi için yönetim prensiplerini ortaya koyan bir politika bulunmalıdır. Kurum verisinin yedekleme işlemleri yedekleme politikasına göre yerine getirilmelidir.

C.25.1.2. Kurumun bütün verisinin, kurum çapında kullanılan işletim sistemlerinin ve uygulamaların tamamının yedeği uygun ve düzenli olarak alınmalıdır.

C.25.1.3. Yedekleme sistemi iş sürekliliği planında yer alan veri yedekleme ihtiyacını karşılamalıdır.

C.25.1.4. Yedeği alınacak veri ve uygulamalar için sınıflandırma yapılmalı ve her bir sınıf için kabul edilmeli veri kaybı süresi belirlenmelidir.

C.25.1.5. Kabul edilir veri kaybı süresi yönetim tarafından onaylanmalıdır.

C.25.1.6. Yedekleme işlemlerinin sağlanması için yedekleme politikasına uygun olarak bir yedekleme planı oluşturulmalıdır.

C.25.1.7. Yedekleme işlerine ait kayıtlar tutulmalıdır.

C.25.1.8. Başarısız olan yedekleme işleri takip edilmeli ve yedeği alınamamış verinin yedeği alınmalıdır.

C.25.1.9. Yedekleme medyaları etiketlenmeli ve hangi medyada hangi yedeğin bulunduğu dair kayıtlar tutulmalıdır.

C.25.1.10. Yedekleme medyalarının kopyaları alınarak ana sistem odasına zarar verebilecek felaketlerden etkilenmeyecek kadar uzakta ve güvenli olarak depolanmalıdır.

C.25.1.11. Yedeklenmiş verinin düzenli aralıklarla geri döndürme testi yapılmalıdır.

C.25.1.12. Yedekleme altyapısı, yedekleme ve geri döndürme işlemleri için talimatlar hazırlanmalıdır.

C.25.1.13. Yedeklemesi alınacak bilginin seviyesi belirlenmelidir.

C.25.1.14. Yedekleme kopyalarının doğru ve tam kayıtları ve dokümanite edilmiş geri yükleme süreçleri sağlanmalıdır.

C.25.1.15. Yedeklemenin türü (tam yedekleme/değişen kayıtların yedeklenmesi), yedeklemenin sıklığı iş gereklerine, güvenlik gereksinimlerine ve bilginin kritiklik derecesine göre belirlenmelidir.

C.25.1.16. Yedeklerin bir kopyası doğal afetlerden ve olası tehlikelerden korumak maksadıyla ana merkezden uzak bir merkezde saklanmalıdır.

C.25.1.17. Yedekleme bilgisine uygun seviyede fiziksel ve çevresel koruma sağlanmalıdır.

C.25.1.18. Herhangi bir tehlike durumunda kullanımını sağlamak maksadıyla yedekleme bilgisi düzenli olarak test edilmelidir.

C.25.1.19. Geri yükleme süreci düzenli olarak kontrol ve test edilmelidir.

C.25.1.20. Gizliliğin önemli olduğu durumlarda yedeklemelerin kriptolu olarak alınması göz önünde bulundurulmalıdır. Bu kapsamda özellikle kişisel sağlık bilgilerinin kriptolu olarak yedeklenmesine dikkat edilmelidir.

C.25.2. İş Sürekliliği Yönetimi

C.25.2.1. Kuruluşun karşılaşılabileceği risklerin olasılığı, zaman içerisindeki etkisi, kritik iş süreçleri belirlenmelidir.

C.25.2.2. Kritik iş süreçleri kapsamındaki varlıklar belirlenmelidir.

C.25.2.3. Hangi bilgi güvenliği olaylarının iş sürekliliğinde kesintilere neden olduğu ve etkisi araştırılmalıdır.

C.25.2.4. Operasyonel risk yönetiminin olabileceği gibi tüm iş sürekliliği sürecinin bir parçasının sigorta ettirilmesi değerlendirilmelidir.

C.25.2.5. Önleyici ve zararı azaltıcı ilave kontroller uygulanmalıdır.

C.25.2.6. Belirlenmiş bilgi güvenliği gereksinimleri için yeterli finansal, kurumsal, teknik ve çevresel kaynakların tahsis edilmesi sağlanmalıdır.

C.25.2.7. Personel güvenliği, bilgi işleme tesisleri ve kurumsal varlıkların korunması garanti altına alınmalıdır.

C.25.2.8. Kabul görmüş iş sürekliliği stratejisi paralelinde bilgi güvenliği gereksinimlerine işaret eden iş sürekliliği planları formüle ve dokümante edilmelidir.

C.25.2.9. Uygulamaya konulan plan ve süreçlerin düzenli olarak test edilmesi ve güncellenmesi sağlanmalıdır.

C.25.2.10. İş sürekliliği yönetiminin kurumun süreçleri ve yapısı ile birleştirilmesi, iş sürekliliği yönetim sorumluluklarının kurum içerisinde uygun seviyelere atanması konuları göz önüne alınmalıdır.

C.25.2.11. Bilgi güvenliğini içeren süreklilik planlarını geliştirme ve gerçekleştirme;

C.25.2.11.1. İş sürekliliği prosedürleri ve tüm sorumluluklar belirlenmelidir.

C.25.2.11.2. Kabul edilebilir bilgi ve hizmet kayıpları belirlenmelidir.

C.25.2.11.3. İş operasyonlarının kurtarılması ve yeniden başlatılması için prosedürler uygulanmalıdır.

C.25.2.11.4. Kurtarma ve yeniden başlatmayla ilgili askıda kalan işlerin tamamlanmasını sağlayan operasyonel prosedürler belirlenmelidir.

C.25.2.11.5. Kabul görmüş işlev ve prosedürler dokümante edilmelidir.

C.25.2.11.6. Kriz yönetimi dâhil kabul görmüş işlev ve prosedürlerle ilgili personel eğitilmelidir.

C.25.2.11.7. Planlar test edilmeli ve güncel bulundurulmalıdır.

C.25.2.12. İş sürekliliği planlarını test etme;

C.25.2.12.1. Farklı senaryoların masa üstü testleri (örnek kesintiler kullanılarak iş kurtarma düzenlemelerinin tartışılması) yapılmalıdır.

C.25.2.12.2. Simülasyonlar (özellikle insanların olay/kriz yönetimindeki rolleri ile ilgili eğitimleri) gerçekleştirilmelidir.

C.25.2.12.3. Teknik kurtarma testleri (bilgi sistemlerinin etkin olarak geri yüklenmesinin sağlanması), yapılmalıdır.

C.25.2.12.4. Alternatif bir yerde geri yükleme (iş süreçlerinin kurtarma operasyonlarına paralel olarak esas yerden uzakta çalıştırılması) test edilmelidir.

C.25.2.12.5. Üreticilerin hizmetleri ve kolaylıkları (haricen sağlanan hizmet ve ürünlerin sözleşme hükümlerini karşılamaının sağlanması) test edilmelidir.

C.25.2.12.6. Tam bir tatbikat (kuruluşun, personelin, malzemenin, tesislerin ve süreçlerin kesintilerin üstesinden gelme durumunun test edilmesi) gerçekleştirilmelidir.

C.25.2.12.7. Sağlık bilgi sistemlerinde iş sürekliliğinin sağlanmasının taşıdığı hayati önem göz önüne alınarak alınacak tedbirler eksiksiz yerine getirilmelidir.

C.26. Bilgi Kaynakları Atık ve İmha Yönetimi

C.26.1. Bakanlık ve Bağlı Kuruluşlar kendi bünyelerinde oluşturacakları arşivden sorumludur. Evraklar idari ve hukuki hükümlere göre belirlenmiş Evrak Saklama Planı'na uygun olarak muhafaza edilmesi gerekmektedir.

C.26.2. Yasal bekleme süreleri sonunda tasfiyeleri sağlanmalıdır. Burada Özel ve Çok Gizli evraklar “Devlet Arşiv Hizmetleri Yönetmeliği” hükümleri gereği oluşturulan “Evrak İmha Komisyonu” ile karar altına alınmalı ve imha edilecek evraklar kırılma veya yakılarak imhaları yapılmalıdır. İmha edilemeyecek evrak tanımına giren belgeler geri dönüşüme devirleri yapılmalıdır.

C.26.3. Bilgi Teknolojilerinin (Disk Storage Veri tabanı dataları vb.) 14 Mart 2005 Tarihli 25755 sayılı Resmi Gazete 'de yayınlanmış, sonraki yıllarda da çeşitli değişikliklere uğramış katı atıkların kontrolü yönetmeliğine ve Basel Sözleşmesine göre donanımların imha yönetimi gerçekleştirilmelidir. Komisyonca koşullar sağlanarak donanımlar parçalanıp, yakılıp (Özel kimyasal maddelerle) imha edilmelidir.

C.26.4. İmha işlemi gerçekleştirecek materyalin özellik ve cinsine göre imha edilecek lokasyon belirlenmelidir.

C.26.5. Uygun şekilde kırılması ve kırılma sürecinden önce veri ünitelerinin adet bilgisi alınmalıdır.

C.26.6. Yetkilendirilmiş personel tarafından imhası gerçekleşen atıklara data imha tutanağı düzenlenmesi ve bertaraf edilen ürünlerin seri numaraları ve adet bilgisinin data-imha tutanağı düzenlenmelidir.

C.26.7. Kırılan parçaların fiziksel muayene ile tamamen tahrip edilip edilmediğinin kontrolü yapılmalıdır.

C.26.8. Tamamen tahrip edilememiş disk parçalarının delme, kesme makinaları ile kullanılamaz hale getirilmelidir.

C.26.9. Hacimsel küçültme işlemi için parçalanmalıdır.

C.26.10. Son ürünlerin gruplar halinde fotoğraflanarak ilgili kişi ve/veya kuruma iletilmesi gereklidir.

C.26.11. Çıkan metallerin sınıflarına göre ayrılarak, biriktirildikten sonra eritme tesislerine iletilmesi gerekmektedir.

C.27. Bilgi Güvenliği Teknik ve Farkındalık Eğitimleri

C.27.1. Kurum içerisinde bilgi güvenliği teknik ve farkındalık eğitimleri için yıllık bir plan yapılmalıdır.

C.27.2. Yıllık planlar çerçevesinde bilgi güvenliği teknik ve farkındalık eğitimleri gerçekleştirilmelidir.

C.27.3. Sunulan bilgi güvenliği teknik ve farkındalık eğitimleri katılım öncesi ve sonrası çeşitli ölçme teknikleriyle ölçülmeli ve eğitim etkililiği hususunda değerlendirme yapılmalıdır.

C.27.4. Kurumların teknik işlerinde (Bilişim faaliyetleri), uygulama geliştirme, sistem güvenliği kapsamında hizmet veren personellerin kişisel gelişimlerinin devamlılığı konusunda eğitimler düzenlenmelidir.

C.27.5. Eğitime katılım formları muhafaza edilmelidir.

C.27.6. Eğitim faaliyetleri işlemlerinin, kurum içerisinde nasıl yürütülmesi gerektiği hususunda bir prosedür geliştirilmelidir.

C.28. Değişim Yönetimi

C.28.1. Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümente edilmelidir.

C.28.2. Yazılım ve donanım envanteri oluşturularak, yazılım sürümleri kontrol edilmelidir.

C.28.3. Herhangi bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenmeli ve dokümente edilmelidir.

C.28.4. Değişiklikler gerçekleştirilmeden önce kurumun ilgili biriminden onay alınmalıdır.

C.28.5. Tüm sistemlere yönelik yapılandırma dokümantasyonu oluşturulmalı, yapılan her değişikliğin bu dokümantasyonda güncellenmesi sağlanarak kurumsal değişiklik yönetimi ve takibi temin edilmelidir.

C.28.6. Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanmalı ve ilgili yöneticiler tarafından onaylanması sağlanmalıdır.

C.28.7. Ticari programlarda yapılacak değişiklikler, ilgili üretici tarafından onaylanmış kurallar çerçevesinde gerçekleştirilmelidir.

C.28.8. Teknoloji değişikliklerinin kurumun sistemlerine etkileri belirli aralıklarla gözden geçirilmeli ve dokümente edilmelidir.

C.28.9. Değişiklik yönetimini işletmek için bir talep yönetim sistemi kurmak ve işletmek önemlidir. Talebin nasıl alınacağı ve değerlendirileceği gibi esaslar tanımlanmalıdır.

C.28.10. Değişiklik onayının, “hangi kontroller ne şekilde yapıldıktan sonra verileceği” tanımlanmalıdır.

C.28.11. Değişiklik öncesi test süreci tanımlanmalıdır.

C.28.12. Değişikliğin varlık kritikliğine göre yapılacağı zaman ve yöntemler tanımlanmalıdır.

C.29. İhlal Bildirim ve Yönetimi

C.29.1. Bilginin gizlilik, bütünlük ve kullanılabilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumlarında mutlaka kayıt altına alınmalıdır.

C.29.2. Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci oluşturulmalıdır.

C.29.3. Bilgi güvenliği ihlâli oluşması durumunda kişilerin tüm gerekli faaliyetleri hatırlamasını sağlamak maksadıyla bilgi güvenliği olayı rapor formatı hazırlanmalıdır.

C.29.4. Güvenlik olayının oluşması durumunda olay anında raporlanmalıdır.

C.29.5. İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.

C.29.6. Güvenlik ihlaline neden olan çalışanlar, üçüncü taraflarla ilgili resmi bir disiplin sürecine başvurulur.

C.29.7. Tüm çalışanlar, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği olayını önlemek maksadıyla güvenlik zayıflıklarını doğrudan kendi yönetimlerine veya hizmet sağlayıcılarına mümkün olan en kısa sürede rapor edilir.

C.29.8. Bilgi sistemi arızaları ve hizmet kayıpları, zararlı kodlar, dos atakları, tamamlanmamış veya yanlış iş verisinden kaynaklanan hatalar, gizlilik ve bütünlük ihlâlleri, bilgi sistemlerinin yanlış kullanımı gibi farklı bilgi güvenliği olaylarını bertaraf edecek tedbirler alınır.

C.29.9. Normal olasılık planlarına ilave olarak olayın tanımı ve sebebinin analizi, önleme, tekrarı önlemek maksadıyla düzeltici tedbirlerin planlanması ve uygulanması, olaylardan etkilenen veya olaylardan kurtulanlarla iletişim, eylemin ilgili otoritelere raporlanması konuları göz önüne alınır.

C.29.10. İç problem analizi, adli incelemeler veya üretici firmadan zararın telafi edilmesi için aynı türdeki olayların izleme kayıtları (log) toplanır ve korunur.

C.29.11. Güvenlik ihlallerinden kurtulmak için gereken eylemler, sistem hatalarının düzeltilmesi hususları dikkate alınır.

C.29.12. Bilgi güvenliği olaylarının değerlendirilmesi sonucunda edinilen bilgi ile edinilen tecrübe ve yeni kontrollerin oluşturulması, aynı olayın tekrar etmesini önleyecek veya yüksek etkili olayların oluşmasını engelleyecektir.

C.29.13. Kanıt toplama; kuruluş içerisinde disiplin faaliyeti için delil toplanırken uygulanacak genel kurallar şunlardır;

- Kanıtın mahkemede kullanılıp kullanılamayacağı ile ilgili kabul edilebilirlik derecesi,
- Kanıtın niteliği ve tamlığını gösteren ağırlığı.

C.31.14. Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, kurum Personel Yönetmeliği gereğince aşağıdaki yaptırımlardan bir ya da birden fazla maddesini uygulayabilir:

- Uyarma,
- Kınama,
- Para cezası,
- Sözleşme feshi.

C.30. Bilgi Güvenliği İzleme ve Denetleme Yönetimi

- C.30.1.** Bilgi Güvenliği Sistemi düzenli olarak denetlenmesi sağlanmalıdır.
- C.30.2.** Kurum yetkilileri tarafından Bilgi Güvenliği İç Denetimleri yapılmalıdır.
- C.30.3.** Hazırlanacak Bilgi Güvenliği İç Denetim soru listeleri hazırlanmalıdır.
- C.30.4.** Denetim yapacak personelin Bilgi Güvenliği konusunda yetkilendirilmiş kurumlardan iç denetim eğitimi almaları, denetime katılacak kişilerin iç denetçi sertifikasının olması gerekir.
- C.30.5.** İç denetimler için bütün birimleri kapsayacak şekilde denetim planı hazırlanmalıdır.
- C.30.6.** Denetim sonuçları iç denetim raporu şeklinde hazırlanmalı ve üst yönetime sunulmalıdır.
- C.30.7.** Denetimlerde tespit edilen bulgular için çözüm önerileri geliştirilmelidir.
- C.30.8.** Bir sonraki yapılacak iç denetimlerde, bir önceki tespit edilen bulguların çözümlenip çözümlenmediği hususunda takip yapılmalıdır.

C.31. Bilgi Güvenliği Testleri

- C.31.1.** Kılavuzda belirtilen standartların uygulanmasının kontrolleri hususunda yıllık plan yapılmalı, bu plan ile takvim günleri belirlenmelidir.
- C.31.2.** Belirlenen yıllık plana uygun olarak kullanıcı seviyesinde, yöneticiler seviyesinde, sistem yürütücü ekip seviyesinde, makineler seviyesinde, network seviyesinde gerekli kontroller, testler yapılmalıdır.
- C.31.3.** Yapılan kontrol, testler sonucunda çıkan sonuçlar puanlandırılarak raporlanmalıdır. Rapor içeriğindeki ilgili bölümlerin puanlandırma seviyesine göre gerekli hallerde ek farkındalık eğitimleri, seminerler verilmelidir. Makine ve network sistemi için gerekli görülen ek ayar düzeltmeleri yapılmalıdır.
- C.31.4.** Puanlandırma sisteminin oluşturulmasında sahadan Bilgi Güvenliği Kılavuzuna uygun olarak oluşturulmuş formlara belirlenecek personel tarafından veri bildirimleri giridirmeli ve bu formlara uygun olarak yılın belirlenecek zamanlarında formlara uygun olarak oluşturulacak puanlamaların fiziksel kontrolleri sağlanmalıdır.
- C.31.5.** Yapılacak kontroller ve testler ISO 27001 sistemine, TÜBİTAK UEKAE, Siber Güvenlik Enstitüsü standartlarına bağlı kalınarak yürütülmelidir.

C.32. Acil Durum Yönetimi

- C.32.1.** Acil durumlar için acil durum ekibi belirlenmelidir ve eğitilmelidir. Acil durum ekibi ve görev tanımları aşağıda belirtilmiştir;
 - C.32.1.1.** Ekip başı:
 - Paniğe engel olur.
 - Acil durumlarda müdahale şeklini belirler ve yönetir

- Acil durumda hemen müdahale edilmesi için tedbir ve takviye için talimatlar verir.
- Ekibindeki kişilerin güvenliğini sağlar.
- Olay yerine gelen itfaiye, emniyet, ambulans vs. ye gereken tüm bilgileri verir.
- Kendi ekibi ile gelen takviye ekiplerin uyumlu çalışmasını sağlar.

C.32.1.2. Haberci:

- Acil durum ihbarı gelmesi ile tüm dahili ve harici ilgisiz telefon görüşmelerini kestirir.
- İlgili tüm birimlere bilgi verir.
- Jandarma ve emniyet ile temasa geçerek dış kargaşaların önlenmesini sağlar.(gerekliyse)
- Varsa yaralıları hakkında hastanelere bilgi aktarır.
- Ekip başının talimatlarını uygular.

C.32.1.3. Müdahale ekibi ve yardımcısı:

- Ekip başının talimatlarıyla olaylara müdahale ederler.
- Olaya müdahalede can güvenliğini ön plana alırlar.
- Olayla ilgili gelen ekiplerin talimatına göre görevine devam ederler.
- Can kurtarma ve enkaz kaldırma çalışmalarına yardımcı olurlar.

C.32.1.4. Kurtarıcı:

- Acil durum ihbarı ile kurumun toplanma bölgesinde bulunur.
- Olay mahallinde önce can olmak üzere kurtarma çalışmaları yapar.
- Kurtarma çalışmalarına katılan diğer tüm insanlara kılavuzluk yapar.
- Olaya müdahale çalışmalarında görevli diğer tüm ekiplerle işbirliği halinde çalışır.

C.32.1.5. Koruyucu:

- Olay bölgesine lüzumsuz araç girişlerini önler.
- Çalışmalara katılmak üzere gelen yardımcı ekiplere yol gösterir.
- Görevlilerin dışındaki insanların olay mahalline girmelerine engel olur.
- Acil duruma müdahale çalışmalarında görevli diğer tüm ekiplerle işbirliği halinde çalışır.

C.32.1.6. İlkyardımcı:

- Acil durum ihbarına göre sağlık - ilkyardım malzemeleri ve sedye ile toplanma bölgesinde ilkyardıma hazır olur.
- İlkyardımı kurallarına göre çok seri ve dikkatli yapar.

C.32.2. Acil durum eylem planı oluşturulmalıdır.

C.32.3. Acil durum planlarının ihtiyaç olmaksızın test edilmesi gerekmektedir.

C.32.4. Acil durum eylem planı test programından elde edilen bulgular, prosedürlere, dokümantasyona ve bir sonraki eğitime dahil edilmelidir.

C.32.5. Olay Yönetimi (Acil Durum Planlaması) aşağıdaki prosedürleri içermelidir;

C.32.5.1. Olayın başka bir etkisi olmaması için kaynak sınırlandırılmalı veya ayrılmalıdır.

C.32.5.2. Olay ve önemi; açıklıklar ve sızılan kaynakların tespit ile belirlenmelidir.

C.32.5.3. Taktik olarak olaydan dolayı ortaya çıkan etkilerin neden olduğu (Organizasyon Öncelikler ve en uygun durum dikkate alınarak), zararın yayılması engellenmelidir.

C.32.5.4. Olayın tekrar gerçekleşmesinin önlenmesi öncelikli hedeftir(PUKÖ Modeline uygun olarak), ardından Düzeltici Eylemler gerçekleştirilebilir.

C.32.5.5. Düzeltici Eylemlerde iletişimin etkileneceği hesaba katılmalıdır.

C.32.5.6. Bilgi Güvenlik Yönetimine, dahili olarak olay hemen raporlanmalıdır.

C.32.6. Olayın belirlenmesi ve Düzenleyici Eylem Prosedürleri, Problemin kaynağı olabilecek tüm deliller, herhangi bir ihlalin meydana gelme olasılığına karşı toplanmalıdır.

C.32.7. Bilgi Güvenliği Yetkilisi, daha sonra ihtiyaç olabilecek kanıtlanabilir delillerin toplanması konusunda eğitilmiş olmalıdır.

C.33. Bilgi Güvenliği Ulaştırma Güvenliği Yönetimi

“Gizlilik” uygulamasının amacı, kamu kurum ve kuruluşlarının güvenliğini sağlamak, yürütülen işlemlerin ve muhafaza edilen her türlü gizlilik dereceli, bilgi, belge, evrak, doküman ve malzemelerin, düşman veya yetkili ve ilgili olmayan kimseler tarafından öğrenilmesine veya elde edilmesine engel olmaktır. Bu amaca ulaşmak için yapılan bütün düzenlemelere ve alınan bütün önlemlere” güvenlik tedbirleri” denir.

C.33.1. Taşınabilir materyaller üzerine iletilen verinin içeriği ile ilgili herhangi bir şey yazmamalıdır. Genel başlıklar kullanılmalıdır. Örneğin gizli evrakların bulunduğu bir cd üzerine “gizli evraklar” yazılmamalıdır.

C.33.2. İçinde veri bulunan taşınır materyal başka bir yere gönderiyorsa tutanak ile yetkili bir kişiye teslim edilmelidir.

C.33.3. Harici taşınabilir disklerin içi mekanik yapıya sahip olduğundan dolayı darbelere karşı çok hassastır. Bu nedenle kullanırken ve taşıırken dikkat edilmelidir. Örneğin özellikle hard diskler taşınırken koruyucu kılıflar içerisinde taşınmalıdır.

C.33.4. Çok gizli evraklar, torba veya çanta gibi kilitli muhafaza içinde ve “Çok Gizli” gizlilik dereceli güvenlik belgesi olan özel kurye ile gönderilirler. Eğer normal kargo ile gönderilmesi zorunlu ise, içerik uygun bir şekilde kript edilir (şifrelenir). Dışarıdan kargonun takip edilmemesi için kargo takip numarasının maskelenmesi yapılmalıdır.

C.33.5. Gizli evraklar veya cd, dvd, usb bellekler gönderilirken, iki adet zarf kullanılmalıdır. Birinci zarfın üzerine içeriğin niteliğine göre sınıflandırılmalı ve zarfın kapağı mühürlenmelidir. İkinci zarf ise normal adres yazılan zarf olmalıdır. “GİZLİ” yazılı olan zarf diğer normal zarfın içine koyulmalıdır.

C.34. Sosyal Mühendislik Zafiyetleri

Sosyal mühendislik, normalde insanların tanımadıkları birisi için yapmayacakları şeyleri yapmalarını sağlama sanatı olarak tanımlanmaktadır. Başka bir tanım ise; İnsanoğlunun zaaflarını kullanarak istediğiniz bilgiyi, veriyi elde etme sanatına sosyal mühendislik denir. Sosyal mühendisler teknolojiyi kullanarak ya da kullanmadan bilgi edinmek için insanların zaaflarından faydalanıp, en çok etkileme ve ikna yöntemlerini kullanırlar.

- C.34.1.** Taşıdığınız ve işlediğiniz verilerin öneminin bilincinde olunmalıdır.
- C.34.2.** Kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket edilmelidir.
- C.34.3.** Arkadaşlarınızla paylaştığınız bilgileri seçerken dikkat edilmelidir.
- C.34.4.** Özellikle telefonda, e-posta veya sohbet yoluyla yapılan haberleşmelerde şifre gibi özel bilgileriniz paylaşılmamalıdır.
- C.34.5.** Şifre kişiye özel bilgidir. Sistem yöneticiniz dahil telefonda veya e-posta ile şifrenizi paylaşmamalısınız. Sistem yöneticisi gerekli işlemi şifrenize ihtiyaç duymadan da yapabilmelidir.
- C.34.6.** Oluşturulan dosyaya erişecek kişiler ve hakları “bilmesi gereken” prensibine göre belirlenmelidir.
- C.34.7.** Erişecek kişilerin hakları yazma, okuma, değiştirme ve çalıştırma yetkileri göz önüne alınarak oluşturulmalıdır.
- C.34.8.** Verilen haklar belirli zamanlarda kontrol edilmeli, değişiklik gerekiyorsa yapılmalıdır.
- C.34.9.** Eğer paylaşımlar açılıyorsa ilgili dizine sadece gerekli haklar verilmelidir.
- C.34.10.** Kazaa, emule gibi dosya paylaşım yazılımları kullanılmamalıdır.

C.35. Sosyal Medya Güvenliği

- C.35.1.** Sosyal medya hesaplarına giriş için kullanılan şifreler ile kurum içinde kullanılan şifreler farklı olmalıdır.
- C.35.2.** Kurum içi bilgiler sosyal medyada paylaşılmamalıdır.
- C.35.3.** Kuruma ait hiçbir gizli bilgi, yazı sosyal medyada paylaşılmamalıdır.

C.36. Sistem Akreditasyonu

(2. versiyonda yazılacaktır)

C.37. Medikal Cihazlar Güvenliği

(2. versiyonda yazılacaktır)

D. KISALTMALAR

T.C. : Türkiye Cumhuriyeti

SB: Sağlık Bakanlığı

SBSGM: Sağlık Bilgi Sistemleri Genel Müdürlüğü

BG: Bilgi Güvenliği

BGYS: Bilgi Güvenliği Yönetim Sistemi

BT: Bilgi Teknolojileri

BSI: British Standards Institute, İngiliz Standartları Enstitüsü

ÇKYS: Çekirdek Kaynak Yönetimi Sistemi

DTVT: Devlet Teşkilatı Veri Tabanı

IEC: International Electrotechnical Commission, Uluslararası Elektroteknik Komisyonu

ISO: International Organization for Standardization, Uluslararası Standartlar Teşkilatı

PUKÖ: Planla-Uygula-Kontrol Et-Önlem Al

E. SÖZLÜK

Açılır Pencere Engelleyicisi (Popup Blocker): Açılır Pencere Engelleyicisi, istenmeyen çoğu açılan pencerenin görüntülenmesini engeller.

ADSL: Asimetrik Sayısal Abone Hattı anlamına gelen hızlı internet erişim teknolojisidir.

Ağ (Network): Ağ birbirine kablolarla veya kablosuz bağlanmış sunucu, yazıcı, bilgisayar, modem gibi birçok haberleşme cihazlarının en ekonomik ve verimli yoldan kullanılmasıdır.

Aldatmaca e-posta (Hoax): Elektronik posta adresi toplamak veya markaları karalamak için oluşturulan yalan haber (asparagas) içeren e-postalardır.

Anti virüs (Virüsten Korunma): Bilgisayarınızı ya da sisteminizi bilgisayar virüslerinden korumaya ve bilgisayar virüslerini temizlemeye yarayan yazılımdır.

Bağlantı Noktası (Port): Bir elektronik devreye, şebekeye veya sisteme giriş ve bağlantı noktasıdır.

Bilgisayar Korsanı (Hacker): Bilgisayar ve haberleşme teknolojileri konusunda bilgi sahibi olan, bilgisayar programlama alanında standardın üzerinde beceriye sahip bulunan ve böylece ileri düzeyde yazılımlar geliştiren ve onları kullanabilen kişidir. Amaçlarına göre farklı adlandırılırlar:

Siyah Şapkalılar: Her türlü programı, siteyi veya bilgisayarı güvenlik açıklarından yararlanarak kırabilen bu en bilindik hackerlar, sistemleri kullanılmaz hale getirir veya gizli bilgileri çalar. En zararlı hackerlar siyah şapkalılardır.

Beyaz Şapkalılar: Beyaz şapkalılar da her türlü programı, siteyi veya bilgisayarı güvenlik açıklarından yararlanarak kırabiliyor ancak kıldığı sistemin açıklarını

sistem yöneticisine bildirerek, o açıkların kapatılması ve zararlı kişilerden korunmasını sağlıyorlar.

Bilgisayar Solucanı (Computer Worm): Bilgisayar solucanı kendi kendini çoğaltabilen ve kendisini bir bilgisayardan diğerine kopyalamak için tasarlanmış kötücül (malware) yazılımdır. Bilgisayar virüsünden farkı bunu otomatik olarak yapmasıdır.

Bilgisayar Virüsü (Computer Virus): Veri girişi yoluyla bilgisayarlara yüklenen, sistemin veya programların bozulmasına, veri kaybına veya olağandışı çalışmasına neden olan yazılım.

Bilişim (Informatics): İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimi.

Bilmesi Gereken Prensibi (Need to Know Principle): Gizlilik dereceli bir ilgiyi, belgeyi, projeyi veya malzemeyi ancak görevi gereği öğrenme ve kullanma sorumluluğu olma ve uygun gizlilik dereceli Şahıs Güvenlik Derecesine sahip olma durumudur.

BIOS (Basic Input/Output System): Temel Giriş/Çıkış Sistemi, bilgisayarın ilk açılma işlevini yerine getiren yazılımdır.

Casus Yazılım (Spyware): Casus yazılım, en başta gelen bir kötücül yazılım (malware) türüdür. Casus yazılım, kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin, kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan yazılım olarak tanımlanır.

Disk Biçimlendirme (Disc Partitions): Diskinizi biçimlendirmek demek diskinizi farklı mantıksal disk bölümlerine ayırmak anlamına gelir.

Örneğin 80 GB alana sahip olan bir disk 30 GB işletim sistemi diski (C:\ sürücüsü) 50 GB kişisel dosyaları ve programları saklamak için arşiv diski (D:\ sürücüsü) olarak iki parçaya ayrılabilir. Hatta bilgisayar üzerine birden fazla işletim sistemi kurulacaksa arşiv diski 40 GB yapıp, 20'şer GB alan da iki işletim sistemi (Örneğin: pardus ve windows) için ayrılabilir.

EFS: Veri Şifreleme Sistemi anlamına gelen bir bilgisayar terimi kısaltmasıdır.

Ekran Koruyucusu (Screen Saver): Bilgisayarda monitörün uzun süre kullanılmadan açık kalması durumunda devreye giren, monitörün ömrünün azalmasını ve parola ile korunduğunda yetkisiz erişimi engelleyen yazılımdır.

Elektronik Sertifika (Electronic Certificate): Elektronik Sertifika, yani elektronik kimlik, sahibinin kişisel bilgilerini ve bu kişisel bilgilere ait açık anahtar bilgisini taşıyan ve taşıdığı açık anahtar bilgisinin, belirtilen kişi veya kuruma ait olduğunu garanti eden belgedir. Elektronik kimlik belgesi kişilere ait olabildiği gibi kurumlara veya web sunucularına ait olabilir.

Exe: Çalıştırılabilir dosya tiplerinin dosya uzantısıdır.

FTP: Dosya aktarım iletişim kuralı, (File Transfer Protocol; FTP), bir dosyayı ağ üzerindeki başka kullanıcıya o ağdaki bilgisayarda geçerli bir kullanıcı ismi ve şifresi ile yollamak için kullanılmaktadır.

Güvenlik Duvarı (Firewall): Güvenlik duvarı kurulduğu sisteme gelen ve giden ağ trafiğini kontrol ederek yetkisiz veya istenmeyen yollardan erişim sağlamasını engellemeye yarayan yazılım veya donanımdır.

Hata (Bug): Bir yazılım ya da donanımda var olan, meydana gelen hata, kod hatasıdır.

Hizmet Paketi (Service Pack): Piyasaya sürülen bilgisayar yazılımlarının, ortaya çıkan hata ve açıklıkların giderecek, varsa yeni özelliklerini ortaya çıkaracak yama tabir edilen programcıkların tek bir paket halinde toplandığı yazılımdır.

HDD: Sabit disk ya da Hard disk kısaca HDD ya da Türkçesi ile sabit disk sürücüsü veri depolanması amacı ile kullanılan manyetik kayıt ortamlarıdır. Önceleri büyük boyutları ve yüksek fiyatları nedeni ile sadece bilgisayar merkezlerinde kullanılan sabit diskler, cep telefonları ve sayısal fotoğraf makineleri içine sığabilecek kadar küçülen boyutları ile günlük hayatımıza girmişlerdir. Sabit disklerin en yoğun kullanım yeri bilgisayarlardır. Ses, görüntü, yazılımlar, veri tabanları gibi büyük miktarlarda bilgi, gerektiğinde kullanılmak üzere sabit disklerde saklanır.

HTTP : HTTP (Hypertext Transfer Protocol, Türkçe Hipermetin Aktarma İletişim Kuralı) bir kaynaktan dağıtılan ve ortak kullanıma açık olan hiper ortam bilgi sistemleri için uygulama seviyesinde bir iletişim kuralıdır.

HTTPs : HTTPS (Secure Hypertext Transfer Protocol, güvenli hipermetin aktarım iletişim kuralı) hipermetin aktarım iletişim kuralının (HTTP) güvenli ağ protokolü ile birleştirilmiş olanıdır. Klasik HTTP protokolüne SSL protokolünün eklenmesi ile elde edilir.

ICMP: Internet Kontrol Mesaj İletişim Kuralı, ICMP(Internet Control Message Protocol), hata mesajları ve TCP/IP yazılımının bir takım kendi mesaj trafiği amaçları için kullanılır. Kontrol amaçlı bir protokoldür.

IEEE: (Institute of Electrical and Electronics Engineers, Elektrik ve Elektronik Mühendisleri Enstitüsü) elektrik, elektronik, bilgisayar, otomasyon, telekomünikasyon ve diğer birçok alanda, mühendislik teori ve uygulamalarının gelişimi için çalışan, kar amacı olmayan, dünyanın önde gelen teknik organizasyonudur.

IEEE 802.1x: Bağlantı noktası tabanlı ağ erişim kontrolü için bir IEEE standartıdır. Bu, ağ protokolleri IEEE 802.1 grubunun bir parçasıdır. Bir LAN veya WLAN eklemek isteyen cihazlara kimlik doğrulama mekanizmasını sağlar.

İç Ağ (Intranet): Kuruluşların, kurumun veya herhangi bir grubun, bilgisayarları arasında güvenli bir şekilde bilgi paylaşması için oluşturulmuş büyük çaplı yerel ağ yapısıdır.

IP adresi: IP (Internet Protokol) adresi, interneti protokolünü kullanan diğer ağlara bağlı cihazların, ağ üzerinden birbirleri ile veri alışı verışı yapmak için kullandıkları adrestir.

İstenmeyen e-posta (Spam): Talep edilmeyen veya istenmeyen e-posta mesajıdır.

İşletim Sistemi (Operating System): İşletim sistemi, bilgisayar donanımının doğrudan denetimi ve yönetiminden, temel sistem işlemlerinden ve uygulama yazılımlarını çalıştırmaktan sorumlu olan sistem yazılımıdır.

Kırılmış (Crack): Ücretli yazılımları ücretsiz kullanmayı sağlayan, program kırıcıları (cracker) tarafından yazılmış programcıkları ve korsan yazılımları ifade eder.

Kriptoloji: Şifre bilimidir. Çeşitli iletilerin, yazıların belli bir sisteme göre şifrelenmesi, bu mesajların güvenli bir ortamda alıcıya iletilmesi ve iletilmiş

mesajın deşifresiyle uğraşır. Kriptoloji=Kriptografi + Kriptoanaliz Kriptoloji bilmi kendi içerisinde iki farklı branşa ayrılır. Kriptografi ; şifreleri yazmak ve Kriptoanaliz ;şifreleri çözmek ya da analiz etmekle ilgilenir.

Kriptografi: Gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür. Bu yöntemler, bir bilginin iletimi esnasında karşılaşılabilecek aktif ya da pasif ataklardan bilgiyi -dolayısıyla bilgi ile beraber bilginin göndericisi ve alıcısını da- koruma amacı güderler. Bir başka deyişle kriptografi, okunabilir durumdaki bir bilginin istenmeyen taraflarca okunamayacak bir hale dönüştürülmesinde kullanılan tekniklerin tümü olarak da gösterilir.

Korsan (Warez): Telif yasaları çiğnenerek ticareti yapılan telif hakkı saklı materyallere denir. Telifli ürünlerin kopyalanmasını, çoğaltılmasını ve dağıtımını yapan kişilere korsan, yapılan işe korsancılık denmektedir.

Kötücül Yazılım (Malware): Kötücül yazılım (malware: İngilizce "malicious software" in kısaltılmışı), bulaştığı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış yazılımların genel adıdır.

Linux: Unix'e fikirsel ve teknik anlamda atıfta bulunarak geliştirilmiş; açık kaynak kodlu, özgür ve ücretsiz bir işletim sistemi çekirdeğidir. Çekirdeğin kaynak kodları GNU Genel Kamu Lisansı çerçevesinde özgürce dağıtılabilir, değiştirilebilir ve kullanılabilir. Linux'un Unix ile herhangi bir kod ortaklığı bulunmamaktadır yani Linux'un kodları sıfırdan başlanılarak yazılmıştır.

MAC Adresi: MAC adresi (Media Access Control, yani Ortam Erişim Yönetimi) bir cihazın ağ donanımını tanımaya yarar, bir anlamda fiziksel adresidir.

Modem: Bilgisayarınızın telefon ya da internet hattına bağlanarak diğer bilgisayarla bağlantı kurmasına yarayan cihazdır.

NTFS: (New Technology File System; Yeni Teknoloji Dosya Sistemi), Windows NT'nin standart dosya sistemidir ve Windows 2000, Windows XP, Windows Server 2003 ve Windows Vista'da da standart olarak kullanılmıştır. Microsoft'un önceki FAT dosya sisteminin yeniden yapılandırılmasıyla oluşmuştur.

Olay Kayıtları (Event Logs): Bir işletim sisteminin tuttuğu kayıtları ifade eder. Olay günlüğü kayıtları, sorunları incelerken ve çözerken size önemli bilgiler sağlar.

Oltalama (Phishing): Yasal bir e-posta gibi görünen ve kişisel bilgilerinizi talep eden bir e-posta mesajıdır. İkna yöntemiyle gizli bilgilerin elde edilmesini amaçlayan bir sosyal mühendislik metodudur.

Otomatik Çalıştır (Autorun): Autorun, taşınabilir disklerin bilgisayara takıldığında istenilen programı veya programları otomatik olarak çalıştırması için kullanılan bir uygulamadır.

Paylaştırılmış Klasör (Shared Folder): Paylaştırılmış klasörler başkasının erişimine izin verdiğiniz ve çoğu zaman dosya paylaşmak amacıyla kullandığımız klasörlerdir.

Privilege: Ayrıcalık, imtiyaz, özel hak.

Rar: Bir dosya sıkıştırma ve arşivleme formatıdır. Eugene Roshal tarafından oluşturulmuş ve oluşturucusunun soyadını almıştır. RAR uzantılı dosyalar .rar şeklinde gözükür.

Robot (Bot): Bot, bilişim dünyasında "robot" anlamında kullanılan yaygın bir terimdir. Pek çok bilgisayar işlemini yarı-otomatik olarak yapabilen robotlar anlamında kullanılır.

TCP/IP: İnternet protokol takımı, İnternet'in çalışmasını sağlayan bir iletişim protokolleri bütünüdür. Bazen TCP/IP protokol takımı olarak da adlandırılır. TCP (Transmission Control Protocol) ve IP (Internet Protocol) ün kısaltmalarıdır.

Truva Atı (Trojan): Bilgisayar yazılımı bağlamında Truva atı zararlı program barındıran veya yükleyen programdır. Terim klasik Truva Atı mitinden türemiştir. Truva atları masum kullanıcıya kullanışlı veya ilginç programlar gibi görünebilir ancak çalıştırıldıklarında zararlıdır.

Tuş Kaydedici (Keylogger): Bilgisayarda yazılanları siz farkında olmadan kaydedebilen yazılım veya donanımlardır.

Sabit disk (Hard Disk): Sabit Disk ya da Hard disk kısaca HDD, veri depolanması amacı ile kullanılan manyetik kayıt ortamlarıdır.

SMS: (İngilizce Short Message Service; Kısa Mesaj Hizmeti), cep telefonu aracılığı ile yazılan mesajın bir cep telefonundan diğer bir cep telefonuna gönderilmesi, mesajlaşma hizmetidir.

SNMP: "Simple Network Management Protocol"ün kısaltması. "Basit Ağ Yönetimi Protokolü" adı verilen bu teknoloji, bilgisayar ağları büyüdükçe bu ağlar üzerindeki birimleri denetlemek amacıyla tasarlanmıştır.

SSH: (Secure Shell) güvenli veri iletimi için kriptografik ağ protokolüdür. Ssh ile ağa bağlı olan iki bilgisayar arasında veri aktarımı güvenlik kanalı üzerinden güvensiz bir ağda yapılır. Bu durumda ağda Ssh ile haberleşen makinelerden biri ssh sunucusu diğeri ssh istemcisi olur. Ssh kabuk hesabına erişim için Unix ve benzeri işletim sistemlerinde protokolün en iyi uygulaması olarak bilinir, ama aynı zamanda Windows üzerindeki hesaplara erişim için de kullanılabilir. SSH uzaktaki makineye bağlanıp kimlik kanıtlaması yapmak için açık anahtarlı şifrelemeyi kullanır ve bu sayede kullanıcıya sistemi kullanmasına izin vermiş olur.

SSL: Secure Socket Layer (Türkçe'ye Güvenli Yuva Katmanı olarak çevrilebilir) protokolü, internet üzerinden şifrelenmiş güvenli veri iletişimi sağlar.

Sunucu: (İngilizce: Server), bilgisayar ağlarında, diğer ağ bileşenlerinin (kullanıcıların) erişebileceği, kullanımına ve/veya paylaşımına açık kaynakları barındıran bilgisayar birimi. Bir ağda birden fazla sunucu birim bulunabilir. Karşıtı istemci (İngilizce: Client) dir.

USB Bellek (USB Flash): Kapasiteleri 256 GB'a kadar ulaşabilen, küçük, hafif, çalışma esnasında sökülüp takılabilir ve taşınabilir veri depolama aygıtlarıdır.

Virüs Tespit Ajanı (Antivirus Agent): Bilgisayarınızı zararlı programlardan korumak için virüsten korunma yazılımının virüsleri tespit eden yazılım parçasıdır.

WEP: WEP (Wired Equivalent Privacy), kablolu ağ bağlantılarında veri bağ tabakasında çalışan şifreleme yöntemidir. Kabloya Eşdeğer Mahremiyet (KEM) olarak Türkçe'ye çevrilebilir.

Wi-fi: Wi-fi: "Wireles Fidelity" kelimelerinin kısaltması olup kablosuz bađlılık veya kablosuz bađlantı anlamına gelir.

WPA: WPA (Wi-Fi Protected Access)Wi-Fi korumalı Eriřim olarak adlandırılır. WEP řifreleme sisteminden daha güvenli olduđu söylenen ve WEP řifrelemeden daha yeni bir teknolojidir.

Yazılım Yaması (Software Patch): Yazılımlarda oluřan bir hatayı ya da programın içeriđindeki hatalı bir fonksiyonu düzelten bir programcıdır.

Zip: (dosya formatı), bir popüler veri sıkıřtırma ve arřivleme formatıdır. ZIP uzantılı dosyalar ".zip" řeklinde gözükür.

Zombi Bilgisayar (Zombie): Zombi bilgisayar, (genelde yalnızca zombi olarak kısaltılır) genel ađa (internet) bađlı, bir kırıcı (hacker) tarafından bilgisayar virüsü veya truva atı ile tehlikeye atılmış bilgisayardır.

F. KAYNAKLAR

1. Sağlık Bilgi Sistemleri Genel Müdürlüğü
2. TUBİTAK-BİLGEM
3. <http://www.bilgiguvenligi.gov.tr/kilavuz-dokumanlar/index.php>
4. www.bilgimikoruyorum.org.tr
5. <http://www.bilgiguvenligi.gov.tr/kurumsal-guvenlik/veri-merkezlerinin-sahip-olmasi-gereken-ozellikler.html>
6. Dr. İzzet Gökhan Özbilgin,
<http://www.bilgiguvenligi.gov.tr/yazilim-guvenligi/yazilim-gelistirme-surecleri-ve-iso-27001-bilgi-guvenligi-yonetim-sistemi.html>
7. http://ocw.metu.edu.tr/pluginfile.php/2629/mod_resource/content/0/chaptervitr/003-5.htm
8. <http://www.sans.org/critical-security-controls/control.php?id=3>
9. Ali Dinçkan, Veri Yedekleme Kılavuzu, TUBİTAK-BİLGEM
10. Ömer Faruk Acar, TÜBİTAK BİLGEM
11. <http://mikailnazli.blogspot.com/2010/01/bilgi-guvenligi.html>
12. <http://web.ogm.gov.tr/birimler/merkez/bilgiislem/Dokumanlar/Forms/AllItems.aspx?RootFolder=http%3a%2f%2fweb%2eogm%2egov%2etr%2fbirimler%2fmerkez%2fbilgiislem%2fDokumanlar%2fBilgiGuvenligi&FolderCTID=0x0120003CFBD24EFB3DA6479A64B187A54853D4>
13. <http://bigb.meb.gov.tr>
14. <http://www.bilgiguvenligi.gov.tr/kurumsal-guvenlik/veri-merkezlerinin-sahip-olmasi-gereken-ozellikler.html>
15. Cumali Yüksek, Sağlık Bakanlığı
16. TUBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, BGYS Risk Yönetim Süreci,2007
17. tr.wikipedia.org
18. <http://edirnebarosu.org.tr/incelemler/adli-bilisim-computer-forensic/>
19. Neşe SAYARI, Türkiye Bilişim Derneği, Bilgi Güvenliği ve Yönetimi
20. Gürkan Özocak, Ceza Muhakemesinde Elektronik Delillerin Tespiti ve Toplanması
21. www.itgovernance.co.uk/files/Infosec_101v1.1.pdf (Information Security and ISO27001 – An Introduction)

22. www.niser.org.my/isms/docs/publications/information_security_management_committee (The Importance of Setting up an Information Security Management Committee in Organization)
23. <http://www.isms.jipdec.jp/en/isms/frame.html> (How to Establish an ISMS Management Framework)

G. YARARLI BAĞLANTILAR

1. <http://www.bilgiguvenligi.gov.tr/son-kullanici-guvenligi-dokumanlari/index.php>
2. <http://www.bilgiguvenligi.gov.tr/bilgi-guvenligi-yonetimi-dokumanlari/index.php>
3. <http://www.bilgiguvenligi.gov.tr/web-guvenligi-dokumanlari/index.php>
4. <http://www.bilgiguvenligi.gov.tr/veritabani-guvenligi-dokumanlari/index.php>
5. <http://www.bilgiguvenligi.gov.tr/microsoft-sistemleri-guvenligi-dokumanlari/index.php>
6. <http://www.bilgiguvenligi.gov.tr/kablosuz-ag-guvenligi/index.php>
7. http://www.bilgimikoruyorum.org.tr/?b110_neden-bilgi-guvenligi
8. http://www.bilgimikoruyorum.org.tr/?b320_sosyal_muhendislik
9. <http://www.bilgiguvenligi.gov.tr/sinir-guvenligi-dokumanlari/index.php>
10. <http://bilgiguvenligi.saglik.gov.tr/Home/Videolar>
11. <http://www.bilgiguvenligi.gov.tr/unix-sistemleri-guvenligi-dokumanlari/index.php>
12. <http://www.bilgiguvenligi.gov.tr/ortak-kriterler-standardi/index.php>
13. <http://www.bilgiguvenligi.gov.tr/sozluk/>

H. KATKIDA BULUNANLAR

Cumali YÜKSEK
Av. Gürbüz YÜKSEL
Dr. M. Mahir ÜLGÜ
Dr. M. İkbāl GÜLTEKİN
Dr. Ünal HÜLÜR
Şimşek MERT
Mustafa ASLAN
Burak AKBULUT
Faruk ÇALIKUŞU
Dilek KARAKAYA
Merve AKÇEŞME
Salim CİMİLLİ
Gamze CİMİLLİ
Emrah EROĞLU
Serkan ATAGÜN
Salih BAÇ
Ergin ÇELİK
Şemsettin COŞKUN
Seydi HİTAY
Mehmet Serkan ORHAN
M. Fatih ULUÇAM
Tamer ERDOĞAN
Büşra YÜKSEL
Tuncay KARAMAN
Gökhan ANALI
Özkan KAYMAK
Alparslan ÖZTÜRK
Barış KAYADELEN
Kaan KALAYCI
Can Özgür ÖZYARDIMCI
Bünyamin KUZU
Mehmet KOÇAKOĞLU
Bayram ERDEMİR
Selcen ŞAHİN
Serkan NARLI

İ. İLETİŞİM

T.C.

Sađlık Bakanlığı

Sađlık Bilgi Sistemleri Genel M¼d¼rl¼đ¼

Bilgi G¼venliđi Birimi

<http://bilgiguvenligi.saglik.gov.tr/>

bgkilavuzu@saglik.gov.tr

Cumali Y¼KSEK

Mustafa ASLAN

Tel : 0(312)585 2433-5851122