FEN BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ PROGRAMI

KURUMSAL BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ UYGULAMASI;VAKIF ÜNİVERSİTESİ ÖRNEĞİ

EMRE DEMİROK

tarafından

YÜKSEK LİSANS

derecesi şartını sağlamak için hazırlanmıştır.

HAZİRAN 2016

Program: BİLİŞİM SİSTEMLERİ

i

KURUMSAL BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ UYGULAMASI;VAKIF ÜNİVERSİTESİ ÖRNEĞİ

EMRE DEMİROK

OKAN ÜNİVERSİTESİ

Bilişim Sistemleri Programı'na

Yüksek Lisans

derecesi şartını sağlamak için sunulmuştur.

Onaylayan:

Prof. Dr. Ahmet Faik KAŞLI
Danışman

Prof. Dr.Ahmet Mesut RAZBONYALI
Üye

Yrd. Doç. Dr. Nevin KARAARSLAN BALIKÇI
2 nci Danışman

Yrd. Doç. Dr. Nurşen TOPÇUBAŞI
Üye

Yrd. Doç. Dr. Fazlı YILDIRIM
Üye

HAZİRAN 2016

Program: BİLİŞİM SİSTEMLERİ

ÖZET

Günümüzde, bilişim sistemleri hayatımızın her alanında vazgeçilmezdir. Tüm kişisel ve kurumsal bilgiler bilişim sistemleri üzerinde bulunmakta ve bir çoğuna internet aracılığıyla erişilebilmektedir. Bilişim sistemlerinin güvenliğinin sağlanması sistemlerin kesintisiz, sorunsuz ve veri kaybı olmadan kullanılabilmesi için önemlidir. Bilgi güvenliği konusunda yeterince tedbir alınamadığı veya farkındalık yaratılamadığı için günümüzde şahıslar, şirketler ve kurumlar siber saldırılar veya farklı yöntemlerle bilgi hırsızlığına maruz kalarak veya sistemlerinde hizmet aksaklıkları yaşayarak maddi veya itibari kayıplar yaşamaktadırlar. İstatiksel araştırmalarda bilgi güvenliği ihlalleri ve kayıp miktarlarının büyük oranlarda meydana geldiği bildirilmektedir.

Bu çalışmadaki amaç, ISO/IEC 27001:2013 bilgi güvenliği yönetim sistemi standartının kontrol hedeflerini, bilgi güvenliği ihlallerine neden olan zafiyet ve tehditlerini, detaylı bir şekilde açıklayarak, bilgi güvenliği yönetim sistemini kurmak isteyen kurumların herhangi danışman hizmeti almadan bu sistemi kurabilmeleri için danışabilecekleri bir kaynak ve bir vakıf üniversitesindeki tüm bilgi varlıkları envanterini kapsayan örnek risk analizi çalışması sunmaktır.

Anahtar Kelimeler: Bilgi güvenliği, ISO/IEC 27001:2013 BGYS (Bilgi Güvenliği Yönetim Sistemi), BGYS, Risk Analizi

ABSTRACT

Nowadays, information systems are indispensable in every area of our lives. All individual ve institutional informations exist in information system and most of them are accessible through internet. Providing security of the information systems is important to be able to use them uninterrupted, troubleless and without data losing. Because of not to be sufficiently taken precauitons or raised awareness about information security, in the present days, individuals, companies and foundations get losses of financial and reputation by being exposed to informaiton theft or getting loss of service in their systems through cyber attcks or different methods. In the statistical researchs, it is stated that Information security incidents and loss amounts take place in large measures.

The aim of the this article is to present a resource to institutions wanting to establish ISMS without taking consultancy service and a risk analysis study including all information assets in one foundation university by explaning vulnerabilities and threats causing information security incidents, requirements of control objectives of ISO/IEC 27001:2013 ISMS standard in detail.

.

Keywords: Information Security, ISO/IEC 27001:2013 ISMS (Information Security Management System), ISMS, Risk Analysis

TEŞEKKÜR

Bu çalışmanın oluşturulması sürecinde desteklerini esirgemeyen danışman hocalarım Sayın Prof.Dr Ahmet KAŞLI ve Sayın Yrd. Doç. Dr. Nevin KARAARSLAN BALIKÇI'ya, sabır ve anlayışından dolayı eşim Aysun DEMİROK'a teşekkürü bir borç bilirim.

İÇİNDEKİLER

TABLO LİSTESİ

ŞEKİL LİSTESİ

KISALTMALAR

BG : Bilgi Güvenliği

BGYS : Bilgi Güvenliği Yönetim Sistemi

BGRY : Bilgi Güvenliği Risk Yönetimi

BT : Bilgi Teknolojileri

PUKÖ : Planla, Uygula, Kontrol Et, Önlem Al

COBIT : Control Objectives for Information Technologies

DES : Digital Encryption Standart

DoS : Hizmet reddi saldırısı, Denial of Service

DMZ : DeMilitarized Zone (Askerden ArındırılmıĞ Bölge)

DPT : T.C. BaĞbakanlık Devlet Planlama TeĞkilatı

ECB : Electronic Codebook HTTP : HyperText Transport Protocol)

FMEA: Failure Mode and Effects Analysis(Olası Hata Türü Ve Etkileri Analizi)

ISACA : Information Systems Audit and Control Association

ISO : Uluslararası Standartlar Örgütü

ITGI : Information Technologies Governance Institude

ITSEC : Information Technology Security Evaluation Criteria

ITIL : Information Technology Infrastructure Library-BT Altyapı Kütüphanesi

LLC : Logical Link Control KPS : Kimlik PaylaĞımı Sistemi xi

MAC : Media Access Control

MERNİS : Merkezi Nüfus İdaresi

NetBEUI : NetBIOS Extended User Interface

PIN : Personal Identification Number- Kişisel Tanımlama Sayısı

UEKAE : Tübitak Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

UYAP : Ulusal Yargı Ağı projesinde

VPN : Virtual Private Network, Sanal Özel Ağ

YTCK : Yeni Türk Ceza Kanunu

I. GİRİŞ

Yaşadığımız yüzyılda bilgisayar teknolojisinin gelişimi ile bilginin erişilmesi ve aktarılması çok hızlı ve basit bir şekilde yapılabilmekte ve fiziki olarak çok küçük cihazlardaki dijital alanlarda milyonlarca bilgi kaydedilebilmektedir. Bilgilerin dijital ortamlarda depolanması, erişime açılması, taşınması birçok güvenlik zafiyetlerini de beraberinde getirmektedir. İnternet ortamında bir çok yöntem (virüsler, kurtçuklar, truva atları, ajan yazılım (spyware), hizmeti durduran saldırılar (DOS, DDOS), kimlik çalma) kullanılarak keşfedilen güvenlik açıkları ile kurum, firma ve şahıslar büyük miktarlarda çok önemli bilgilerini çaldırarak veya sistemlerinde hizmet kayıpları yaşayarak maddi ve itibari zarara uğramaktadırlar. Bu tip olaylar iç ve dış paydaşlarda güvensizlik duygusu oluşturduğundan, beraberinde geri kazanılması çok güç olan pazar, müşteri emek ve para kayıplarını getirmektedir.

İnternet ortamından bilgi, belge, kimlik bilgisi ve hatta para hırsızlığı günümüzde çok fazla duyduğumuz bir durumdur. FBI'a bağlı IC3 (Internet Crime Complaint Center) tarafından yayınlanan 2013 Şikayetler Raporu Şekil 1.1. de yıllara göre internet üzerinden maddi zarara uğrayan kişilerin açtığı şikayetlerin sayısını göstermektedir.

[1] Method of evaluating loss amounts: FBI IC3 Unit staff reviewed for validity all complaints that reported a loss of more than $100,000. Analysts also converted losses reported in foreign currencies to U.S. dollars. The final amounts of all reported losses above $100,000 for which the complaint information did not support the loss amount were excluded from the statistics.

Şekil 1.1. (FBI IC3, 2013)[1]

Şekil 1.2. de Symantec şirketi tarafından yapılan araştırmaya göre düzenlenen 2013 yılında gerçekleşen güvenlik ihlal olayları ve çalınan kimlik bilgilerinin grafiği sunulmuştur.

Şekil 1.2. (Symantec, 2013)[2]

[1] FBI IC3. (2013, 10 10). *2013_IC3Report.* 12 09, 2014 tarihinde The Internet Crime Complaint Center: ttp://www.ic3.gov/media/annualreport/2013_IC3Report.pdf adresinden alındı

[2] Symantec. (2013, 04 01). *Archived Publications.* 12 09, 2014 tarihinde Symantec Enterprise:http://www.symantec.com/security_response/publications/archives.jsp adresinden alındı

Ayrıca, iç paydaşlardaki küskünler, casuslar, bilgi güvenliği konusunda bilinçsiz personel, çalışma, arşiv ve bilgi sistem odalarına erişim kontrolünün yetersiz olması, yedeklerin eksik olması, iş sürekliliği planının olmaması veya yetersiz olması, kurum iletişim sistemlerinde güvenliğin sağlanmaması gibi konular bilgi güvenliğinin sağlanmasında zafiyet olarak değerlendirilip, tedbir alınması gereken hususlardan birkaçıdır.

Hem internet ortamındaki gün geçtikçe artan siber saldırılar, hem de kurum içi iş süreçlerinde bilgi güvenliği politikalarının uygulanmaması bilginin gizliliği, bütünlüğü ve erişilebilirliğinde büyük tehditler oluşturmaktadır. Sadece güvenlik cihazları veya sadece alınan bir kaç güvenlik kontrolü ile bu tehditlerin önüne geçip bilgi güvenliğini sağlamak mümkün değildir. Bilgi güvenliğini sistemini her açıdan değerlendirilmiş kapsamlı ve canlı bir süreç şeklinde oluşturabilmek gerekir. Bu konuda önde gelen uluslararası standart olan ISO/IEC 27001 BGYS standardı detaylı hazırlanmış bir kılavuz olarak başvurabileceğimiz kaynaktır.

Türkiye'de ISO:27001 Bilgi Güvenliği Yönetim Sistemi belgesi sadece bir devlet ve bir vakıf üniversitesi tarafından alınmıştır. ULAKBİM tarafından yapılan etkinlik ve konferanslarda üniversitelerin BGYS sistemlerini kurup işletmesinin önemli olduğu belirtilmektedir. BGYS belgesini İlk alan üniversite Okan Üniversitesi'dir. Okan Üniversitesi yaklaşık 1.500'ü aşkın personeli ile dört ayrı kampüste 20.000'den fazla

öğrenciye eğitim-öğretim hizmeti sunmaktadır. Web, e-posta, yazılım yönetimi ve geliştirilmesi, dosya sunucu yönetimi, yazıcı sistemi, bilgisayar laboratuarları,

kablolu ve kablosuz ağ sistemleri, kamera ve turnike geçiş sistemleri, kampüs alışveriş sistemleri gibi bir çok hizmetleri sunan büyük bir bilgi işlem ağ alt yapısına sahiptir. Bu alt yapının kontrollü, kesintisiz ve güvenli işletilebilmesi ISO:27001 BGYS standartı gereklilikleri ile büyük ölçüde sağlamıştır.

II. KAVRAMSAL ÇERÇEVE

2.1. Bilgi

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 (ÖNEL, 2007). Bilgi tanımını detaylandırmadan önce aşağıda veri ve enformasyon kavramlarını da inceleyelim.

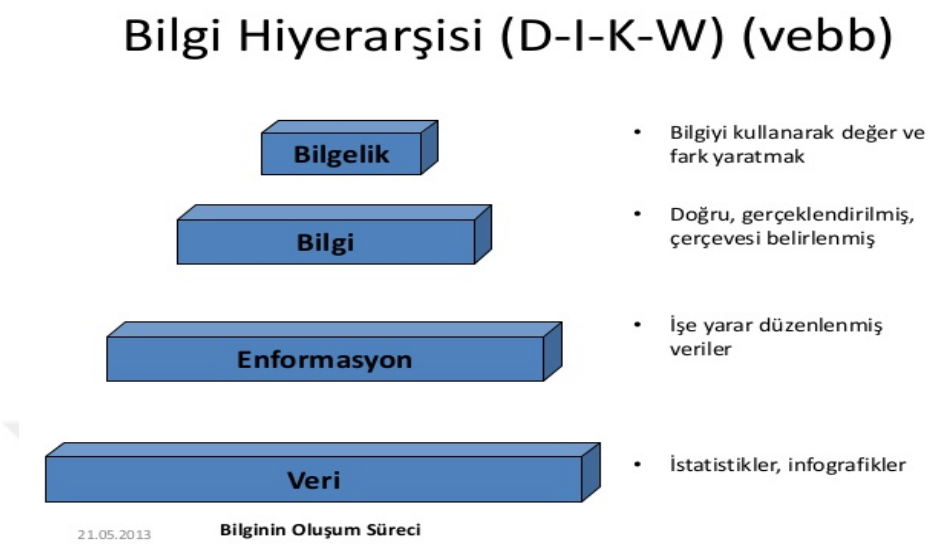
Veri; Veri, bir anlamı olan ve kaydedilebilen gerçekler. (Bir kişinin ismi, adresi, telefon numarası, vs.) .Veri, olguların, kavramların veya talimatların, insan tarafından veya otomatik yolla, iletişim, yorumlama ve işleme amacına uygun bir biçimde ifadesidir(ANSI Tanımı) (KALAY, 2014). Veriler ham, işlenmemiş, düzenlenmemiş, ilişkilendirilmemiş, hemen anlam verilemeyen sembol, harf, rakam, işaret ve izlenimlerdir (Öğüt, 2001).Veri enformasyonun temel hammadesidir.

Enformasyon; Enformasyon bir mesajdır, genellikle belge şeklinde ya da görsel ve işitsel iletişim mesajıdır. Her mesajda olduğu gibi enformasyonda da bir verici ve bir de alıcı vardır. Enformasyonun amacı, alıcının bir konudaki algılama şeklini değiştirmek, karar ya da davranışı üzerinde bir etki yaratmaktır. Enformasyon alıcısını biçimlendirmek zorundadır ve onun bakış açısında ya da anlayışında bir fark yaratmalıdır. Bu bağlamda enformasyon fark yaratan veridir. Veri çeşitli yollarla

(bağlama yerleştirmek (amaca yöneltmek), sınıflandırmak, hesaplamak, düzelrmek, özetlemek) anlamlar ve değerler eklenip ilişkilendirilerek enformasyona dönüştürülür (Thomas H. Davenport, 2013). Enformasyon organize edilmiş, düzenlenmiş veridir.

Bilgi; Enformasyon veriden türediği gibi bilgi de enformasyondan türer. Bu türeme 4 C kelimeleri (comparison, consequences, connection, conversation) aracılığıyla meydana gelir. Bilgi, tecrübe, değerler, bağlamsal enformasyon, yeni deneyim ve enfrormasyonu değerlendirmek ve birleştirmek için bir iskelet sağlayan uzman kavrayışdan oluşan akışkan karışımdır (Thomas H. Davenport, 2013). Bilgi yorumlanarak işe yarar hale getirilmiş ve anlamlandırılmış enformasyondur.

Şekil 2.1. de bilgi oluşum evreleri ve veri, enformasyon ve bilgiyi tanımlayan bilgi hiyerarşisi piramiti sunulmuştur. Bilgi hiyerarşisi kendi içinde veri, enformasyon, bilgi ve akıl şeklinde sıralanırken teknik ve bilişsel eylemler de; toplama, düzenleme, özetleme, analiz, sentez ve karar alma şeklinde sıralanmaktadır. Veriden akla kadar geçen süreçte zihinsel bir takım faaliyetler sürmektedir. Bu süreçte elde edilen veriler toplanmakta, düzenlenmekte ve anlamlı bir topluluk haline getirilmektedir. Sonrasında özetlenerek analiz edilmekte ve sentezlenerek bilgi haline gelmektedir. Son olarak bilgi haline gelen enformasyon karar alma aşamasını tamamlayarak akıl haline dönüşmektedir. (BoteLab, 2014)



Şekil 2.1. Bilgi Hiyerarşisi (Saba, 2013)[3]

2.2 Bilgi Teknolojileri

Bilginin toplanmasını, işlenmesini, saklanmasını, herhangi bir yere iletilmesini herhangi bir yerden erişilmesini sağlayan iletişim ve bilgisayar teknolojileri "bilişim teknolojisi" olarak adlandırılmaktadır. (UZAY, 2001)

Günümüzde bilgi teknolojileri bilimin her alanında, kurumlarda, hastanelerde, okullarda, bankalarda, ulaşımda, evlerde vazgeçilmez bir ihtiyaç ve ülkelerin askeri ve ekonomik gelişimlerinde rekabet aracı olmuştur.

Bilgi teknolojileri sayesinde ihtiyacımız olan bilgilere her zaman her yerden erişilebilmektedir, hızlı bir şekilde dünyanın her yerine sesli, görüntülü ve yazılı iletişim kurulabilmektedir.

[3] Saba, G. (2013, 5 21). Retrieved 10 31, 2015, from SlideShare: http://www.slideshare.net/GamzeSaba/knowledge-management-24307129

Bilgi teknolojileri üretim maliyetlerini, kağıt kullanımını, fiziksel alan ihtiyacını azaltır, zamanın etkin kullanılmasını sağlar, verimliliği arttırır.

Bilişim teknolojileri ürünlerini ve kapsamını belirtmek adına bazı ürün örneklerini aşağıdaki başlıklarda kısaca belirmek isterim.

-**İletişim Ürünleri:** Sabit ve mobit telefon santalleri ve cihazları, telsizler,kablolu ve kablosuz sistemler, uydu sistemleri ,e-posta yazılımları ve sunucuları.

-Güvenlik Ürünleri: Biometric tanıma sistemleri, kameralar, turnikeler, alarm sistemeri

-Baskı Ürünleri: Yazıcı, fotokopi makinesi, çizici, üç boyutlu yazıcı, matbaa sistemleri

-Depolama Ürünleri: Disk, sunucu, CD&DVD , hafıza kartları,

-Bilgisayar Ağı Ürünleri: Switch, modem, router, access point,

-Tıp Alanında Ürünler: Tomografi ve röntgen cihazları, diş tedavi üniteleri, tahlil sistemleri,

-**Görsel ve İşitsel Basın Ürünleri:** Radyo, TV, Web, İnternet tv ve radyo

-**Yazılımlar:** Web ve masaüstü tabanlı programlar (hasta kayıt programı, market satış programı, depo takip programı vb.)

-**Askeri Alanda Ürünler:** Radar, silah ve gece görüş sistemleri.

-**Üretim Alanında Ürünler:** CNC tezgahlar, araba üretim hatları, robotlar

2.3. Bilgi Güvenliği

Bilgi, düşünerek, akıl yürüterek, gözlem yaparak ya da araştırarak keşfedilme ve geliştirilme, insan beynine, fiziki ya da dijital ortamlara kaydedilme, kullanılıp

değerlendirilme, çeşitli vasıtalarla aktarılma veya yok edilme özelliklerine sahip bir yaşam döngüsü içindedir. Bilginin yaşam döngüsü içindeki her aşamasında gizlilik, bütünlük ve yetkili erişilebilirliğinin sağlanması bilgi güvenliğinin üç temel prensibidir (ISO/IEC-27001, 2013). Bilgi güvenliği, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişim, kullanım, değiştirilme, ifşa edilme, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemek olarak tanımlanır ve "gizlilik", "bütünlük" ve "erişilebilirlik" olarak isimlendirilen üç temel unsurdan meydana gelir. Bu üç temel güvenlik öğesinden herhangi biri zarar görürse güvenlik zaafiyeti oluşur (PESEN, 2015).

Bilgi güvenliği en genel tanımıyla bilginin, üretim ve hizmet sürekliliği sağlamak, parasal kayıpları en aza indirmek üzere tehlike ve tehdit alanlarından korunmasıdır Günümüzde bilgiye sürekli erişimi sağlamak ve bu bilginin son kullanıcıya kadar bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden güvenli bir şekilde sunulması zorunluluk haline gelmiştir (BENSGHİR, 2011).

2.3.1. Bilgi Güvenliği Kavramları

ISO (International Organization for Standardization, Uluslararası Standartlar Örgütü), CISSP (Certified Information Security Systems Professional –Profosyonel Sertifikalı Bilgi Güvenliği Sistemleri) gibi uluslararası bilgi güvenliği kurumları kayaklarına göre de bilgi güvenliği genel olarak CIA (confidentiality, integrity, availability) gizlilik, bütünlük, erişilebilirlik, başlıkları altında incelenmektedir.

2.3.1.1. Gizlilik

İçerden ve dışardan sözel, fiziki (basılı doküman) ve elektronik ortamlardaki veriye yetkisiz kişiler tarafından erişilmesinin engellenmesidir.Gizliliğin sağlanması ve önem derecesi kuruma (askeri, banka, hastane) kişilere (avukat-müvekkil,psikiyatr-hasta) ya da bilginin önemine göre değişebilir.Bilgi ve belgeler ÇOK GİZLİ,GİZLİ, KİŞİYE ÖZEL, KURUMA YA DA HİZMETE ÖZEL, TASNİF DIŞI gibi örnek önem derecelerine göre tasnif edilebilmektedir. Kurumsal standartlar, kişi veya kurumlar arasında yapılan anlaşmalardaki gizlilik taahhüdü maddeleri ile gizliliğin korunması sağlanır.

Bilgi Güvenliğinde bilgi yerine para olduğunu düşünürsek, bir kişi kendisine ait paranın diğer kişiler tarafından harcanmasını istemez, aynı zamanda kendi rızası olmadan borç olarak alınması ya da kullanılmasının engellenmesi gerekmektedir (G.Watkins, 2008).

2.3.1.2. Bütünlük

Bütünlük bilginin her ortamda yok edilmeden, bozulmadan ve değişikliğe uğramadan, eksiksiz ve doğru bir şekilde muhafaza edilip hizmete sunulmasıdır. 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 (ÖNEL, 2007).

Bilgi varlıklarının bütünlüğünde bilinçli ya da bilinçsiz değişiklik veya bozulmalar olmaması için teknik ve idari tedbirler alınmalı ve kontrol edilmelidir.

2.3.1.3. Erişilebilirlik (Kullanılabilirlik)

Erişilebilirlik 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 (ÖNEL, 2007). Erişimlerin kim, ne zaman, nereye, işlem başlıkları altında kayıt altına alınması ve control edilmesi yaşanabilecek güvenlik olayı öncesinde erken teşhis sağlaması ve olay sonrasında geriye dönük takip yapılabilmesi açısından önemlidir.

2.3.2. Bilgi Güvenliği Türleri

Bilgi iletişim teknolojilerinde en kritik konu bilgi güvenliğidir**.** Fakat bu konu o kadar geniş ve derindir ki, kendi alt başlıkları arasında bile birçok ihtisas alanına bölünür. Securosis firması tarafından yapılan çalışma ile bilgi güvenliği türleri kategorileri ve alt başlıkları aşağıda sunulmuştur (PESEN, 2015).

2.3.2.1. Ağ Güvenliği (Network Security)

- İçerik Güvenliği (Content Security)
    - E-Posta
    - Web
- Çevresel Savunma (Perimeter Defense)
    - Firewall/VPN (Güvenlik Duvarı / Sanal Özel Ağ)

    - IPS (Saldırı Önleme Sistemi (Intrusion Prevention System))
    - UTM (Birleştirilmiş Tehdit Yönetimi (Unified Threat Management))
- NAC (Network Access Control)
- Wireless (Kablosuz)
- İzleme (Monitoring)
    - NBA/NAD
    - Adli (Forensics)
- Yönetilir Servisler (Managed Services)
    - İzleme (Monitoring)
    - Yönetim (Management)

2.3.2.2. Uç/Son Nokta/Kullanıcı Güvenliği (Endpoint Security)

- Uç/Son Nokta/Kullanıcı Savunması (Endpoint Defense)
    - Anti-Malware
    - Ana Bilgisayar Güvenlik Duvarı (Host Firewall)
    - Ana Bilgisayar Tabanlı Saldırı Önleme Sistemi (HIPS)
    - Uygulamalar İçin Beyaz Listeleme (Application Whitelisting)
- Disk Şifreleme (Disk Encryption)
- Cihaz Kontrolü (Device Control)
- Mobil Güvenlik (Mobile Security)
- Uzaktan Erişim / VPN (Remote Access / VPN)

2.3.2.3. Veri Güvenliği (Data Security)

- Veritabanı Güvenliği (Database Security)
    - Veritabanı Değerlendirme (Database Assessment)
    - Veritabanı Aktivite Kontrolü/İzleme (Database Activity Monitoring)
    - Veritabanı Şifreleme (Database Encryption)
- Veri Kaybı/Sızıntısı Önleme (Data Loss Prevention)
    - DLP Çözümleri (DLP Solutions)
        - Tam Çözüm/Takım (Full Suite)
        - Ağ DLP (Network DLP)
        - Uç Nokta DLP (Endpoint DLP)
        - İçerik Keşfi (Content Discovery)
    - Veri Kaybı Önleme Özellikleri (DLP Features)
- Şifreleme (Encryption)
    - Dosya/Klasör (File/Folder)
        - Dağıtık Şifreleme (Distributed Encryption)
    - Anahtar Yönetimi (Key Management)
    - SAN/NAS
    - Uygulama Şifrelemesi (Application Encryption)
- Erişim Yönetimi (Access Management)
    - Yetki Verme Yönetimi (Entitlement Management)
    - Dosya Aktivitesi İzleme (File Activity Monitoring)

2.3.2.4. Uygulama Güvenliği (Application Security)

- Web Uygulama Güvenlik Duvarları (Web Application Firewalls)
- Uygulama Testi (Application Testing)
    - Dinamik Uygulama Testi (Dynamic Application Testing)
    - Statik Uygulama Testi (Static Application Testing)
- Güvenli Geliştirme (Secure Development)
    - Tehdit Modelleme (Threat Modeling)
    - Geliştirme Süreci (Development Process)
    - Test Metodolojileri (Testing Methodologies)
- Web Uygulama Değerlendirme (Web Application Assessment)
    - Web Güvenlik Açığı Değerlendirmesi (Web Vulnerability Assessment)
    - Web Penetrasyon Testi (Web Penetration Testing)
- Yönetilir Servisler (Managed Services)
    - Değerlendirme / Testler (Assessment / Testing)
    - Yönetilir Web Uygulama Güvenlik Duvarları (Managed Web Application Firewall (WAF))

2.3.2.5. Kimlik ve Erişim Yönetimi (Identity and Access Management)

- Dizinler (Directories)
- Kimlik Doğrulama (Authentication)
- Sağlama / Hazır Hale Getirme (Provisioning)
- Web Erişim Yönetimi (Web Access Management)
- Federation

2.3.2.6. Güvenlik Yönetimi (Security Management)

- Uyumluluk/Uygunluk
    - IT-GRC
    - PCI
    - SOX
    - HIPAA
    - NERC-CIP
    - Gizlilik/Mahremiyet (Privacy)
- Güvenlik Operasyonları (Security Operations)
    - Güvenlik Bilgi ve Olay Yönetimi (SIEM)
    - Log Yönetimi (Log Management)
- Sistem Yönetimi (System Management)
    - Yama Yönetimi (Patch Management)
    - Konfigürasyon Yönetimi (Configuration Management)
- Güvenlik Açığı Yönetimi (Vulnerability Management)
    - Güvenlik Açığı Değerlendirmesi (Vulnerability Assessment)
    - Penetrasyon Testi (Penetration Testing)
- Olay Müdahale (Incident Response)

2.3.2.7. Sanallaştırma ve Bulut (Virtualization and Cloud)

- Sanallaştırma Güvenliği (Virtualization Security)
    - Sanal Makine Güvenliği (Virtual Machine Security)

- Sanallaştırma Altyapı Güvenliği (Virtualization Infrastructure Security)

- Bulut Güvenliği (Cloud Security)
  - Bulut Güvenik Servisleri (Cloud Security Services)
  - Bulut Güçlendirme (Cloud Hardening)
  - Bulut Risk Yönetimi (Cloud Risk Management)

2.3.3 Bilgi Güvenliğini Tehdit Eden Unsurlar

Bilişim korsanları (hackerlar) kurum ve şahısların bilgisayar sistemlerine erişip bilgilerini kullanılamaz/erişilemez hale getirerek zarar verebilmekte ya da ele geçirdikleri bilgileri farklı amaçlarla kullanıp başkalarına ifşa etmektedirler.

Bilişim teknolojileri kullanılırken ortaya çıkan tehditlere karşı kurumsal ya da bireysel düzeyde önlemlerin alınması için ilgililere farkındalık eğitimlerinin verilmesi gerekmektedir.

Tehditler sistemler üzerindeki zafiyetler aracılığıyla etkin olmaktadır. Tehdit ve zafiyetin bir araya gelmesi riski oluşturur, tehdidin gerçekleşme olasılığı ile etki derecesi hesaplanarak riskin derecelendirmesi yapılır.Aşağıda örnek thedit listesi sunulmuştur, bu tehditler kurumların yapısına göre geliştirilebilir.

Örnek Tehdit Listesi (Bayraktaroğlu, 2008);

Yedekleme Medyalarında bozulma

Gizli Kanallardan Bilgi Sızdırılması

Kaza veya arızalardan oluşabilecek hasar

Kablo hasarları

Disipline edilmemiş aksiyonlar veya tehditin farkedilemesi

Hizmet kesintisi tehdidi

Ekipmanın tahrip edilmesi tehdidi

Gizli Bilginin Ortaya Çıkması

Şifreleme anahtarının ele geçirilmesi

Tozlanma, kirlenme

Çevresel kirlilikten (gürültü, haberleşme dahil) etkilenme

Çevresel felaketler

Yangın

Su taşması, su basması

Kötü niyetle istifade (Fraud)

Hardware arızası

Rutubet ve aşırı sıcaklık

Hatalı bilgi girişi

Bilginin sınıfılandırılması hatası

Yetersiz ve test edilmemiş veri yedekleri

Unutulmuş erişim hakları

Gizli dinleme

Fiziksel müdahele

Güç sağlayıcı, klima arızaları, elektiriksel anaomaliler

Kuruma ait bilgilerin özel amaçlarla kullanımı

İnternet ortamında bir çok yöntem (virüsler, kurtçuklar, truva atları, ajan yazılım (spyware), hizmeti durduran saldırılar (DOS, DDOS), kimlik çalma) kullanılarak keşfedilen güvenlik açıkları ile kurum, firma ve şahıslar büyük miktarlarda çok önemli bilgilerini çaldırarak veya sistemlerinde hizmet kayıpları yaşayarak maddi ve itibari zarara uğramaktadırlar.

Başlıca kullanılan yöntemler şunlardır;

Solucanlar (Worms)

Bağımsız şekilde çalışan, kendi kendine çoğalabilen, insan müdahelesi olmadan bilgisayar ağları aracılığıyla yayılan zararlı yazılımlardır.

Casus Yazılımlar (Spyware)

Kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin, kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan zararlı yazılım olarak tanımlanır. Kullanıcıların haberi olmadan sistemlere bulaşabilen casus yazılımlar, kişisel gizliliğe karşı gerçekleştirilen en önemli saldırılardan biridir.

Truva Atı

Truva atlarının iki türü vardır. Birincisi,kullanışlı bir programın bir hacker tarafından tahribata uğrayıp içine zararlı kodlar yüklenip program açıldığında yayılan cinsi. Örnek olarak çeşitli hava durumu uyarı programları, bilgisayar saati ayarlama yazılımları ve paylaşım programları (p2p) verilebilir. Diğer türü ise bağımsız bir program olup başka bir dosya gibi görünür. Örneklemek gerekirse oyun veya kalıp dosyası gibi kullanıcıyı aldatmaya yönelik bir takım yönlendirici karışıklık ile programın harekete geçirilmesine ihtiyaç duyulmaktadır (Vikipedi, 2015).

Hizmetin Engellenmesi Saldırıları (DDoS Distributed Denial of Service)

Hedeflenen kullanıcı veya kullanıcılara bir sunucu veya ağ sistemini kullanılamaz hale getirmek amacıyla yapılan saldırıdır.

Virüsler (Virus)

Kullanıcının bilgisi olmadan bir dosya ya da programın içinde gizli bir şekilde bulaşan çalıştığında bilgisayarın çalışma şeklini değiştiren, başka dokuman ya da programlara zarar veren, ağ üzerinden otomatik olarak yayılabilen zararlı programlardır.

Reklam Destekli Yazılımlar (Adware)

Kullanıcı bilgisayarlarında reklamlar görüntülemek,web arama isteklerini reklam web sitelerine yönlendirmek için ziyaret ettiğiniz web sitelerinin türleri gibi hakkınızdaki pazarlama verilerini toplamak amacıyla tasarlanmış izinli veya izinsiz olarak çalışan yazılımlara verilen addır. Casus yazılımların sistemlere bulaşma teknikleri kullanıcılar tarafından çok iyi bilinmelidir. Bilgi ve bilgisayar güvenliğini sağlamada en önemli tedbirlerin başında gelen, bilgisayar sisteminin, yama ve güncellemelerle sürekli güncel tutulması ve İnternet üzerinde bilinmeyen programların indirilip, çalıştırılmaması gibi önlemler casus yazılımlara karşı da korunma sağlayacaktır (Vikipedi, 2015).

Sazan Avlama (Phishing)

Kullanıcılara sahte e-posta ve link gönderip aldatarak kullanıcının kredi kartı numarasını, ATM Kart numarasını, CVV2 bilgisini, şifre ve parolalarınızı, hesap

numaralarınızı, internet bankacılığında kullanılan kullanıcı adı ve şifrelerininin ele geçirilmesini sağlayan dolandırıcılık yöntemidir.

2.3.4 Bilgi Güvenliği Yönetim Sistemleri

2.3.4.1 ITIL (*Information Technology Infrastructure Library*)

ITIL'I türkçe olarak "Bilişim teknolojileri altyapı kütüphanesi" olarak açıklayabiliriz. ITIL en iyi uygulamaların (best practices), deneyimlerin bir araya toplanması, getirilmesi ile oluşturulmuş bir kütüphanedir. ITIL büyük küçük tüm organizasyonlara göre ölçeklenebilen süreç merkezli bir yaklaşımı destekler.

Amaçları;

• Maliyetleri Düşürmek

• Erişilebilirliği Arttırmak

• Kapasiteyi Ayarlamak

• İş Gücünü Arttırmak

• Kaynakların Verimli Kullanılmasını Sağlamak

• Ölçeklebilirliği Arttırmak

• Yüksek Kalitede BT Hizmeti vermek

ITIL 1980 yılında İngiliz Hükümetinin Merkezi Bilgisayar ve Telekominikasyon Dairesi Başkanlığı'nı (Şimdiki adıyla The Office of Government Commerce OGC) kamu ve özel kurumlarda Bilgi Teknolojileri kaynaklarının etkin ve mali olarak sorumlu kullanımının sağlanması için bir sistem geliştirme görevi vermesi ile ortaya çıkmıştır (Central).

İlk ITIL kitabı olan Hizmet Seviyesi Yönetimi(Service Level Management) 1989 yılında yayımlanmıştır hemen ardından sırası ile Servis Masası, Süreç Yönetimi ve Değişiklik Yönetimi kitapları yayımlanmıştır.2001 yılında ITIL V2, 2007 yılında ITIL V3 sürümü yayınlanmıştır. Üçüncü Sürüm aşağıdaki 5 ana bölümden oluşur.

– Hizmet Stratejisi (Service Strategy)

– Hizmet Tasarımı (Service Design)

– Hizmet Geçişi (Service Transition)

– Hizmet Yönetimi (Service Operation)

– Sürekli Servis Gelişimi (Continual Service Improvement)

Hizmet Stratejisi (Service Strategy)

Servis Yönetiminin uygulanması,geliştirilmesi ve tasarlanması konusunda rehber niteliğindedir. Bu konuda BT Organizasyonlarının müşterilerine farklı hizmetler sunmasını ve operasyonel etkinliğini artırmasını amaçlar.

Service Design (Hizmet Tasarım)

Servis Tasarımı, iş gereksinimleri değişimi sürecinde önemli bir eleman ve Genel servis yaşam döngüsü içerisinde önemli bir katmandır.

Özelleştirilebilir ve Yenilikçi BT Hizmetleri tasarımı, süreçler, politikalar ve belgeler de dahil olmak üzere mevcutta kabul edilmiş ve gelecekteki iş gereksinimlerini karşılamak için oluşturulan mimarilerdir.

Başarılı bir tasarımın yapılabilmesi için 4P (People,Product,Processes, Partners) tasarımının doğru yapılmasına bağlıdır. (Oğraş, 2011)

Service Design Package (SDP);

Servis Yaşam döngüsünün her bir aşamasındaki gereklilikleri ve bir BT Servisinin bütün yönlerini tanımlar. Bir SDP, her yeni servis,

Service Transition (Hizmet Geçiş)

Hizmet geçiş rolü, Operasyonel süreçte kullanılmak üzere iş gerekliliklerini iletir. Hizmet geçişi, Servis tasarım aşamasından Hizmet tasarım paketini alması ile başlar ve Operasyonel aşamaya devam eden operasyon ve hizmet desteği için gerekli tüm bilgileri ve elemanaları teslim eder.

İş Koşulları, gereksinimleri yada varsayımlar tasarım sürecinden sonra değişime uğradıysa, Hizmet geçiş aşamasında gerekli hizmeti sunmak için bir takım değişiklikler gerekebilir. Unutulmaması gereken en önemli nokta Hizmet Geçişi sadece uygulamalarla ve/veya normal şartlar altında nasıl kullanıldığı ile değil hizmetlerin tüm yönleri ile uygulanmasından sorumludur. (Oğraş, 2011)

Service Operation (Hizmet Operasyon)

Hizmet Operasyonu, Kullanıcılarına ve Müşterilerine belirlenmiş hizmet seviyesini sağlayacak olan uygulama yönetimi, teknoloji ve altyapı hizmet desteği sunar.

Bu hizmetler sadece servis yaşam döngüsünün bu aşamasında işe gerçek değerini verir. Hizmet yaşam döngüsü, Hizmet operasyonu aşamasında, kabul edilen parametreler dahilinde faaliyet sağlamakla ilgilenir. Herhangi bir hizmet kesintisi meydana geldiğinde, Servis operasyonu olabildiğince çabuk şekilde servisleri geri yüklüyerek iş etkisini en aza indirger. (Oğraş, 2011)

"Reactive-Proactive", "Internal-External", "Cost-Quality", "Stability-Flexibility" arasında denge sağlamak durumundadır. Eğer bu dengeyi kuramazsa Hizmet Operasyonu kötü olarak görünüyor olucaktır.

En önemli kısımlardan biri ise operasyon esnasında olan iletişimdir ver her ne olursa olsun iletişimin doğru algılanması kurulması gerekir. Bu ilişkiler;

BT Hizmet sağlayıcı ile kullanıcı arasındaki iletişim.

BT Hizmet sağlayıcı ile Müşteri arasındaki iletişim.

BT Hizmet sağlayıcı içerisinde yer alan farklı süreçler, fonksiyonlar ve takımlar arasındaki iletişim.

BT Hizmet sağlayıcı ile tedarikçileri arasındaki iletişim.

Continual Service Improvement (Hizmet İyileştirme Sürekliliği)

Değişen iş ihtiyaçlarına göre fonksiyonların, süreçlerin ve hizmetlerin yeniden uyumlu hale getirilmesi sürecidir. Aynı zamanda Genel Hizmet yönetimi içerisindeki kalite yönetim yöntemleri uygulama tutarlığı ile ilgilenir.

ITIL içerisinde "**Ölçü (Measurement)**" kritik bir rol almaktadır. Hizmet iyileştirme sürekliliğinin bi parçası, aynı zamanda Hizmet seviyesi Yönetiminin ve tüm süreçlerin önemli bir parçasıdır.

Hizmet Seviyesi Yönetimi (SLM) aynı zamanda Servis Tasarım yaşam döngüsü aşamasının içerisindeki süreçlerden birisidir. Bir çok aktivite ve nesne Hizmet iyileştirme sürekliliği ile ortaktır. Özellikle her iki Hizmet seviyesi yönetimi ve iyileştirme sürekliliği düzenli ölçüm, servislerin gözden geçirilmesini ve servis yönetim başarımının diğer yönlerini vurgulamaktadır.

Service Improvement Program (SIP); Hizmet İyileştirme Planı yada Hizmet İyileştirme Programı, Hizmet iyileştirme sürekliliğinin bir parçası olarak yada Hizmet seviyesi yönetimi sürecinin bir parçası olarak yürütülen periyodik hizmet değerlendirmesinin birincil çıktısıdır. (Oğraş, 2011)

2.3.4.2 COBIT

Tanım olarak CobiT, "Control Objectives for Information and Related Technology" nin kısaltılmış halidir. Türkçe ifade etmek gerekirse "Bilgi ve ilgili teknoloji için kontrol hedefleri". Bu tanım, CobiT'in amacını ifade etmesi açısından önemlidir. CobiT, Bilgi Teknolojileri yönetiminde ulaşılması gereken **hedefleri** ortaya koymaktadır.

CobiT'i, ITIL, CMMI ve ISO standartlarından ayıran en büyük özelliği tüm BT fonksiyonlarını kapsayan bir çerçeve sunmasıdır. Farklı şekilde ifade etmek gerekirse CobiT içerisinde yer alan 34 süreci bir arada değerlendirdiğinizde BT yönetiminin her alanını kapsama almış olursunuz. Bu nedenle diğer standartlardan farklı şekilde, CobiT'in tek veya grup halinde BT süreçlerine değil BT'nin yönetilmesine odaklandığını söylemek doğru olur.

CobiT'in diğer bir özelliği de, içerisindeki süreçlerin nasıl uygulanması gerektiğine dair detaylı çözüm yöntemleri içermemesidir. Esas olarak kontrol hedeflerinden oluşmaktadır ve bu hedefler o süreç içerisinde sağlanması gereken en iyi uygulamaları açıklamaktadır. Fakat birkaç istisna dışında bu süreçlerin hiçbiri için kontrol hedeflerine ulaşılmasını sağlayacak bir yöntem, şablon veya tasarım önermemektedir. Örnek vermek gerekirse, DS5 Sistem Güvenliğinin

Sağlanması sürecinde sistemlere ve bilgiye erişen kişilerin kimliklerinden emin olunması gerektiği belirtilir. Ancak bunun yapılması için kullanılabilecek yöntemlerden (kullanıcı adı/şifre, biyometrik kimlik doğrulama, token, fiziksel sınırlama vb) bahsedilmez. Uygulama sırasında bu tür kontrol örneklerine ihtiyaç duyulabileceği göz önünde bulundurularak ISACA tarafından "CobiT Control Practices" adında CobiT'e ek bir kılavuz dokümanı yayınlanmıştır.

CobiT aşağıdaki genel özellikleri gösterir:

- Bilgi Teknolojileri'nin şirketin iş (ticari) amaçlarına hizmet etmesi gerektiğini benimser,
- BT stratejisi ile iş stratejisinin uyumunu sağlamaya çalışır,
- Bu özellikleriyle modern BT Yönetiminin kabul görmüş kurallarını içerir,
- İçerisindeki 34 süreç ile neredeyse tüm BT fonksiyonlarını kapsar,
- Diğer BT yönetimi standartları ile (ISO, ITIL, CMMI, MOF, vb) uyumludur,
- Her sektörden ve her boyuttaki şirket tarafından kullanılabilir,
- Denetim, süreç iyileştirme, süreç yönetimi, ölçüm, karşılaştırma vb farklı kullanım amaçları vardır.

CobiT içerisinde 4 ana başlık altında toplam 34 süreç bulunmaktadır. Yukarıda da belirttiğimiz gibi bu 34 süreç, pek çok şirket için BT fonksiyonlarının hemen hepsini kapsar. CobiT içerisinde aşağıdaki süreçler bulunmaktadır: (TUTU, COBIT Nedir, 2010)

Planlama ve Organizasyon

PO 1 Stratejik BT planının tanımlanması

PO 2 Bilgi mimarisinin tanımlanması

PO 3 Teknolojik yönün belirlenmesi

PO 4 BT süreçlerinin organizasyonunun ve ilişkilerinin tanımlanması

PO 5 BT yatırımlarının yönetimi

PO 6 Yönetimin amaçlarının iletilmesi

PO 7 BT İnsan kaynakları yönetimi

PO 8 BT Kalite yönetimi

PO 9 BT riskinin değerlendirilmesi ve yönetimi

PO 10 Proje yönetimi

Edinim ve Kurulum

AI 1 Çözümlerin belirlenmesi

AI 2 Uygulama yazılımının geliştirilmesi ve bakımı

AI 3 Teknoloji alt yapısının oluşturulması ve bakımı

AI 4 Operasyon ve kullanımın sağlanması

AI 5 BT kaynaklarının satın alınması

AI 6 Değişiklik yönetimi

AI 7 Çözümlerin ve değişikliklerin uygulanması ve akredite edilmesi

Hizmet ve Destek

DS 1 Hizmet seviyelerinin tanımlanması ve yönetimi

DS 2 Üçüncü kişilerden alınan hizmetlerin yönetimi

DS 3 Performans ve kapasite yönetimi

DS 4 Hizmet sürekliliğinin sağlanması

DS 5 Sistem güvenliğinin sağlanması

DS 6 Maliyetlerin belirlenmesi ve dağıtılması

DS 7 Kullanıcıların eğitimi

DS 8 Hizmet sunumu yönetimi ve olay yönetimi

DS 9 Konfigürasyon yönetimi

DS 10 Problem yönetimi

DS 11 Veri yönetimi

DS 12 Fiziksel çevre yönetimi

DS 13 Operasyon yönetimi

İzleme ve Değerlendirme

ME 1 Bilgi sistemleri performansının izlenmesi ve değerlendirilmesi

ME 2 İç kontrolün izlenmesi ve değerlendirilmesi

ME 3 Mevzuata uyumun sağlanması

ME 4 Bilgi sistemlerine ilişkin kurumsal yönetişimin temini

Detaylı kontrol hedefleri

Detaylı kontrol hedeflerinde sürecin işletilmesi ile ulaşılması gerekli hedefler yani iyi uygulamalar bulunmaktadır. Detaylı kontrol hedefleri, her süreç için farklı şekilde kategorilere göre ayrılmıştır. Bu bölüm ayrıca, CobiT esaslı denetimlerde uyulması gerekli bir kriter listesi olarak kullanılır. Benzer şekilde

CobiT uyumluluğunun sağlanması amacıyla gerçekleştirilen süreç iyileştirme çalışmalarının da dayanak noktası detaylı kontrol hedefleridir.

Örnek olarak "DS3 Performans ve Kapasite Yönetimi" süreci üzerinden ilerlemek istersek, içerisinde şu kategoriler altında, ulaşılması gerekli hedefler bulunmaktadır: (TUTU, 2010)

- DS3.1 Performans ve kapasite planlaması
- DS3.2 Mevcut kapasite ve performans
- DS3.3 Gelecekteki kapasite ve performans
- DS3.4 BT kaynaklarının erişilebilirliği
- DS3.5 İzleme ve raporlama

2.3.4.3 PCI DSS

Payment Card Industry (PCI) Veri Güvenliği Standardı (Data Security Standard)

PCI DSS, ödeme hesabı veri güvenliğini sağlamak için kapsamlı gereklilikler ve şartlar, PCI Güvenlik Standartları Konseyi'nin kurucu ödeme markalarından American Express, Discover Financial Services, JCB International, MasterCard Worldwide ve Visa Inc. Inc. International tarafından geliştirilmiştir.

PCI DSS programı, banka ve finans kurumları aracılığıyla gerçekleştirilen e-ticaret işlemlerinde sıkça rastlanan ve ciddi kayıplara yol açan kredi kartı yolsuzlukları ve kötüye kullanılan bilgilere karşı bir koruma sağlamayı hedeflemektedir. Bunu gerçekleştirebilmek için PCI DSS programı güvenlik süreçlerindeki, yönergelerdeki ve web sitesi konfigürasyonlarındaki zafiyetlerin tespit edilmesi ve giderilmesini öngörür. Bu programın asıl amacı kredi kartı hesap

verilerinin kredi kartı ile işlem yapan üye işyerleri ve finans kurumlarında, PCI DSS uyarınca güvenli bir şekilde saklanmasının sağlanmasıdır.

Internet üzerinden kredi kartı ile işlem yapan üye işyerleri ve finans kurumları PCI Veri Güvenliği Standardına uygunluklarını kanıtlamak ile yükümlüdürler. (PCI Güvenlik)

2.3.4.4 HIPAA

Kimlik hırsızlığı, dolandırıcılık ve hasta bilgilerinin kötüye kullanılma ihtimali olan bir dönemde 1996 tarihli Amerika'da çıkan **"Health Insurance Portability and Accountability Act (HIPAA)" (Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası)**, kişisel sağlık bilgilerinin özel ve hasta kontrolünde kalmasını sağlamayı amaçlamaktadır.

İnternet uygulamaları ya da elektronik sistemler vasıtasıyla, bireylerin korunmuş sağlık bilgilerini aktaran organizasyonlar, HIPAA standartlarının yükümlülüklerini yerine getirmek zorundadırlar. Bu organizasyonlar, ilaç mağazaları, eczaneler, kaza ve sağlık sigortaları, tıbbi hizmet planı veren şirketler, tıbbi cihaz satan ve kiralayan şirketler, bireysel hekim klinikleri, hastaneler vb gibi organizasyonlar olabilir. HIPAA, bireylerin korunmuş veya korunması gereken sağlık bilgilerini mahremiyete ve güvenliğe uygun olarak geliştirilen bir takım idari, fiziksel ve tekniksel ihtiyat standartlarıdır. (POŞUL, 2010)

2.3.4.5 ISO 27001 Bilgi Güvenliği Yönetim Sistemi

İngiltere de BSI (İngiliz Standartlar Enstitüsü) tarafından Bilgi Güvenliği Standartları BS7799-1 altında ortaya çıkmış, 1995 yılında BS7799 olarak yayınlanan standart daha sonra BS7799-2:1999 olarak yayınlanmıştır.

Uluslararası Standartlar Komitesi (ISO) ise Bilgi Güvenliği ile ilgili standardın birinci bölümünü 2000 yılında ISO/IEC 17799 olarak yayınlamıştır.

Bilgi Güvenliği Yönetimi İçin Uygulama Prensiplerini ve kontrol listelerini içeren standart 15 Ekim 2005 tarihinde ISO/IEC 27001:2005 olarak yayınlanmış daha sonra 25 Eylül 2013 tarihinde ISO/IEC 27001 :2013 versiyon güncellemesi yapılmıştır.

Şekil 2.2 ISO 27001Standardı Tarihçesi (Kosutic, 2013)[4]

Bilgi insan hayatının her evresinde, bilimin her alanında, ülkelerin askeri ve ekonomik gelişimlerinde geçmişten günümüze vazgeçilmez bir ihtiyaç ve rekabet aracı olmuştur. Bilgi, düşünerek, akıl yürüterek, gözlem yaparak ya da araştırarak

[4] Kosutic, D. (2013, 10 08). Retrieved 01 02, 2016, from ISO 27001 Academy: http://www.iso27001standard.com/blog/2013/10/08/infographic-new-iso-27001-2013-revision-what-has-changed/

keşfedilme ve geliştirilme, insan beynine, fiziki ya da dijital ortamlara kaydedilme, kullanılıp değerlendirilme, çeşitli vasıtalarla aktarılma veya yok edilme özelliklerine sahip bir yaşam döngüsü içindedir. Bilginin yaşam döngüsü içindeki her aşamasında gizlilik, bütünlük ve yetkili erişilebilirliğinin sağlanması bilgi güvenliğinin üç temel prensibidir (ISO/IEC 27001, 2013).

Bilginin Gizliliği; İçerden ve dışardan sözel, fiziki (basılı doküman) ve elektronik ortamlardaki veriye yetkisiz kişiler tarafından erişilmesinin engellenmesidir.

Bilginin Bütünlüğü; Bilginin her ortamda bozulmadan ve değişikliğe uğramadan muhafaza edilip hizmete sunulmasıdır.

Bilginin Erişilebilirliği; Bilginin yetkisi olan kişiler tarafından her zaman ulaşılabilir ve kullanılabilir durumda olmasını sağlamaktır.

Bilgi güvenliğinin küçük ölçekteki kurum ve firmalarda daha kolay bir şekilde sağlayabilme olasılığı varken, aşağıdaki özelliklere sahip büyük ölçekli kurum ve firmalarda bilgi güvenliğinin sağlanmasında bir çok yönden karmaşıklıklar ve zorluklar oluşabilmektedir.

- Farklı bölgelerde faaliyet gösteren alt unsurlarının olması
- Farklı profilde ve çok sayıda personele sahip olması
- Geniş iletişim ağının olması,
- Bilgi teknolojileri cihazları ve uygulamalarının fazla olması
- Hizmet verilen müşteri sayısının ve profilinin fazla olması
- Büyük bir alanda konuşlu olması
- Sahip olduğu bilgilerin çok büyük kapasitelerde olması
- Tabi olduğu yasal mevzuatların fazla olması

2.3.5 Bilgi Güvenliği Yönetim Sistemi Kullanmanın Faydaları

- Bilgi varlıklarının korunması için kontroller oluşturarak kişilerin bireysel kontrollerine bağımlı olmadan, sistemi tesadüflere bırakmadan korumada süreklilik sağlar.
- Dış paydaşlar ile uygun sözleşmeler yapılarak elde edilen bilgilerin gizliliğinin korunmasını sağlar.
- Müşterilere ve sponsorlara bilgilerinin koruma altında olduğu güvencesini verir.
- Sürekli denetimler ile uygunsuzlukların tespit edilerek gerekli iyileştirmeler ile sistemin canlı kalmasını sağlar.
- Bilgi güvenliği bilincinin sağlanması için gerekli eğitimlerin verilmesini sağlar.
- Oluşturulacak afet planları ile her durumda iş devamlılığı sağlar
- Risk analizi ile zafiyet tespit edilip, risk işleme planı ile gerekli tedbirlerin alınmasını sağlar.
- Kurum bilgi varlıklarının ve önem derecelerinin tespit edilmesini sağlar.

III. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNİN KURULMASI

3.1 ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi Standardının Maddelerinin İncelemesi

BGYS kurulumu ve işletiminde *PUKÖ* (Planla / Uygula / Kontrol Et / Önlem Al), adım - adım plan yaparak sonuca ulaşmakta kullanılan sistematik bir yaklaşım kullanılmaktadır.

Tablo 3.1. PUKO ISO:27001 (ÇALIK, 2013)[5]

PUKÖ	27001:21013 deki Bölümler	
Planla	4. Organizasyon Bağlamı 6.Planlama	5.Liderlik
Uygula	7.Destek 8.Operasyon	
Kontrol-et	9.Performans Değerlendirme	
Önlem al	10.İyileştirme	

a) Planla (BGYS'nin kurulması) BGYS politikası, amaclar, hedefler, surecler ve prosedurlerin gelistirilmesidir.

b)Uygula (BGYS'nin gerceklestirilmesi ve isletilmesi) BGYS politikası, kontroller, surecler ve prosedürlerin gerceklestirilip isletilmesidir.

[5] ÇALIK, O. (2013, 05 12). *Ulusal Bilgi Güvenliği Kapısı*. Retrieved 05 18, 2016, from Bilgi Güvenliği: http://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/iso-27001-2013-bilgi-guvenligi-yonetim-sistemi-standardindaki-degisiklikler-ve-yenilikler.html

c)Kontrol Et (BGYS'nin izlenmesi ve gozden gecirilmesi) BGYS politikası, amaclar ve surec performansının değerlendirilmesi, uygulanabilen yerlerde olculmesi ve sonucların rapor edilmesidir.

d)Onlem al (BGYS'nin surekliliğinin sağlanması ve iyilestirilmesi)

Yonetimin gozden gecirme sonuclarına dayalı olarak, duzeltici ve onleyici faaliyetlerin gerceklestirilmesidir. Bilgi guvenliği yonetimi, surekli devam eden bir gelişim sureci olarak dusunulmelidir. PUKO modelinde gosterildiği gibi bir dongu icinde durmaksızın sürekli devam etmelidir. PUKO modeli ozet olarak ne yapılacağına karar verilmesi, kararların gerceklestirilmesi, calıstığının kontrol edilmesi hedefine uygun calısmayan kontroller icin onlemlerin alınmasıdır. (PEHLİVAN, 2010)

Bu durumda, Bilgi Guvenliği Yonetim Sistemi kurmak isteyen kurumlarda gorev yapan yönetici ve personelde genellikle asağıdaki yanlıs algılamalar olmaktadır:

a) BGYS'nin kapsamı bilgi islem birimidir.

b) BGYS'yi kurmaktan ve yurutmekten sorumlu ust

duzey yonetici bilgi islem birimi baskanıdır.

c) BGYS bir bilgi teknolojileri projesidir.

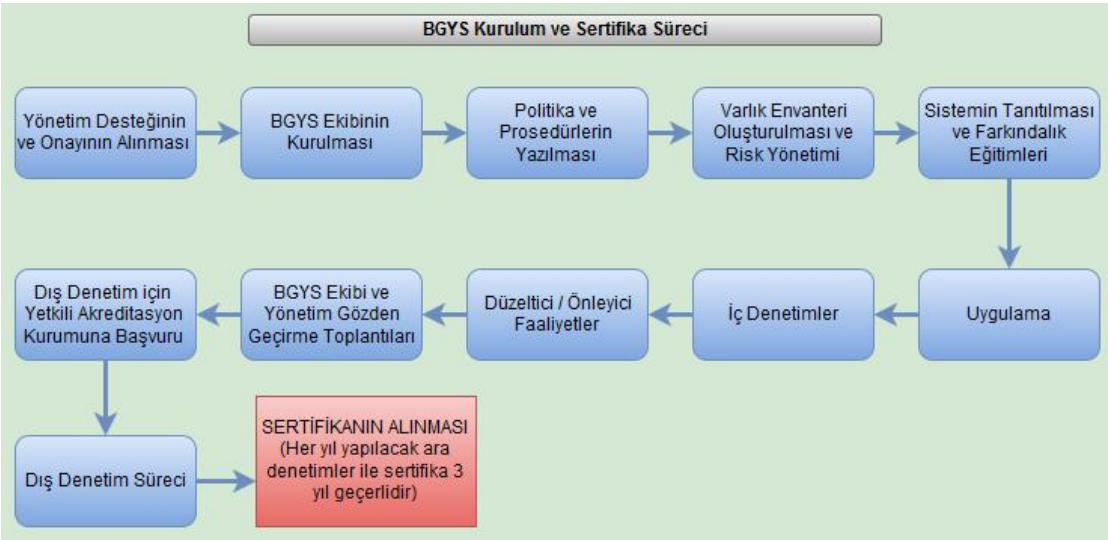
d) BGYS'nin sadece ve doğrudan bilgi islem birimi ile bağlantısı vardır.

e) BGYS'nin sadece ve doğrudan guvenlik teknolojileri ile bağlantısı vardır.

f) BGYS bir yazılım/donanım/servis tedarik projesidir.

g) BGYS, tamamen baska bir kuruma yaptırılabilen bir projedir (PEHLİVAN, 2010)

ISO 27001 standardının tum gereklerinin yerine getirilmesini takiben dıs denetim icin basvurulabilir. Bu denetimin akredite bir sertifikalandırma kurumu tarafından gerceklestirilmesi gerekir. Denetimi gerceklestirecek kurum once dokumantasyonu gözden gecirir. Bu dokumantasyon guvenlik politikasını, risk değerlendirmesi dokumanlarını, risk eylem planını, uygunluk beyanı ve guvenlik prosedurlerini icermelidir. Bu incelemeyi takiben, ileriki bir tarihte denetçiler tarafından yerinde denetim gerceklestirilir. Bu denetimde, kurulusunuzun buyukluğune ve isinizin tipine uygun kontrollerin, tarafınızca hazırlanmıs bulunan prosedurlerde tanımladığınız sekilde yapılıp yapılmadığı gozden gecirilir. Basarılı bir denetimi takiben ISO 27001 sertifikası alınır. Alınan sertifikadan sonra yılda bir ya da iki kez, firmanın belirleyeceği periyotlara gore $yenilemeye yonelik gozden gecirme tetkikleri gerceklestirilir. Alınan belge 3 yıl gecerlidir ve 3. Yılın sonunda yeniden belgelendirme tetkiki yapılarak sureci icerisindeki gelismeleriniz gozden geçirilir. (PEHLİVAN, 2010)



Şekil 3.1. BGYS Süreci

3.1.1 ISO 27001:2013 BGYS Standardı Başlıkları;

Başlıklarda Bilgi Güvenliği Yönetim Sisteminin oluşumunda izlenmesi gereken aşamalar ve bu aşamalar gerçekleştirilirken yapılması gereken en az gereksinimler ifade edilmektedir. Bu başlıkların bir kaçı aşağıdaki örnek (Örnek-1) ile detaylı açıklanmıştır.

0	Introduction /Giriş
1	Scope /Kapsam
2	Normative references / Atıf yapılan standartlar ve/veya dokümanlar
3	Terms and definitions /Terimler ve tarifleri
4	Context of the organization / Kurum Bağlamı
5	Leadership /Liderlik
6	Planning /Planlama
7	Support /Destek
8	Operation /Operasyon
9	Performance evaluation /Performans değerlendirme
10	Improvement /İyileştirme

Şekil 3.2. ISO 27001:2013 BGYS Standardı Başlıkları

Örnek -1

5.Liderlik; Bu başlıkta üst yönetimin bilgi güvenliği yönetim sistemi kurulmasında yerine getirmesi gereken sorumluluklar ifade edilmektedir. Sistemin kurulup, işletilmesi için gerekli organizasyon yapısının resmi olarak kurulması, rollerin dağıtılması, bilgi güvenliği politikasının onaylanıp yayınlanması, sistemin gözden geçirilip geliştirilmesinde gerekli yönetim katılımının sağlanması gibi konular üst yönetim sorumluluğu olarak açıklanıp, kontrollerde aranan gerekliliklerdendir. Oluşturulacak politika ve prosedürlerde bu gerekliliklerin nasıl, ne zaman, kim /kimler tarafından yerine getirileceği ve nasıl kayıt altına alınacağı mutlaka belirtilmelidir. Örnek;_Sistemin gözden

geçirilmesi yılda 1 defa ilgili yöneticilerin (yönetici makamları detaylı olarak yazılır) katılacağı Yönetim Gözden Geçirme toplantısı ile yapılmaktadır, toplantı da görüşülen konular ve kararlar Toplantı formu ile kayıt altına alınmaktadır.

7.Destek: Kurumun bilgi güvenliği yönetim sistemi için gerçekçi kaynak planlaması yapması ve planlanan kaynakları gerektiğinde sağlaması, bilgi güvenliği organizasyonu içerisinde görev alacak personelin risk değerlendirme, güvenlik(fiziki, teknik, insan kaynakları, yasalar), bilgi güvenliği olay yönetimi gibi konularda bilgi ve becerilere sahip olması, tüm personelde bilgi güvenliği farkındalığı yaratılması, kurum içi ve dışı iletişim gereksinimlerinin tespit edilip işletim planlarının oluşturulması, basılı bilginin saklanması, sınıflandırılması ve yok edilmesi ile ilgili prosedürlerin uygulanabilir şekilde oluşturulması ve tüm bu gerekliliklerin kayıtlarda gösterilmesi bu başlık altında incelenmektedir.

Örnek; "BGYS ekibinde risk değerlendirme ve bilgi güvenliği olay yönetiminde görevli personele eğitim aldırılması, kurum içinde her yıl en az iki defa BGYS farkındalık eğitimi verilmesi" eğitim planına yazılır ve gerçekleştirildiğinde ilgili formlar ile kayıt altına alınır.

3.1.2 ISO 27001:2013 BGYS Standardı Kontrol Hedefleri (Ek-A);

ISO 27001 bilgi güvenliği yönetim sistemi kontrol hedefleri insan kaynakları politikalarından iş sürekliliği planlarına kadar çok detaylı olarak hazırlanmış bir dokümandır. Bilgi güvenliğinin sağlanmasında rol oynayabilecek her konu için

gereklilikler tespit edilerek sistemin oluşumu ve devamlılığı sağlanmaktadır. Prosedür ve Politika örnekleri EK B, EK C, EK D, EK E' de sunulmuştur.

A.5: Bilgi Güvenliği Politikaları / Information Security Policies ;

ISO/IEC 27000:2014(E) Bilgi Güvenliği Yönetim Sistemi Genel Tanım ve Terimlere göre Politika: Bir organizasyonun üst yönetimi tarafından resmi olarak açıklanan, organizasyonun amaçları ve hedefleridir (ISO/IEC, 2013). Politikalar üst yönetim düzeyinde, kapsamlı ve net ifadeler ile oluşturulmalıdır. Politikalar ile ilgili detaylar ve açıklamalar prosedür, akış şemaları, talimatlar da belirtilmelidir.

Bu kapsamda kurumun bilgi güvenliği politikası dokümanı oluşturulur. Bu doküman kurumun bilgi güvenliği tarifi, geniş kapsamlı hedefi ve amacının yanında fiziki güvenlik, zararlı yazılım güvenliği, temiz masa temiz ekran, iş sürekliliği, ağ yönetimi, internet erişimi ve benzerleri gibi, daha da çeşitlendirebileceğimiz konularda kurumunu politikalarını içermelidir. Bu konular tek bir politika dokumanı altında olabileceği gibi, kurumun yapısına ve seçimine göre farklı konularda farklı dokümanlarda oluşturulabilir.

A.6: Bilgi Güvenliği Organizasyonu / Organization of Information Security;

Bilgi güvenliği sorumlulukları tanımlanıp tayin edilir, görev ayrımları yapılır, iç ve dış paydaşlarla irtibatlar tanımlanır, mobil cihazlar ile ve evden/dış ofisten çalışırken uygulanacak politika ve güvenlik önlemleri oluşturulur.

A.7: İnsan Kaynakları Güvenliği / Human Resource Security;

Personel güvenliğini sağlamak için işe almadan önce, iş esnasında ve iş akdinin sonlanmasında uygulanacak politika ve güvenlik tedbirleri oluşturulur.

A.8: Varlık Yönetimi / Asset Management ;

Kurum bilgi varlıklarının envanteri oluşturulup varlıkların sorumluları belirlenir. Varlıkların kullanımı ve iadesi ile ilgili prosedür oluşturulur. Bilginin (basılı ya da elektronik ortamda bulunan) sınıflandırılması, sınıfına göre etiketlenmesi, varlıkların ve bilgi yüklü ortamlar/medyaların yönetimi bilgi sınıfına göre uygun olarak muhafaza edilmesi, yok edilmesi veya transfer edilmesi ile ilgili yetkisiz erişim, hatalı kullanım veya bozulma gibi durumların önüne geçmek için prosedürler oluşturulur.

A.9: Erişim Kontrol / Access control ;

Bilgi ve bilgi işleme erişimlerini sınırlamak ve kontrol altında tutabilmek için kurumun gerekliliklerine göre prosedür oluşturulur. Prosedürde ağ ve ağ servislerine kontrollü erişim sağlanması, kullanıcı hesapları açılması/kapatılması ve sistemlere erişim haklarının yönetimi ve periyodik olarak gözden geçirilmesi, sistem ve uygulamalara erişim kontrolleri ile ilgili kurallar oluşturulur.

A.10: Kriptografi / Cryptography ;

Kurumda kripto sistemi kullanılıyorsa kripto sistemi kullanım ve anahtar yaşam döngüsü prosedürü oluşturulur.

A.11: Fiziki ve Çevresel Güvenlik / Physical and Environmental Security ;

Fiziki çevrenin ve fiziki çevreye erişimin kurallarının belirlenmesi, kritik bilgi içeren oda ve ofislerin (güvenli alan) yetkisiz erişime, yangın su baskını gibi olaylara karşı alınacak tedbirlerin belirlenmesi, güvenli alanlarda çalışma kurallarının belirlenmesi, yetkisiz erişim olan alanların tespit edilip kontrol altına alınması, malzeme güvenliğinin sağlanması(kablo güvenliği, temiz masa politikası, malzemelerin bakımı) gibi konuları içeren prosedür oluşturulur.

A.12: İşlem Güvenliği / Operations Security ;

Bilgi işleme hizmetleri işlemlerinin doğru ve güvenilir olmasını, zararlı yazılımlara karşı korunmasını, veri kayıplarının engellenmesini sağlamak için işletme, değişim yönetimi, kapasite planlama, test ve canlı çalışma ortamlarının ayrı tutulması prosedürleri oluşturulur. Zararlı yazılımlardan korunma, yedekleme, kayıt alma ve izleme, hassasiyet testleri yönetimi gibi prosedürler oluşturulur.

A.13: İletişim Güvenliği / Communications Security;

Ağ üzerindeki bilginin korunması, bilgi transferinde güvenliğin sağlanması için ağ kontrolleri, ağ servislerinin güvenliği, kurum içi ve dışı veri transferi güvenliği konularında prosedürler oluşturulması gerekmektedir.

A.14: Sistem Tedarik, Geliştirme ve Bakım / System Acquisition, Development and Maintenance

Güvenli yazılım geliştirme, sistem değişikliği ve bakım, güvenli dış kaynak yazılım desteği, sistem güvenlik testleri, sistem/cihaz ya da yazılım kabul için gereklilikleri içerir.

A.15: Tedarikçi Güvenliği / Supplier Relationships

Tedarikçilerin kurum varlıklarına erişiminde ortaya çıkacak riskleri azaltmak için tedarikçiler tarafından kabul edilmiş ve belgeye dayandırılmış bilgi güvenliği gereklilikleri ile tedarikçi hizmetlerinin izlenmesi ve gözden geçirilmesi için prosedürler oluşturulmalıdır.

A.16: Bilgi Gvenliği Olay Yönetimi / Information Security Incident Management

Güvenlik olayları ve zafiyetlerindeki iletişimde ve güvenlik olaylarının yönetiminde sürekli ve etkili bir yol belirlemek için prosedür ve sorumluların yönetimi, bilgi güvenliği olaylarının ve zayıflıklarının raporlanması, güvenlik olaylarına yanıt verilmesi, kanıtları toplanması gibi gereklilikleri içerir.

A.17: İş Devamlılığı Planının Bilgi Güvenliği Yönleri / Information Security Aspects of Business Continuity Management

Kurumunun iş devamlılığı yönetim sistemlerine bilgi güvenliği devamlılığı planlarının dahil edilip, iş devamlılığı planları oluşturulması, planların gerçekleştirilip kayıtlarının tutulması, gerekirse bilgi işleme tesislerinin yedeğinin sağlanması gibi gereklilikler için prosedürler oluşturulması gerekir.

A.18: Politikilar (İç gereklilik) ve Yasalara (dış gereklilik) Uyum / Compliance; with internal requirements, such as policies, and with external requirements, such as laws

Bilgi güvenliği ile ilgili yasal yaptırımların aksine doğabilecek bilgi güvenliği ihlallerini engelleyebilmek için bağlı olunan yasal gerekliliklerin takip edilmesi ve tanımlanması, kayıtların korunması, varlık kullanım haklarının belirlenmesi (lisans gibi), kişisel kimlik tanımlama bilgilerinin korunması, tüm oluşturulan politika/prosedür ve işlem süreçlerinin bağımsız denetçiler tarafından belirli aralıklarla denetlenmesi konularında gereklilikler içerir.

IV. VARLIK ENVANTERİ VE RİSK ANALİZİ

4.1 Varlık Envanteri

Kurumun Varlık Envanter Listesi'nde varlıklara ait aşağıdaki bilgilerin yer alması envaterin takibi açısından önemlidir.

- Varlık Adı
- Varlık Grubu
- Varlık Sahibi Personel/Departman
- Varlık Emanetçisi Personel/Departman
- Varlık Değeri Gizlilik-Bütünlük-Erişilebilirlik
- Elde Ediliş Tarihi
- Yedek Durumu
- Bulunduğu Yer

Kurumda kullanılan iç iletişim yöntemleri ile çalışanlar tarafından yeni belirlenmiş veya sisteme dahil olmuş varlıklar Bilgi Güvenlik Ekip Lideri'ne bildirilir.Varlık Envanteri kontrol altında tutularak, envantere dahil edilen veya çıkarılan varlıklar için revize edilir.

Varlıkların, Tablo 4.1. de belirtilrn değerlere göre, BGYS Ekibi tarafından Gizlilik, Bütünlük ve Erişilebilirlik güvenlik hedefleri açısından değerlerinin seviyesi belirlenebilir.

Tablo 4.1. Varlık Değerleri (KOÇ, 2008)[6]

	Varlık Değerleri			
Güvenlik Hedefi	**Düşük (1)**	**Orta (2)**	**Yüksek (3)**	**Çok Yüksek (4)**
GİZLİLİK	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritik seviyesi altındaki bilgi kurumu etkilemez.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritik seviyesi altındaki bilgi kurumu çok az etkiler.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan kritik bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.
BÜTÜNLÜK	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritik seviyesi altındaki bilgi kurumu etkilemez.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritik seviyesi altındaki bilgi kurumu çok az etkiler.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.
ERİŞİLEBİLİRLİK	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritik seviyesi altındaki bilgi kurumu etkilemez.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritik seviyesi altındaki bilgi kurumu çok az etkiler.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.

Ayrıca, üniversitede yönetimi tarafından gerek elektronik ortamda bulunan bilgilerin gerekse basılı ortamda saklanan dokümanların sınıflandırılması (ÇOK GİZLİ, GİZLİ, HİZMETE ÖZEL, TASNİF DIŞI vs.) gizlilik seviyelerine göre

[6] KOÇ, F. (2008, 03 20). UEKAE BGYS0003-Varlık Envanteri Oluşturma Kılavuzu. Kocaeli, Gebze, Türkiye.

etiketlenmesi, saklanması ve erişilebilmesi ile ilgili prosedürler geliştirilmeli ve uygulamaya konmalıdır.

4.2 Risk Değerlendirme

4.2.1 Tehditlerin Ve Zayıflıkların Belirlenmesi

Tanımlanan herbir varlık için zayıflıklar ve zayıflıklara göre herbir varlık için tehdit belirlenir.Herbir tehdit için risk değerlendirmesi yapılır. Örnek Tablo 4.2. Zayıflık Listesi ve Tablo 4.3. Tehdit Listesi örnek olarak oluşturulmuştur.

Tablo 4.2. Zayıflık Listesi

Sıra No	Zayıflık Listesi
1	Binanın Dış Doğa Şartlarına Göre Yetersiz Olması
2	Laptoplarda Kurum Bilgilerinin Yer Alması
3	Dokümanların güvensiz saklanmas
4	Dokümanların kontrolsüz çoğaltılması
5	Dokümanların imha edilmemesi
6	Periyodik yenilemenin yapılmaması
7	Yangın
8	Fiziksel Güvenliğin Bulunmaması
9	Şifre yönetimi yetersizliği
10	İşletim sistemi açıklıkları ve hataları
11	Anti-virus yazılımının çalışmaması,zararlı yazılımlar
12	Dış kaynak kullanımında işletilen prosedür (ögrenci e-posta) ve yönetmeliklerin veya şartnamelerin eksikliği/yetersizliği
13	Kaynak kodlardaki açıklıklar
14	Şifre yönetimi yetersizliği
15	Erişim izinlerinin yanlış verilmesi
16	Kullanıcı bilgi eksikliği, yanlış kullanımı veya kasıt,yetkilendirme hataları
17	Şifre yönetimi yetersizliği
18	İşletim sistemi açıklıkları ve hataları
19	Anti-virus yazılımının çalışmaması,zararlı yazılımlar
20	Periyodik bakım eksikliği
21	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık
22	Periyodik bakım eksikliği
23	Voltaj değişikliklerine, ısıya, neme, toza, yıldırım düşmesine duyarlılık
24	Turnikelerin ısıya, neme, toza duyarlılığı

25	Erişim izinlerinin yanlış verilmesi
26	Kaynak kodlardaki açıklıklar
27	Switch odalarına girişlerde yetersiz fiziksel kontrol
28	Konfügürasyondaki güvenlik açıkları ve içerik güvenliği yazılımının düzgün çalışmaması
29	Uzak erişim bağlantılarının güvenli olmaması
30	Donanım arızaları
31	Kullanıcı hataları
32	Servis sağlayıcının hata ve kusurları
33	İnternet hattının zarar görmesi
34	Periyodik bakım eksikliği, donanım ve sensör arızaları
35	Fiziki güvenlik yetersizliği
36	Lisans belge ve bilgilerinin kaybolması
37	Lisans envanterinin güncel olmaması
38	Sistem odası izolasyonun eksik olması
39	Su baskını (binanın doğa şartlarına yetersiz oluşu)
40	Deprem,Yangın
41	Cihazın uzun süre açık bırakılması
42	Kritik personel seçiminde hatalı davranılması ya da yedeğinin bulundurlumaması
43	Güvenlik farkındalığı eksikliği
44	Donanımların veya yazılımların yanlış kullanılması
45	İşe alımda yetersiz özgeçmiş incelemesi ve doğrulaması

Tablo 4.3. Tehdit Listesi

Sıra No	**Tehdit Listesi**
1	Donanımın bozulması nedeniyle erişimin durması
2	Hırsızlık ve kasten zarar verme
3	Sunucu hizmetlerinin devre dışı kalması
4	İşletim sisteminin çökmesi
5	Başkaarının kimliğine bürünme
6	Kullanıcı hesabı bilgilerinin 3. şahıslarla paylaşılması ve e-posta erişiminde dışa bağımlılık.
7	Bilgi hırsızlığı
8	Kurum prestijinin zarar görmesi
9	Verilerin silinmesi, çalınması ya da değiştirilmesi
10	Yetkisiz kullanım
11	Maddi kayıp
12	Cihaz arızalanması
13	Güç dalgalanmaları, tozlanma, donanım arızaları
14	Turnike ve kart okuyucuların arızalanması

15	Sistemin düzenli çalışmaması
16	Sistemin düzenli çalışmaması ve gizliliğin ve bütünlüğün ihlal edilmesi
17	Konfügürasyonların silinmesi
18	Yetkisiz ağ erişimi ve bölgesel bilgi sistem hizmetleri kesintisi
19	Bölgesel bilgi sistem hizmetleri kesintisi
20	Kasıtlı ya da kazara hasar verme
21	İnternetten yapılan hacker saldırılarına maruz kalmak
22	İnternette açık olarak giden verilerin dinlenmesi ,veri hırsızlığı
23	İşletim sisteminin çökmesi,
24	Kullanıcı dosyalarına erişim problemi
25	Tüm bilgi sistem servislerinin devre dışı kalması
26	Dosyaların silinmesi veya çalınması
27	Kurumun tüm internet hizmetinin devre dışı kalması
28	Kampüsün tüm kablosuz internet hizmetinin devre dışı kalması
29	Akü destek süresinin azalması
30	Mali işlemlerin aksaması
31	E-kütüphane hizmetinin devre dışı kalması
32	DNS hizmetinin devre dışı kalması
33	CRM hizmetinindevre dışı kalması
34	Disaster (Felaketten Kurtarma) hizmetinin durması
35	Öğrenci işlemlelerinin aksaması
36	Uzaktan eğitim hizmetinin devre dışı kalması
37	Lisans hizmetinin devre dışı kalması
38	Windows güncelleştirme hizmetinin devre dışı kalması
39	Anti-virus yönetim programı devre dışı kalması
40	İnternetten veya iç ağdan saldırılara açık olma
41	İnternet kesintisi
42	Sistem Odası alarm sisteminin devre dışı kalması
43	5651- Erişim ve Yerel Sağlayıcıları Yasasl Yükümlülükleri kanununu yerine getirememe
44	Log kaydının düzgün alınaması
45	Cihazları çalınması ya da zarar görmesi
46	Lisansız ve zararlı yazılımların yüklenebilmesi
47	Saldırı kaynak noktası olarak kullanıma açık olmak
48	Kişisel veri kaybı
49	Fazla ya da eksik lisans kullanımı
50	Kontrolsüz giriş ve erişim
51	Personel hataları
52	Cihaz ömrünün kısalması

4.2.2 Risk Değerlendirme Metedolojisi

Olası Hata Türü ve Etkileri Analizi (Failure Mode and Effects Analysis – FMEA) risk öncelik sayısı belirleme formulü kullanılmıştır. Metodun temelinde; sistem ve alt sistemler değerlendirilip, sistemin eksiklerinden kaynaklanan potansiyel hata türleri tespit edilir. Sistemlerin kalitesi, güvenilirliği ve korunabilirliği arttırılır.

Belirlenen herbir tehdit için risk hesaplaması yapılır. Risk öncelik sayısı için aşağıdaki formül uygulanır.

- P: Her bir hata modunun oluşma olasılık değeri,
- S: Hatanın ne kadar önemli olduğunun değeri,
- D: Hataların keşfedilmesinin zorluk derecelendirilmesi,

RÖS = PxSxD

Risk Öncelik Sayısı = Gerçekleşme Sıklığı x İş Etki Değeri (Şiddet) x Fark Edilebilirlik

İş Etki Değeri

Tehditin işin kesintiye uğratılması açısından etkisi tanımlanır. Bu kesinti; bilgi varlığının bütünlüğünün, gizliliğinin ve kullanılabilirliğinin zarar görmesi açısından dikkate alınır. Methodolojisi aşağıdaki Tablo 4.4. de verilmiştir.

Tablo 4.4. İş Etki Tablosu

ETKİ	TEHDİTİN ÖZELLİĞİ	PUAN
Çok Yüksek	Tehdit varlıkların süresiz olarak işlem yapamamasına ve tamamiyle zarar görmesine yol açar.Hasarın giderilmesi ve önlem alınması için	5

	önemli harcamalar gerekir. Sistemin tamamen baştan dizayn edilmesini ve yapılandırılmasını gerektirir.Kurumun çıkarları misyonu, prestiji büyük zarar görebilir veya etkilenebilir.İnsan hayatı kaybı ve ciddi yaralanmalar gerçekleşebilir.Bilgi sistem hizmetleri tamamen durabilir.	
Yüksek	Tehdit varlıklara büyük ölçüde zarar verir ve/veya birçok kişi ve kurumun kendisi /prestiji zarardan etkilenebilir. Varlığa bir sure erişilemeyeceğinden iş süreçlerinde gecikme olur.Tamir ve yeniden konfügürasyon gerekir. Hasarın giderilmesi ve önlem alınması için harcamalar gerekebilir.Bilgi sistemleri hizmetleri kısmen verilemeyebilir.	4
Normal	Tehditin varlıklar üzerinde orta düzeyde etkisi olur, varlıklara kısa sureli erişim sağlanamaz. Tamir ve yeniden konfügürasyona gerek olabilir. Varlık ya da sistem sahiplerine kötü ün kazandırabilir. Kurumun çıkarları, prestiji etkilenmez.	3
Az	Tehditin varlıklar üzerinde küçük etkisi olur,varlığı tamir etmeye ya da yeniden konfügürasyona gerek yoktur.Bazı varlıklara kısa sureli erişim olmayabilir.Bilgi sistemleri genel çalışması	2

	etkilenmez.Kurumun çıkarları, prestiji etkilenmez.	
Yok	Tehditin varlık üzerinde hiç etkisi yoktur.	1

Gerçekleşme Sıklığı

Gerçekleşme sıklığı değerlendirilirken ve sıklık aralığı tespit edilirken zayıflıkların çokluğu ve var olan kontrollerin bu zayıflıkları ne kadar kapatabildiği, saldırgan motivasyonu, tehdit biçiminin uygulama kolaylığı, bilginin rakipler için cazibesi, personelin psikolojisi, uygulamanın hassas ve kontrol edilemeyen (politikaya uymama – kuralın etrafında dolaşma) çalışan davranışı gibi unsurlar değerlendirilir. Puanlama 1 – 10 arasında yapılabilir.

Tablo 4.5. Gerçekleşme Sıklığı

GERÇEKLEŞME SIKLIĞI	**GERÇEKLEŞME SAYISI (Yılda)**	**PUAN**
Çok Yüksek: Hata neredeyse kaçınılmaz	10'dan fazla	5
Yüksek: Tekrarlayan hatalar	5-10	4
Orta: Tesadüfi hatalar	3-5	3
Düşük: Nispeten az gerçekleşen	1-2	2
Çok Düşük: İhtimal dahilinde olmayan hatalar	0	1

Farkedilebilirlik

Farkedilebilirlik değerlendirilirken, kontrollerin neler olduğu, envanterin kullanım şekli ve yedekleme sıklığı gibi unsurlar göz önüne alınarak gerçekleşen tehlikenin farkedilme ihtimaline göre bir puan verilmelidir.

Tablo 4.6. Farkedilebilirlik

Farkedilebilirlik	Fark Edilme Şekli	Puan
Kesinlikle Farkedilemez	Kontroller potansiyel hataları ve takribinde olacakları engelleyemez veya farkedemez.	5
Düşük	Kontrollerin potansiyel hataları ve takribinde olacakları engelleme veya farketme ihtimali çok düşük	4
Normal	Kontrollerin potansiyel hataları ve takribinde olacakları engelleme veya farketme ihtimali normal	3
Çok Yüksek	Kontrollerin, potansiyel hataları ve takribinde olacakları engelleme veya farketme ihtimali çok yüksek.	2
Neredeyse Kesin	Kontroller potansiyel hataları ve takribinde olacakları neredeyse kesinlikle engeller veya farkeder.	1

4.2.3 Risklerin Sınıflandırılması

Risk analizi yapılırken belirlenen her tehlikenin iş etki puanı, gerçekleşme ihtimal puanı ve farkedilebilirlik puanları Risk İşleme Tablosu ’na işlenerek risk değerleri bulunur. Risk sınıflandırması, risk puanı aralıklarına göre Tablo 4.7. deki gibi yapılabilir.

Tablo 4.7. Risklerin Sınıflandırılması

Risk Puanı	**Kategori**	**Risk İşleme**
0 – 10	Kabul edilebilir risk	Kontrol veya Faaliyet gerekmez.
10 – 40	Orta dereceli risk	Kontrol veya faaliyet gerekir.
40– 50	Yüksek ve kabul edilemez risk	Faaliyet gerekir.

4.2.4 Risk İşleme Planlaması

Risk değerlendirme tamamlandıktan sonra riskin işlemesi yapılımalıdır. Risk işleme seçenekleri şunlardır:

- Riskin kabulü
- Riskten kaçınma
- Riski azaltma ve kontrol etme
- Riskin transferi

Kabul edilebilir risk seviyesi 0 – 10 puan arası riskler olarak tanımlanmıştır. Tüm varlıklar için hedefimiz riskleri bu seviyeye çekmektir. Aksi belirtilmedikçe bütün risklerin azaltılması ve kontrol edilmesi birincil aksiyondur. Bazı riskler bu seviyeye çekilemediğinden bunların göze alınması ve riskin kabulü yönetim tarafından yapılabilir.

10 – 40 puan arasındaki riskler için kontrol yöntemleri tanımlanır. Riski kontrol etmek ve azaltmak için kontroller ve uygun yönetim eylemleri yapılır. Bu eylemlerle birlikte sorumlular / sorumluluklar tayin edilmelidir.

Uygulama düzeyinde riski azaltamadığımız ve yönetimce kabul edilemez riskler için riskten kaçınma opsiyonu geçerlidir. Riske neden olan uygulamadan vazgeçilmesi ve iş sürecinin ve prosedürünün farklılaştırılması risk işleme seçeneklerinden biridir.

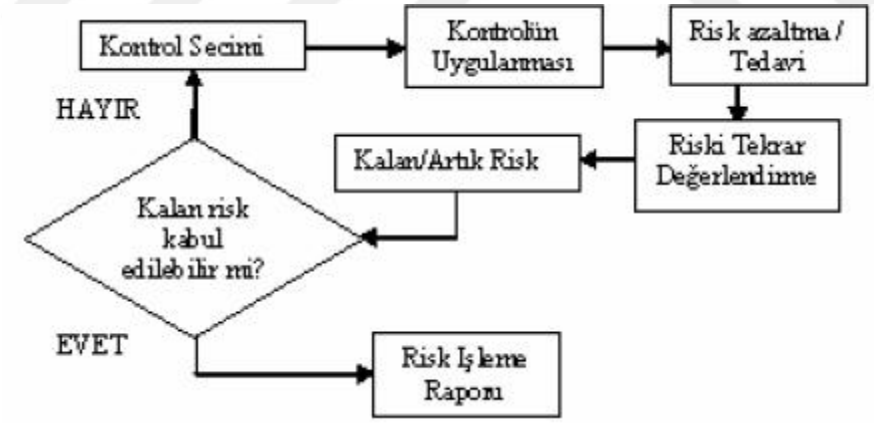
Riskin kurumunuz kontrollerini aştığı durumlarda (yangın, deprem, sabotaj, afet, soygun, vb.) emniyet güçleri, kamu acil durum kurumları, sigorta kurumlarına risk transfer edilebilir.

Risk işlemede birincil işlem kontrollerin seçilmesidir. Riskin azaltması ve kontrol edilmesi her zaman ilk seçenek olmalıdır. Kontroller; uygulayıcısının ve bu uygulamayı izleyip ölçecek ilgili personelin görüşlerinin alınması, konuyla ilgili teknik iç – dış uzmanların ve danışmanların görüşlerinin alınması ile seçilir. Seçilen kontroller ISO 27001 Standartının EK – A bölümündeki maddelerden seçilmeye çalışılmalıdır. Burada kontrol amaçları ve kontrollerin ifadesi yer alır. Bu kontrollerin teknik düzeyde nasıl uygulanacağı konu uzmanları ve kontrolü uygulayacak kişilerin seçimiyle oluşturulur. Seçilen en uygun kontrolün maliyeti tespit edilir ve riski azaltılacak varlıkla ilgili yapılan varlık değerlendirmesi ve iş etkisinden dolayı potansiyel mali zararla kıyaslaması yapılır. Maliyet fayda analiz sonucu seçilen kontrolün uygulanabilir olup olmadığına karar verilir. Uygulanabilir kontroller hayata geçirilir. Uygulanabilir olmayan kontroller için

tekrar gözden geçirme yapılarak maliyet fayda dengesi sağlanana kadar araştırma süreci devam eder.

Uygulanan kontroller ile ilgili kayıtlar risk işleme planından belirtilir. Maliyetler ve alınan sonuçlar BGYS toplantılarında görüşülür ve riskin yeni durumda ölçüm sonucu risk işleme planındaki ilgili yere yazılır. Risk puanı kabul edilebilir seviyeye çekilene kadar gerekiyorsa yeni kontroller uygulanır ve ölçümlere devam edilir.

Risk isleme sureci sonrasında geriye kalan ve artık risk (*residual risk*) olarak adlandırılan riskler, kabul edilen riskler veya tamamen ortadan kaldırılamayan risklerdir. Risk yonetim surecinde yapılan kontrol secimi sonucunda artık riski azaltmaya yonelik bir akıs diyagramı Sekil 4.1. ile aşağıda sunulmuştur.



Şekil 4.1. Risk Yönetim Süreci (ATSAN, 2010)[7]

Yapılan risk analiz çalışması **EK A Risk İşleme Planı** dokümanı olarak sunulmuştur.

[7] ATSAN, K. (2010, 01 04). *ITMS DAYS Sunumları* . Retrieved 05 16, 2016, from ITMS Days: http://www.itmsdays.com/sunumlar.php

V. SONUÇ

Bilgi güvenliği yönetim sistemi kurulumu kapsamında; Öncelikle bilgi güvenliği yönetim sisteminin kurulumu konusunda üniversite yönetiminin onayı ve desteği alındıktan sonra, ISO:27001:2013 Bilgi Güvenliği Yönetim Sistemi Standartı maddeleri kapsamında politika ve prosedürler yazılıp, risk analizleri ve iş sürekliliği planları yapılmıştır.Uygulanabilirlik bildirgesi ile gerekliliklerin nasıl, ne sıklıkta gerçekleştirileceğinin listesi oluşturulduktan sonra, BGYS sistemi hakkında tüm üniversiteye bilgilendirme ve farkındalık eğitimleri verilerek uygulamaya geçilmiştir.Yapılan iç denetimler ve gözden geçirme toplantılarından sonra düzenelmeler yapılarak dış denetimin son hazırlıkları tamamlanmıştır.

Kurulum sürecinde bilgi güvenliğinin çok detaylı bir şekilde her açıdan değerlendirilerek, sürekli gelişen ve kontrol edilen canlı bir sistem olarak oluşturulması gerektiği anlaşılmıştır. Aksi takdirde oluşacak yeni zafiyet ve tehditlerin tespiti ve karşı tedbir alınması sağlanamayacağından sistemin etkin şekilde işletilmesi mümkün olmayacaktır. Yönetim tarafından, bilgi güvenliğinin bir süreç olarak benimsenmesi, bu sürecin doğru ve etkin işlemesini sağlayacak uygulanabilir politika ve denetimlerin oluşturulması ve gerekli kaynak ve eğitimlerin verilmesine destek sağlanması sürecin en önemli aşamasıdır.

Bilgi güvenliği yönetim sistemini yalnızca güvenlik cihazları veya politikalar belirlenmesi ile oluşturulacak bir sistem olarak değil, ISO 27001: 2013 BGYS standardı başlıkları ve kontrol hedefleri gerekliliklerinin gerektirdiği gibi yönetim desteği alınmış, insan faktörü ön planda tutularak gerekli eğitimler sağlanmış,

güncel risk değerlendirmeleri ve planları oluşturulmuş, uygulanabilir politika ve prosedürler yaratılmış, gerektiği şekilde denetimlerin yapıldığı, benimsenmesi gereken bir kültür ve sistem olarak uygulamak gerçeği ortaya çıkmaktadır.

VI. KAYNAKLAR

Vikipedi. (2015, 06 05). Retrieved 01 02, 2016, from Vikipedi: https://tr.wikipedia.org/wiki/Casus_yaz%C4%B1l%C4%B1m

ATSAN, K. (2010, 01 04). *ITMS DAYS Sunumları* . Retrieved 05 16, 2016, from ITMS Days: http://www.itmsdays.com/sunumlar.php

Bayraktaroğlu, E. (2008, 11 08). *Bilgi Güvenliği Yönetim Sistemi - Tehditler* . Retrieved 01 02, 2016, from https://www.bilgiguvenligi.gov.tr: https://www.bilgiguvenligi.gov.tr/kurumsal-guvenlik/bilgi-guvenligi-yonetim-sistemi-tehditler-3.html

BENSGHİR, T. K. (2011, 11 23). Retrieved 11 01, 2015, from Dokuz Eylül Üniversitesi: http://www.deu.edu.tr/UploadedFiles/Birimler/19430/BGUVENLIK_TBENSGHIR_Kas%C4%B1m2011.ppt

Central, I. (n.d.). *ITIL Central*. Retrieved 01 02, 2016, from ITIL Central: http://itsm.fwtk.org/History.htm

ÇALIK, O. (2013, 05 12). *Ulusal Bilgi Güvenliği Kapısı*. Retrieved 05 18, 2016, from Bilgi Güvenliği: http://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/iso-27001-2013-bilgi-guvenligi-yonetim-sistemi-standardindaki-degisiklikler-ve-yenilikler.html

FBI IC3. (2013, 10 10). *2013_IC3Report.* Retrieved 12 09, 2014, from The Internet Crime Complaint Center: http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf

G.Watkins, S. (2008). *An Introduction to Information Security and ISO/IEC 27001.* IT Governance Publishing-9781905356690.

GÖKŞEN, M. E. (2009, 10 01). *Sosyal Bilimler Enstitüsü Dergisi.* Retrieved 12 10, 2014, from Dokuz Eylül Üniversitesi: www.sbe.deu.edu.tr/dergi/cilt11.say%C4%B14/Eminagao%C4%9Flu%20Goksen%2011.4.pdf

ISO/IEC. (2013, 10 01). ISO/IEC 27000:2014. Geneva, CH-1211, Switzerland.

ISO/IEC 27001. (2013, 10 01). ISO/IEC 27001. Geneva, CH-211, Switzerland.

ISO/IEC-27001. (2013, 10 01). ISO/IEC 27001:2013. Geneva, CH-1211, Switzerland.

KALAY, Y. (2014). *Vt Kullanıcıları.* Retrieved 10 31, 2015, from Yıldız Teknik Üniversitesi: http://www.yildiz.edu.tr/~ukalay/index_files/VT/vt_files/01-Giris.pdf

KOÇ, F. (2008, 03 20). UEKAE BGYS0003-Varlık Envanteri Oluşturma Kılavuzu. Kocaeli, Gebze, Türkiye.

Kosutic, D. (2013, 10 08). Retrieved 01 02, 2016, from ISO 27001 Academy: http://www.iso27001standard.com/blog/2013/10/08/infographic-new-iso-27001-2013-revision-what-has-changed/

L.Simon, K. D. (2002). *Art of Deception.* USA: Wiley.

Oğraş, O. (2011, 03 25). *MSHOWTO*. Retrieved 01 02, 2016, from MSHOWTO: http://www.mshowto.org/itil-nedir-surec-haritalari-versiyon-farkliliklari-ve-standardizasyon.html

Öğüt, A. (2001). *Bigi Çağında Yönetim.* Ankara: Nobel Yayın Dağıtım.

ÖNEL, A. D. (2007, 08 28). *UEKAE-BGYS.* Retrieved 11 01, 2015, from https://www.bilgiguvenligi.gov.tr/bilgi-guvenligi-yonetimi-dokumanlari/uekae-bgys-0001-bilgi-guvenligi-yonetim-sistemi-kurulum-kilavuzu.html

PEHLİVAN, V. M.-İ. (2010). ISO 27001:2005 Bilgi Güvenliği Yönetimi Standardı. *Mühendislik Bilimleri ve Tasarım Dergisi*, 49-56.

PESEN, M. M. (2015, 06 08). *Bilgi Güvenliği Nedir ve Nasıl Sınıflandırılır*. Retrieved 11 01, 2015, from Sibergah: http://www.sibergah.com/genel/bilgi-guvenligi-nedir-ve-nasil-siniflandirilir/

Resmi Gazete. (2013, 11 11). *20131111-6.htm.* Retrieved 12 09, 2014, from Resmi Gazete: http://www.resmigazete.gov.tr/eskiler/2013/11/20131111-6.htm

Saba, G. (2013, 5 21). Retrieved 10 31, 2015, from SlideShare: http://www.slideshare.net/GamzeSaba/knowledge-management-24307129

Symantec. (2013, 04 01). *Archived Publications.* Retrieved 12 09, 2014, from Symantec Enterprise: http://www.symantec.com/security_response/publications/archives.jsp

Thomas H. Davenport, L. P. (2013). *Working Knowledge: How Organizations Manage What They Know.* Harvard Business Press.

TUTU, İ. (2010, 11 21). *Çözüm Park.* Retrieved 01 02, 2016, from http://www.cozumpark.com/blogs/cobit-itil/archive/2010/11/21/cobit-nedir.aspx

UEKAE. (2008, 02 21). *UEKAE BGYS-0013 ISO IEC 27001 Denetim Listesi* . Retrieved 12 09, 2014, from Bilgi Güvenliği:

https://www.bilgiguvenligi.gov.tr/bilgi-guvenligi-yonetimi-dokumanlari/uekae-bgys-0013-iso-iec-27001-denetim-listesi.html

Verry, J. (2013, 11 4). *Information Security Blog*. Retrieved 12 10, 2014, from Pivot Point Security: http://www.pivotpointsecurity.com/risky-business/iso-27001-universities

Vikipedi. (2015, 11 16). *Vikipedi*. Retrieved 01 02, 2016, from Vikipedi: https://tr.wikipedia.org/wiki/Truva_at%C4%B1_%28bilgisayar%29

VII. EKLER

EK A Risk İşleme Planı

EK B Erişim Yönetimi Prosedürü

EK C Haberleşme ve İşletim Yönetimi Prosedürü

EK D Ağ ve Sistem Yönetimi Prosedürü

EK E Politikalar

EK F LS.BİS.010 Uygulanabilirlik Bildirgesi Listesi_Rev01

EK G FR.BİS.016 Sistem Kontrol Formu

VIII. ÖZGEÇMİŞ

Emre DEMİROK, 26.11.1981 tarihinde Bursa'da doğdu. Kazım Karabekir İlköğretim Okulu'nda başladığı ilk ve orta öğretimini 1995 yılında tamamladı. Lise öğrenimi için Teknik Astsubay Hazırlama Okulu'nu kazanıp 3 yıllık öğrenimi tamamladıktan sonra Muhabere Elektronik Bilgi Sistemleri Okulu'nda 1 yıl süren Bilgi Sistemleri eğitimini 1999 yılında tamamlayarak mezun oldu. Anadolu Üniversitesi İşletme Fakültesi Yönetim Organizasyon bölümündeki lisans öğrenimini 2005 yılında tamamladı.

1999-2012 yılları arasında Türk Silahlı Kuvvetleri Bilgi İşlem birimlerinin çeşitli kademelerinde ve NATO – Afganistan RCC-Karargahı'nda görev yaptı. 2012 yılında Okan Üniversitesi ailesine katılarak 2012-2015 yılllarında Bilgi İşlem Yöneticisi olarak çalıştı.

2014 yılında Okan Üniversitesi Fen Bilimleri Enstitüsü Bilişim Teknolojileri programında yüksek lisans eğitimine başladı. 2015 yılında Londra / İngiltere'de ISO 27001:2013 Bilgi Güvenliği Yönetim Sistemi Baş Denetçi eğitimi ve sınavına katılarak denetçi sertifikası aldı. Emre DEMİROK, evli ve Okan Üniversitesi Genel Sekreter Yardımcısı olarak görev yapmaktadır.

EK A RİSK İŞLEME PLANI

RİSK İŞLEME OPSİYONU
A) RİSK KABUL
B) RİSKTEN KAÇINMA
C)RİSK AZALTMA VE KONTROL
D)RİSK TRANSFERİ

NO	VARLIK	ZAYIFLIK	TEHDİT	RİSK DEĞERLENDİRME					RİSK İŞLEME							
				İŞ ETKİ DEĞERİ	GERÇEKLEŞME SIKLIĞI	FARK EDİLEBİLİRLİK	RİSK PUANI	RİSK İŞLEME OPSİYONU	SEÇİLEN YENİ KONTROL /EYLEM	SORUMLU	UYGULAMA TARİHİ	İŞ ETKİ DEĞERİ	GERÇEKLEŞME SIKLIĞI	FARK EDİLEBİLİRLİK	RİSK PUANI	KALAN RİSK
1	Bilgi Güvenliği Dokümantasyonu	Dokümanların güvensiz saklanması (hırsızlık)	Verilerin kaybolması	3	1	2	6	A							0	6
2	Back up (Kaset, CD ve DVD)	Periyodik yenilemenin yapılmaması	Donanımın bozulması nedeniyle erişimin durması,veri kaybı	3	2	2	12	C	Her yıl mevcut kaset toplamının 3/1 i oranında yeni kaset alınması	Sistem Birimi		3	1	2	6	6
		Yangın	Veri kaybı	4	1	4	16	C	Çelik Kasa Alınması	Sistem Birimi		4	1	3	12	4
		Manyetik Bozulma	Veri kaybı	3	2	3	18	C	Senelik Kasetlerin 2 kopya alınması	Sistem Birimi		3	1	4	12	6
		Fiziksel Güvenliğin Bulunmaması	Hırsızlık ve kasten zarar verme	3	2	1	6	A							0	6
3	Öğrenci Domain Sunucusu	Şifre yönetimi yetersizliği	Sunucu hizmetlerinin devre dışı kalması veya başkalarının kimliğine bürünme	4	1	3	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		3	1	2	6	6
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi	3	1	1	3								0	3
		Anti-virus yazılımının çalışmaması,zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve veri kaybı oluşması	3	1	1	3								0	3
4	Öğrenci E-posta Hesapları	Dış kaynak kullanımında işletilen prosedür (ögrenci e-posta) ve yönetmeliklerin veya şartnamelerin eksikliği/yetersizliği	Kullanıcı hesabı bilgilerinin 3. şahıslarla paylaşılması ve e-posta erişiminde dışa bağımlılık.	4	1	1	4								0	4
5	Kurum Web Sitesi www.okan.edu.tr	Kaynak kodlardaki açıklıklar	Yetkisiz kullanım, web sitesinin devre dışı kalması, bilgi hırsızlığı, kurum prestijinin zarar görmesi	4	1	3	12	C	Yıllık Sızma testlerinin mutlaka yapılması	Yazılım Birimi		4	1	2	8	4
		Şifre yönetimi yetersizliği	Verilerin silinmesi, çalınması ya da değiştirilmesi	3	1	3	9	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Yazılım Birimi		3	1	2	6	3
		Erişim izinlerinin yanlış verilmesi	Verilerin silinmesi, çalınması ya da değiştirilmesi	4	1	3	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Yazılım Birimi		3	1	2	6	6
6	Kurum Web Sitesi Veritabanı	Şifre yönetimi yetersizliği	Verilerin silinmesi, çalınması ya da değiştirilmesi	3	1	1	3	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Yazılım Birimi		3	1	2	6	-3
		Erişim izinlerinin yanlış verilmesi	Verilerin silinmesi, çalınması ya da değiştirilmesi	4	1	3	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Yazılım Birimi		4	1	1	4	8
7	Kurum Web Sitesi Sunucusu	Şifre yönetimi yetersizliği	İşletim sistemi hizmetlerinin ve websitesinin devre dışı kalması, bilgi hırsızlığı,kurum prestijinin zarar görmesi	4	1	3	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Yazılım Birimi		4	1	1	4	8
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi ve web sitesinin çalışmaması.	4	1	1	4								0	4

		Zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve veri kaybı oluşması	4	1	1	4								0	4
8	Fakülte web siteleri	Kaynak kodlardaki açıklıklar	Yetkisiz kullanım, web sitesinin devre dışı kalması, bilgi hırsızlığı, kurum prestijinin zarar görmesi	3	1	1	3								0	3
		Şifre yönetimi yetersizliği	Verilerin silinmesi, çalınması ya da değiştirilmesi	3	1	1	3								0	3
		Erişim izinlerinin yanlış verilmesi	Verilerin silinmesi, çalınması ya da değiştirilmesi	3	1	1	3								0	3
9	Fakülte web siteleri Veritabanı	Şifre yönetimi yetersizliği	Verilerin silinmesi, çalınması ya da değiştirilmesi	3	1	2	6								0	6
		Erişim izinlerinin yanlış verilmesi	Verilerin silinmesi, çalınması ya da değiştirilmesi	3	1	2	6								0	6
10	Fakülte web siteleri Sunucusu	Şifre yönetimi yetersizliği	Sunucu hizmetlerinin devre dışı kalması veya başkalarının kimliğine bürünme	3	1	1	3								0	3
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi	3	1	1	3								0	3
		Zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve veri kaybı oluşması	3	1	1	3								0	3
11	Okim Web Sitesi	Kaynak kodlardaki açıklıklar	Yetkisiz kullanım, web sitesinin devre dışı kalması, bilgi hırsızlığı, kurum prestijinin zarar görmesi	3	1	1	3								0	3
		Şifre yönetimi yetersizliği	Verilerin silinmesi, çalınması ya da değiştirilmesi	3	1	1	3								0	3
		Erişim izinlerinin yanlış verilmesi	Verilerin silinmesi, çalınması ya da değiştirilmesi	3	1	3	9								0	9
12	Okim Veritabanı	Şifre yönetimi yetersizliği	Verilerin silinmesi, çalınması ya da değiştirilmesi	3	1	2	6								0	6
		Erişim izinlerinin yanlış verilmesi	Verilerin silinmesi, çalınması ya da değiştirilmesi	3	1	2	6								0	6
13	OLB Web Sitesi	Kaynak kodlardaki açıklıklar	Yetkisiz kullanım, web sitesinin devre dışı kalması, bilgi hırsızlığı, kurum prestijinin zarar görmesi	3	1	1	3								0	3
		Şifre yönetimi yetersizliği	Verilerin silinmesi, çalınması ya da değiştirilmesi	3	1	1	3								0	3
		Erişim izinlerinin yanlış verilmesi	Verilerin silinmesi, çalınması ya da değiştirilmesi	3	1	3	9								0	9
14	Okim & OLB Sunucusu	Şifre yönetimi yetersizliği	İşletim sistemi hizmetlerinin ve websitesinin devre dışı kalması, bilgi hırsızlığı,kurum prestijinin zarar görmesi	3	1	2	6								0	6
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi ve web sitesinin çalışmaması.	3	1	1	3								0	3
		Zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve veri kaybı oluşması	3	1	1	3								0	3
15	Users.okan.edu.tr Web Sitesi	Kaynak kodlardaki açıklıklar	Yetkisiz kullanım, web sitesinin devre dışı kalması, bilgi hırsızlığı, kurum prestijinin zarar görmesi	2	1	1	2								0	2
		Şifre yönetimi yetersizliği	Verilerin silinmesi, çalınması ya da değiştirilmesi	2	1	1	2								0	2
		Erişim izinlerinin yanlış verilmesi	Verilerin silinmesi, çalınması ya da değiştirilmesi	2	1	1	2								0	2
16	Users.okan.edu.tr Sunucusu	Şifre yönetimi yetersizliği	İşletim sistemi hizmetlerinin ve websitesinin devre dışı kalması, bilgi hırsızlığı,kurum prestijinin zarar görmesi	2	1	1	2								0	2
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi ve web sitesinin çalışmaması.	2	1	1	2								0	2
		Anti-virus yazılımının çalışmaması,zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve veri kaybı oluşması	2	1	1	2								0	2

17	Öğrenci web sitesi stu.okan.edu.tr	Kaynak kodlardaki açıklıklar	Yetkisiz kullanım, web sitesinin devre dışı kalması,kullanıcı bilgilerinin çalınması, kurum prestijinin zarar görmesi	3	1	3	9								0	9
		Şifre yönetimi yetersizliği	Verilerin silinmesi, çalınması ya da değiştirilmesi	3	1	1	3								0	3
		Erişim izinlerinin yanlış verilmesi	Verilerin silinmesi, çalınması ya da değiştirilmesi	3	1	2	6								0	6
18	Alt Siteler	Kaynak kodlardaki açıklıklar	Yetkisiz kullanım, web sitesinin devre dışı kalması	3	1	3	9								0	9
		Şifre yönetimi yetersizliği	Verilerin silinmesi, çalınması ya da değiştirilmesi	3	1	1	3								0	3
		Erişim izinlerinin yanlış verilmesi	Verilerin silinmesi, çalınması ya da değiştirilmesi	3	1	2	6								0	6
19	Web Yedekleme Sunucusu	Şifre yönetimi yetersizliği	İşletim sistemi hizmetlerinin ve websitesinin devre dışı kalması, bilgi hırsızlığı	2	1	2	4								0	4
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi	2	1	1	2								0	2
		Zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve veri kaybı oluşması	2	1	1	2								0	2
20	Dosya Sunucu Kullanıcı Dosyaları	Kullanıcı bilgi eksikliği, yanlış kullanımı veya kasıt,yetkilendirme hataları	Verilerin silinmesi ya da bilgi hırsızlığı	4	1	3	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	1	1	4	8
21	Dosya Sunucu	Şifre yönetimi yetersizliği	Sunucu hizmetlerinin devre dışı kalması veya önemli bilgilerin hırsızlığı	4	1	3	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	1	1	4	8
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi,kullanıcı dosyalarına bir süre erişim problemi	3	1	1	3								0	3
		Anti-virus yazılımının çalışmaması,zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve veri kaybı ,kullanıcı dosyalarına bir süre	3	1	1	3								0	3
22	Tuzla Kampüsü Santral	Periyodik bakım eksikliği	Cihazın arızalanması	4	2	2	16	C	Yıllık bakım sözleşmelerinin yapılması	Yapı İşleri		4	2	1	8	8
		Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	4	1	2	8								0	8
23	Kadıköy Kampüsü Santral	Periyodik bakım eksikliği	Cihazın arızalanması	3	2	2	12	C	Yıllık bakım sözleşmelerinin yapılması	Yapı İşleri		3	2	1	6	6
		Voltaj değişikliklerine, ısıya, neme, toza, yıldırım düşmesine duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	3	1	2	6								0	6
24	Mecidiyeköy Kampüsü Santral	Periyodik bakım eksikliği	Cihazın arızalanması, maddi zarar	3	2	2	12	C	Yıllık bakım sözleşmelerinin yapılması	Yapı İşleri		3	2	1	6	6
		Voltaj değişikliklerine, ısıya, neme, toza, yıldırım düşmesine duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	3	1	2	6								0	6
25	Güvenlik Kamera Sistemi	Kamera fiziksel durumları	Cihazların sökülmesi yada zarar görmesi	3	2	2	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Yapı İşleri		3	2	1	6	6
		Kayıt cihazı problemleri	Kayıt alınamaması	3	2	2	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Yapı İşleri		3	2	1	6	6
26	Kapı Güvenlik Sistemi Turnikeleri	Periyodik bakım eksikliği	Turnike ve kart okuyucuların arızalanması	2	2	2	8									
		Turnikelerin ısıya, neme, toza duyarlılığı	Donanım arızaları	3	2	1	6								0	6
27	Kapı Güvenlik Sistemi	Erişim izinlerinin yanlış verilmesi	Yetkisiz erişim	3	1	2	6								0	6
		Kaynak kodlardaki açıklıklar	Sistemin düzenli çalışmaması	3	3	1	9								0	9

27	Yazılımı	Kullanıcı bilgi eksikliği, yanlış kullanımı veya kasıt	Sistemin düzenli çalışmaması veya gizliliğin ve bütünlüğün ihlal edilmesi	3	3	1	9								0	9
28	Kapı Güvenlik Sistemi Sunucusu	Şifre yönetimi yetersizliği	Sunucu hizmetlerinin devre-dışı kalması ve kartlı giriş hizmetinin devre dışı kalması, veri kaybı	4	1	3	12								0	12
		İşletim sistemi açıklıkları ve hataları	Sunucu hizmetlerinin devre-dışı kalması ve kartlı giriş hizmetinin devre dışı kalması, veri kaybı	3	1	1	3								0	3
		Anti-virus yazılımının çalışmaması,zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve kartlı giriş hizmetinin devre dışı kalması, veri kaybı	3	1	1	3								0	3
29	Ağ Cihazları Konfügürasyon Dosyaları	Kullanıcı bilgi eksikliği, yanlış kullanımı veya kasıt	Dosyaların silinmesi veya çalınması	3	1	2	6								0	6
30	Tüm Kampüsler Kenar Switchler	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	3	1	1	3								0	3
		Periyodik bakım eksikliği	Cihazın arızalanması	3	1	1	3								0	3
		Şifre yönetimi yetersizliği	Konfügürasyonların silinmesi ve yetkisiz ağ erişimi ve bölgesel bilgi sistem hizmetleri kesintisi	4	1	3	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	1	2	8	4
		Switch odalarına girişlerde yetersiz fiziksel kontrol	Kasıtlı ya da kazara hasar verme	3	1	3	9								0	9
		Odalarda açıkta bulunan portların aktif olması	Yetkisiz erişim	2	3	3	18	C	Portların kapatılması ve bunların yılda 1 kez güncelliğinin kontol edilmesi	Sistem Birimi		2	1	1	2	16
31	Tuzla Kampüsü Omurga Switch	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	4	2	1	8								0	8
		Şifre yönetimi yetersizliği	Konfügürasyonların silinmesi ve yetkisiz ağ erişimi ve kurumun tüm bilgi sistem servislerinin devre dışı kalması	4	2	2	16	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	1	1	4	12
32	Kadıköy Kampüsü Omurga Switch	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	4	2	1	8								0	8
		Şifre yönetimi yetersizliği	Konfügürasyonların silinmesi ve yetkisiz ağ erişimi ve kampüsün tüm bilgi sistem servislerinin devre dışı kalması	4	2	2	16	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	1	1	4	12
34	Mecidiyeköy Kampüsü Omurga Switch	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	4	2	1	8								0	8
		Şifre yönetimi yetersizliği	Konfügürasyonların silinmesi ve yetkisiz ağ erişimi ve kampüsün tüm bilgi sistem servislerinin devre dışı kalması	4	2	2	16	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	1	1	4	12
35	Tuzla Kampüsü Firewall	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	4	2	1	8								0	8
		Şifre yönetimi yetersizliği	Konfügürasyonların silinmesi, yetkisiz erişim ve kurumun tüm internet hizmetinin devre dışı kalması	4	2	2	16	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	2	1	8	8
		Konfügürasyondaki güvenlik açıkları ve içerik güvenliği yazılımının düzgün çalışmaması	Yetkisiz erişim ve internetten yapılan hacker saldırılarına maruz kalmak	4	2	1	8								0	8
		Uzak erişim bağlantılarının güvenli olmaması	İnternette açık olarak giden verilerin dinlenmesi ,veri hırsızlığı	4	2	2	16	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	2	1	8	8
		Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	4	2	1	8								0	8

36	Kadıköy Kampüsü Firewall	Şifre yönetimi yetersizliği	Konfügürasyonların silinmesi, yetkisiz erişim ve kampüsün tüm internet hizmetinin devre dışı kalması	3	2	1	6								0	6
		Konfügürasyondaki güvenlik açıkları ve içerik güvenliği yazılımının düzgün çalışmaması	Yetkisiz erişim ve internetten yapılan hacker saldırılarına maruz kalmak	3	2	1	6								0	6
		Uzak erişim bağlantılarının güvenli olmaması	İnternette açık olarak giden verilerin dinlenmesi ,veri hırsızlığı	3	1	3	9									
37	Mecidiyeköy Kampüsü Firewall	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	4	2	1	8								0	8
		Şifre yönetimi yetersizliği	Konfügürasyonların silinmesi, yetkisiz erişim ve kampüsün tüm internet hizmetinin devre dışı kalması	3	2	1	6								0	6
		Konfügürasyondaki güvenlik açıkları ve içerik güvenliği yazılımının düzgün çalışmaması	Yetkisiz erişim ve internetten yapılan hacker saldırılarına maruz kalmak	3	2	1	6								0	6
		Uzak erişim bağlantılarının güvenli olmaması	İnternette açık olarak giden verilerin dinlenmesi ,veri hırsızlığı	3	1	3	9									
39	Tuzla Kampüsü Kablosuz Ağ Kontroller Cihazı	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	3	1	1	3								0	3
		Şifre yönetimi yetersizliği	Konfügürasyonların silinmesi, yetkisiz erişim ve kampüsün tüm kablosuz internet hizmetinin devre dışı kalması	3	2	2	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		3	2	1	6	6
40	Kadıköy Kampüsü Kablosuz Ağ Kontroller Cihazı	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	3	1	1	3								0	3
		Şifre yönetimi yetersizliği	Konfügürasyonların silinmesi, yetkisiz erişim ve kampüsün tüm kablosuz internet hizmetinin devre dışı kalması	3	1	1	3								0	3
41	Mecidiyeköy Kampüsü Kablosuz Ağ Kontroller Cihazı	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	3	1	1	3								0	3
		Şifre yönetimi yetersizliği	Konfügürasyonların silinmesi, yetkisiz erişim ve kampüsün tüm kablosuz internet hizmetinin devre dışı kalması	3	1	1	3								0	3
43	Tüm Kampüsler Kablosuz Erişim Cihazları	Koruma kafesi olmaması	Cihazların çalınması	3	2	2	12	C	Tüm Cihazlara Koruma Kafesi takılması	Yapı İşleri		3	1	2	6	6
44	Tuzla Kampüsü SAN Switch	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	4	1	1	4								0	4
		Şifre yönetimi yetersizliği	Konfügürasyonların silinmesi,kurum veri depolama ünitelerine erişimin kesilmesi	4	2	2	16	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	2	1	8	8
45	Kadıköy Kampüsü SAN Switch	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	4	2	1	8								0	8
		Şifre yönetimi yetersizliği	Konfügürasyonların silinmesi,kurum disaster merkezi depolama ünitelerine erişimin kesilmesi	3	2	1	6								0	6
46	Tuzla ve Kampüsü Yedekleme Ünitesi	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları,kasete yedeklerin doğru alınamaması	3	1	1	3								0	3
47	Kadıköy Kampüsü Yedekleme Ünitesi	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları,kasete yedeklerin doğru alınamaması	3	1	1	3								0	3
48	Tuzla Kampüsü Sistem Odası Kesintisiz Güç Kaynağı	Isıya, neme, toza, duyarlılık	Tozlanma, donanım arızaları,akülerin ömrünün daha cabuk bitmesi	3	1	1	3								0	3
		Periyodik bakım eksikliği	Akü destek süresinin azalması, cihazın arızalanması	3	1	4	12	C	Bakımlarını 4 aylık periyodlarda mutlaka yapılması	Sistem Birimi		3	1	2	6	6

49	Kadıköy Kampüsü Sistem Odası Kesintisiz Güç Kaynağı	Isıya, neme, toza, duyarlılık	Tozlanma, donanım arızaları,akülerin ömrünün daha cabuk bitmesi	3	1	1	3								0	3
		Periyodik bakım eksikliği	Akü destek süresinin azalması, cihazın arızalanması	3	1	4	12	C	periyodlarda mutlaka yapılması	Sistem Birimi		3	1	2	6	6
50	Mecidiyeköy Kampüsü Sistem Odası Kesintisiz Güç Kaynağı	Isıya, neme, toza, duyarlılık	Tozlanma, donanım arızaları,akülerin ömrünün daha cabuk bitmesi	3	1	1	3								0	3
		Periyodik bakım eksikliği	Akü destek süresinin azalması, cihazın arızalanması	3	1	4	12	C	Bakımlarını 4 aylık periyodlarda mutlaka yapılması	Sistem Birimi		3	1	2	6	6
52	Tuzla Kampüsü Storage	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	4	1	1	4								0	4
		Şifre yönetimi yetersizliği,disk arızaları	Konfügürasyonların silinmesi, yetkisiz erişim ve kurumun tüm sunucu hizmetinin devre dışı kalması	4	2	2	16	C	Yedek disk bulundurulması	Sistem Birimi		4	2	1	8	8
53	Kadıköy Kampüsü Storage	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	4	1	1	4								0	4
		Şifre yönetimi yetersizliği,disk arızaları	Disk konfügürasyonların silinmesi, disaster sunucu hizmetinin devre dışı kalması	4	2	2	16	C	Yedek disk bulundurulması	Sistem Birimi		4	2	1	8	8
54	Tuzla Kampüsü Diğer Sanal Sunucular	Şifre yönetimi yetersizliği	İşletim sistemi hizmetlerinin devre dışı kalması, yetkisiz erişim	3	1	1	3								0	3
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi	3	1	1	3								0	3
		Zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve veri kaybı oluşması	3	1	1	3								0	3
55	Tuzla Kampüsü Kimlik Doğrulama Sunucusu	Şifre yönetimi yetersizliği	İşletim sistemi hizmetlerinin ve internet kimlik doğrulama hizmetinin devre dışı kalması	3	1	2	6								0	6
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi	3	1	2	6								0	6
		Zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve veri kaybı oluşması	3	1	2	6								0	6
56	Tuzla Kampüsü Sanallaştırma Sunucuları(ESX)	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	4	1	3	12	C	Yedek Sunucu ve disk bulundurulması	Sistem Birimi		4	1	2	8	4
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi, tüm bilgi işlem hizmetlerinin devre dışı kalması	4	1	3	12	C	Güncelleştirmelerin zamanında ve önce test ortamında yapılması	Sistem Birimi		4	1	2	8	4
		Zararlı yazılımlar	Sunucu hizmetlerinin ve tüm bilgi işlem hizmetlerinin devre-dışı kalması ve veri kaybı oluşması	4	1	3	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	1	1	4	8
57	Tuzla Kampüsü Primary Domain Controller Sunucusu	Şifre yönetimi yetersizliği	E-posta ve oturum açma hizmetinin devre dışı kalması, başkasının kimliğine bürünme	4	1	2	8								0	8
		İşletim sistemi açıklıkları,hataları	İşletim sisteminin çökmesi,E-posta ve oturum açma hizmetinin devre dışı kalması	4	1	3	12	C	Güncelleştirmelerin zamanında ve önce test ortamında yapılması	Sistem Birimi		4	1	1	4	8
		Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	4	1	2	8								0	8
		Zararlı yazılımlar	E-posta ve oturum açma hizmetinin devre dışı kalması, başkasının kimliğine bürünme	4	1	3	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	1	1	4	8
		Donanım arızaları	E-posta ve oturum açma hizmetinin devre dışı kalması, veri kaybı	4	1	3	12	C	Yedek Sunucu ve disk bulundurlması	Sistem Birimi		4	1	1	4	8
		Şifre yönetimi yetersizliği	E-posta ve oturum açma hizmetinin devre dışı kalması, başkasının kimliğine bürünme	3	1	2	6	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		3	1	1	3	3

58	Additional Domain Controller Sunucuları	İşletim sistemi açıklıkları,hataları	İşletim sisteminin çökmesi,E-posta ve oturum açma hizmetinin devre dışı kalması	3	1	2	6								0	6
		Zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve veri kaybı oluşması	3			0	C							0	0
59	Tuzla Kampüsü E-Posta Sunucuları	Şifre yönetimi yetersizliği	E-posta hizmetinin devre dışı kalması,yetkisiz erişim, bilgi hırsızlığı, başkasının kimliğine bürünme	4	2	2	16	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	2	1	8	8
		İşletim sistemi açıklıkları,hataları	İşletim sisteminin çökmesi,E-posta hizmetinin devre dışı kalması	4	1	3	12	C	Güncelleştirmelerin zamanında ve önce test ortamında yapılması	Sistem Birimi		4	1	1	4	8
		Zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve veri kaybı oluşması	4	2	2	16	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		3	1	1	3	13
60	Personel E-postaları	Kullanıcı hataları	Veri kaybı	3	1	2	6								0	6
61	Tuzla Kampüsü Muhasebe Yazılımı	Kaynak kodlardaki açıklıklar	Yetkisiz kullanım, mali işlemlerin aksaması, bilgi hırsızlığı, maddi kayıp,kurum prestijinin zarar görmesi	4	1	2	8								0	8
		Şifre yönetimi yetersizliği	Yetkisiz kullanım, mali işlemlerin aksaması, bilgi hırsızlığı, maddi kayıp,kurum prestijinin zarar görmesi	4	1	2	8								0	8
		Erişim izinlerinin yanlış verilmesi	Yetkisiz kullanım, mali işlemlerin aksaması, bilgi hırsızlığı, maddi kayıp,kurum prestijinin zarar görmesi	4	1	2	8								0	8
		Dışardan firma desteği	Verilerin silinmesi ya da bilgi hırsızlığı	4	2	2	16	C	yedeklerin alınması ve firma ile yapılan sözlemeye gizlilik tahhüt maddesi eklenmesi	Sistem Birim/Mali iŞler		4	1	2	8	8
62	Tuzla Kampüsü Muhasebe Veritabanı	Şifre yönetimi yetersizliği	Verilerin silinmesi, çalınması ya da değiştirilmesi, maddi kayıp,kurum prestijinin zarar görmesi	4	1	2	8								0	8
		Erişim izinlerinin yanlış verilmesi	Verilerin silinmesi, çalınması ya da değiştirilmesi, maddi kayıp,kurum prestijinin zarar görmesi	4	1	2	8								0	8
63	Tuzla Kampüsü Muhasebe Sunucusu	Şifre yönetimi yetersizliği	İşletim sistemi hizmetlerinin ve mali işlemlerin aksaması, bilgi hırsızlığı, maddi kayıp,kurum prestijinin zarar görmesi	4	1	3	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	1	1	4	8
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi ve mali işlem sürecinin aksaması	4	1	3	12		Güncelleştirmelerin zamanında ve önce test ortamında yapılması						0	12
		Anti-virus yazılımının çalışmaması,zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve veri kaybı oluşması	4	1	3	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	1	1	4	8
64	Öğrenci Bilgi Sistemi Yazılım	Kaynak kodlardaki açıklıklar	Yetkisiz kullanım, öğrenci işlemlelerinin aksaması, bilgi hırsızlığı, maddi kayıp,kurum prestijinin zarar görmesi	3	1	2	6								0	6
		Şifre yönetimi yetersizliği	Yetkisiz kullanım, öğrenci işlemlelerinin aksaması, bilgi hırsızlığı, maddi kayıp,kurum prestijinin zarar görmesi	3	1	2	6								0	6
		Erişim izinlerinin yanlış verilmesi	Yetkisiz kullanım, öğrenci işlemlelerinin aksaması, bilgi hırsızlığı, maddi kayıp,kurum prestijinin zarar görmesi	3	1	2	6								0	6

		Dışardan firma desteği	Verilerin silinmesi ya da bilgi hırsızlığı	4	2	2	16	C	yedeklerin alınması ve firma ile yapılan sözlemeye gizlilik tahhüt maddesi eklenmesi	m Birim/Öğrenci İşleri		4	1	2	8	8
65	Öğrenci Bilgi Sistemi Veritabanı	Şifre yönetimi yetersizliği	Verilerin silinmesi, çalınması ya da değiştirilmesi, maddi kayıp,kurum prestijinin zarar görmesi	4	1	2	8								0	8
		Erişim izinlerinin yanlış verilmesi	Verilerin silinmesi, çalınması ya da değiştirilmesi, maddi kayıp,kurum prestijinin zarar görmesi	4	1	2	8								0	8
66	Öğrenci Bilgi Sistemi Sunucuları	Şifre yönetimi yetersizliği	İşletim sistemi hizmetlerinin ve mali işlemlerin aksaması, bilgi hırsızlığı, maddi kayıp,kurum prestijinin zarar görmesi	4	1	3	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	1	1	4	8
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi ve süreclerin aksaması	4	1	3	12		Güncelleştirmelerin zamanında ve önce test ortamında yapılması						0	12
		Anti-virus yazılımının çalışmaması,zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve veri kaybı oluşması	4	1	3	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	1	1	4	8
67	Anti-Virüs Sunucusu	Şifre yönetimi yetersizliği	Sunucu hizmetlerinin devre-dışı kalması ve anti-virus yönetim programı devre dışı kalması	3	1	2	6								0	6
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi ve anti-virus yönetim programı devre dışı kalması	3	1	1	3								0	3
		Anti-virus yazılımının çalışmaması,zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve anti-virus yönetim programı devre dışı kalması	3	1	2	6								0	6
68	Lisans Sunucusu	Şifre yönetimi yetersizliği	Sunucu hizmetlerinin devre-dışı kalması ve laboratuarlara lisans hizmetlerinin devre dışı kalması	3	1	2	6								0	6
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi ve laboratuarlara lisans hizmetlerinin devre dışı kalması	3	1	1	3								0	3
		Anti-virus yazılımının çalışmaması,zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve laboratuarlara lisans hizmetlerinin devre dışı kalması	3	1	2	6								0	6
69	Windows Güncelleştirme Sunucusu	Şifre yönetimi yetersizliği	Sunucu hizmetlerinin devre-dışı kalması ve güncelleştirme merkezi yönetim programı konfügürasyonunda bozulma	3	1	2	6								0	6
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi ve windows güncelleştirme hizmetinin devre dışı kalması	3	1	1	3								0	3
		Anti-virus yazılımının çalışmaması,zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve güncelleştirme merkezi yönetim programı konfügürasyonunda bozulma	3	1	2	6								0	6
70	Kütüphane veritabanı	Şifre yönetimi yetersizliği	Verilerin silinmesi, çalınması ya da değiştirilmesi	3	1	2	6								0	6
		Erişim izinlerinin yanlış verilmesi	Verilerin silinmesi, çalınması ya da değiştirilmesi	3	1	2	6								0	6
71	Kütüphane Sunucusu	Şifre yönetimi yetersizliği	Sunucu hizmetlerinin devre-dışı kalması ve e-kütüphane hizmetinin devre dışı kalması	3	1	2	6								0	6
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi ve e-kütüphane hizmetinin devre dışı kalması	3	1	1	3								0	3

		Anti-virus yazılımının çalışmaması,zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve e-kütüphane hizmetinin devre dışı kalması	3	1	2	6								0	6
72	Harici DNS sunucular	Şifre yönetimi yetersizliği	Sunucu hizmetlerinin devre-dışı kalması ve DNS hizmetinin devre dışı kalması, veri kaybı	4	1	3	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	1	1	4	8
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi ve DNS hizmetinin devre dışı kalması, veri kaybı	4	1	2	8								0	8
		Anti-virus yazılımının çalışmaması,zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve DNS hizmetinin devre dışı kalması, veri kaybı	4	1	3	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	1	1	4	8
73	CRSM Sunucusu	Şifre yönetimi yetersizliği	Sunucu hizmetlerinin devre-dışı kalması ve CRM hizmetinin devre dışı kalması, veri kaybı	3	1	2	6								0	6
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi ve CRM hizmetinin devre dışı kalması, veri kaybı	3	1	1	3								0	3
		Anti-virus yazılımının çalışmaması,zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve CRM hizmetinin devre dışı kalması, veri kaybı	3	1	2	6								0	6
74	CRM veritabanı	Şifre yönetimi yetersizliği	Verilerin silinmesi, çalınması ya da değiştirilmesi				0								0	0
		Erişim izinlerinin yanlış verilmesi	Verilerin silinmesi, çalınması ya da değiştirilmesi				0								0	0
75	Yazdırma sunucusu	Şifre yönetimi yetersizliği	Sunucu hizmetlerinin devre-dışı kalması ve merkezi yazdırma hizmetinin durması	3	1	2	6								0	6
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi ve merkezi yazdırma hizmetinin durması	3	1	1	3								0	3
		Anti-virus yazılımının çalışmaması,zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve merkezi yazdırma hizmetinin durması	3	1	2	6								0	6
76	Kadıköy Kampüsü Disaster Sunucuları	j değişikliklerine, ısıya, neme, toza, duya	üç dalgalanmaları, tozlanma, donanım arızala	4	1	2	8								0	8
		Şifre yönetimi yetersizliği	Sunucu hizmetlerinin devre dışı kalması,veri hırsızlığı,	3	1	3	9								0	9
		İşletim sistemi açıklıkları ve hataları	Sunucu hizmetlerinin devre-dışı kalması ve disaster (felaket kurtarma) hizmetinin durması	3	1	1	3								0	3
		Zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve disaster (felaket kurtarma) hizmetinin durması	3	1	2	6								0	6
		Donanım arızaları	elaket kurtarma sisteminin devre dışı kalmas	4	1	3	12	C	Yıllık bakım sözleşmelerinin yapılması ya da yedek disk bulundurulması	Sistem Birimi		4	1	1	4	8
77	Kadıköy Kampüsü Dosya Sunucu Belgeleri	Kullanıcı bilgi eksikliği, yanlış kullanımı veya kasıt,yetkilendirme hataları	Verilerin silinmesi ya da bilgi hırsızlığı	3	1	2	6								0	6
78	Kadıköy Kampüsü Dosya Sunucusu	Şifre yönetimi yetersizliği	Sunucu hizmetlerinin devre dışı kalması veya önemli bilgilerin hırsızlığı	3	1	2	6								0	6
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi,kullanıcı dosyalarına bir süre erişim problemi	3	1	1	3								0	3
		Anti-virus yazılımının çalışmaması,zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve veri kaybı ,kullanıcı dosyalarına bir süre erişim problemi	3	1	2	6								0	6
		Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	4	1	2	8								0	8
		Şifre yönetimi yetersizliği	Sunucu hizmetlerinin ve uzaktan eğitim hizmetinin devre dışı kalması,veri kaybı,kurum prestijinin zarar görmesi	4	1	3	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	1	1	4	8

79	Uzaktan Eğitim Merkezi Sunucusu	İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi, uzaktan eğitim hizmetinin devre dışı kalması,veri kaybı,kurum prestijinin zarar görmesi	4	1	3	12	C	Güncelleştirmelerin zamanında ve önce test ortamında yapılması			4	1	1	4	8
		Zararlı yazılımlar	Sunucu hizmetlerinin ve uzaktan eğitim hizmetinin devre dışı kalması,veri kaybı,kurum prestijinin zarar görmesi	4	1	3	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	1	2	8	4
		Donanım arızaları	Uzaktan eğitim sisteminin kabul edilemez süre devre dışı kalması	4	1	3	12	C	Yıllık bakım sözleşmelerinin yapılması	Sistem Birimi		4	1	1	4	8
		Dışardan firma desteği	Verilerin silinmesi ya da bilgi hırsızlığı	4	2	2	16	C	yedeklerin alınması ve firma ile yapılan sözlemeye gizlilik tahhüt maddesi eklenmesi	Sistem Birim/UZEM		4	1	2	8	8
80	Kadıköy Kampüsü Lisans Sunucusu	Şifre yönetimi yetersizliği	Laboratuarlara lisans hizmetlerinin devre dışı kalması	3	1	2	6								0	6
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi ve laboratuarlara lisans hizmetlerinin devre dışı kalması	3	1	1	3								0	3
		Anti-virus yazılımının çalışmaması	Laboratuarlara lisans hizmetlerinin devre dışı kalması	3	1	2	6								0	6
81	Mecidiyeköy Kampüsü Additional Domain Controller	Şifre yönetimi yetersizliği	E-posta ve oturum açma hizmetinin devre dışı kalması, başkasının kimliğine bürünme	3	1	2	6	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		3	1	1	3	3
		İşletim sistemi açıklıkları,hataları	İşletim sisteminin çökmesi,E-posta ve oturum açma hizmetinin devre dışı kalması	3	1	2	6								0	6
		Zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve veri kaybı oluşması	3			0	C							0	0
82	Kadıköy Kampüsü Sanallaştırma Sunucusu	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları				0								0	0
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi, kadıköy kampüsü tüm bilgi işlem hizmetlerinin devre dışı kalması				0								0	0
		Zararlı yazılımlar	Sunucu hizmetlerinin ve kadıköy kampüsü tüm bilgi işlem hizmetlerinin devre-dışı kalması ve veri kaybı oluşması				0								0	0
		Donanım arızaları	Kadıköy Kampüsü bilgi sistem hizmetlerinin verilememesi	4	1	3	12	C	Yedek Sunucu bulundurlması	Sistem Birimi		4	1	1	4	8
83	Tuzla Kampüsü IPS Sistemi	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	3	1	2	6								0	6
		Şifre ıönetimi yetersizliğ, kaonfügürasyon güvenlik açıkları	Konfügürasyon silinmesi,sistemin İnternetten veya iç ağdan saldırılara açık olması	4	2	3	24	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	2	2	16	8
84	Tuzla Kampüsü İnternet Hattı	İnternet hattının zarar görmesi	Dışarıdan tüm sistemlere geçici süre ulaşamama, kurumun prestij kaybı	4	2	1	8								0	8
		Servis sağlayıcının hata ve kusurları	Dışarıdan tüm sistemlere geçici süre ulaşamama, kurumun prestij kaybı	4	1	1	4								0	4
85	Kadıköy Kampüsü İnternet Hattı	İnternet hattının zarar görmesi	İnternet kesintisi	3	2	1	6								0	6
		Servis sağlayıcının hata ve kusurları	İnternet kesintisi	3	1	1	3								0	3
86	Mecidiyeköy Kampüsü İnternet Hattı	İnternet hattının zarar görmesi	İnternet kesintisi	3	2	1	6								0	6
		Servis sağlayıcının hata ve kusurları	İnternet kesintisi	3	1	1	3								0	3
88	Tuzla Kampüsü Sistem Odası Klima Sistemi	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	4	1	2	8								0	8
		Periyodik bakım eksikliği, donanım arızaları	Sistem odası sıcaklığının artması, sistemlerin kapanması, maddi zarar, yangın, kurum prestijinin zarar görmesi	4	2	2	16	C	Yıllık bakım sözleşmesinin ya da bakımının yapılması	Sistem Birimi		4	1	1	4	12

89	Kadıköy Kampüsü Sistem Odası Klima Sistemi	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	4	1	2	8								0	8
		Periyodik bakım eksikliği, donanım arızaları	Sistem odası sıcaklığının artması, sistemlerin kapanması, maddi zarar, yangın, kurum prestijinin zarar görmesi	4	2	2	16	C	Yıllık bakım sözleşmesinin ya da bakımının yapılması	Sistem Birimi		4	1	1	4	12
90	Mecidiyeköy Kampüsü Sistem Odası Klima Sistemi	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	4	1	2	8								0	8
		Periyodik bakım eksikliği, donanım arızaları	Sistem odası sıcaklığının artması, sistemlerin kapanması, maddi zarar, yangın, kurum prestijinin zarar görmesi	4	2	2	16	C	Yıllık bakım sözleşmesinin ya da bakımının yapılması	Sistem Birimi		4	1	1	4	12
92	Tuzla Kampüsü Sistem Odası Alarm Sistemi	Periyodik bakım eksikliği, donanım ve sensör arızaları	Yangın,su baskını ve yetksiz erişimde uyarı göndermeme ve bu durumda önemli maddi zarar , sistemlerin çalışmaması	3	2	1	6									
93	Kadıköy Kampüsü Sistem Odası Alarm Sistemi	Periyodik bakım eksikliği, donanım ve sensör arızaları	Yangın,su baskını ve yetksiz erişimde uyarı göndermeme ve bu durumda önemli maddi zarar , sistemlerin çalışmaması	4	1	2	8								0	8
95	Tuzla Kampüsü Sistem Odası Yangın Söndürme Sistemi	Periyodik bakım eksikliği, söndürme gazı azalması	Yangın anında devreye girememesi ya da yetersiz olması,maddi zarar, tüm bilgi işlem hizmetlerinin zarar görmesi, veri kaybı	4	1	3	12	C	Yıllık bakım sözleşmesinin ya da bakımının yapılması	Sistem Birimi		4	1	2	8	4
96	Tuzla Kampüsü Merkezi Log Sistemi	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	4	1	2	8								0	8
		Şifre yönetim yetersizliği	Konfügürasyon silinmesi, log veri kaybı	4	1	2	8	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	1	1	4	4
		Konfügürasyonun doğru yapılmaması yada bozulması	Log kaydının doğru alınamaması,5651 yasasını yerine getirememe	4	1	2	8								0	8
		Donanım arızaları	5651 yasasını yerine getirememe, veri kaybı	3	1	3	9									
97	Kadıköy Kampüsü Log Sistemi	Voltaj değişikliklerine, ısıya, neme, toza, duyarlılık	Güç dalgalanmaları, tozlanma, donanım arızaları	4	1	2	8								0	8
		Şifre yönetim yetersizliği	Konfügürasyon silinmesi, log veri kaybı	4	1	2	8								0	8
		Konfügürasyonun doğru yapılmaması yada bozulması	Log kaydının goğru alınamaması,5651 yasasını yerine getirememe	4	1	2	8								0	8
		Donanım arızaları	5651 yasasını yerine getirememe, veri kaybı	3	1	3	9									
98	Laboratuar Masa Üstü Bilgisayarları	Fiziki güvenlik yetersizliği	Cihazların çalınması ya da zarar görmesi	3	1	1	3								0	3
		Periyodik bakım eksikliği,voltaj değişikliklerine duyarlılık	Donanım arızaları, Kişisel veri kaybı,bilgisayarın bir süre kullanılamaması	3	1	1	3								0	3
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi,bilgisayarın kullanılamaması,kişisel veri kaybı	3	1	1	3								0	3
		Şifre yönetimi yetersizliği	Lisansız ve zararlı yazılımların yüklenebilmesi	3	1	3	9								0	9
99	Masa Üstü Bilgisayarlar	Fiziki güvenlik yetersizliği	Cihazların çalınması ya da zarar görmesi	3	1	1	3								0	3
		Periyodik bakım eksikliği,voltaj değişikliklerine duyarlılık	Donanım arızaları, Kişisel veri kaybı,bilgisayarın bir süre kullanılamaması	3	1	1	3								0	3
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi,bilgisayarın kullanılamaması,kişisel veri kaybı	3	1	1	3								0	3
		Anti-virus yazılımının çalışmaması,zararlı yazılımlar	Kişisel veri kaybı, saldırı kaynak noktası olarak kullanılması,	3	1	1	3								0	3
		Şifre yönetimi yetersizliği	Lisansız ve zararlı yazılımların yüklenebilmesi	3	1	3	9								0	9
		Fiziki güvenlik yetersizliği	Cihazların çalınması ya da zarar görmesi	3	1	2	6									

100	Diz üstü ve Tablet bilgisayarlar	Periyodik bakım eksikliği	Donanım arızaları, Kişisel veri kaybı,bilgisayarın bir süre kullanılamaması	3	1	1	3								0	3
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi,bilgisayarın kullanılamaması,kişisel veri kaybı	3	1	1	3								0	3
		Anti-virus yazılımının çalışmaması,zararlı yazılımlar	Kişisel veri kaybı, saldırı kaynak noktası olarak kullanılması,	3	1	1	3								0	3
		Şifre yönetimi yetersizliği	Lisansız ve zararlı yazılımların yüklenebilmesi	3	1	3	9								0	9
101	İşletim Sistemi ve Program Lisans Bilgileri	Lisans belge ve bilgilerinin kaybolması	Fazla ya da eksik lisans kullanımı	3	1	2	6								0	6
		Lisans envanterinin güncel olmaması	Fazla ya da eksik lisans kullanımı, gereksiz lisans alınması	3	1	2	6								0	6
102	Tuzla Kampüsü Sistem odası	Fiziki güvenlik yetersizliği	görmesi,yetkisiz erişim, veri kaybı.tüm bilgi işlem hizmetlerinin devre dışı kalması,maddi zarar, kurum prestijinin	4	1	3	12	C	Şifreli ve çelik kapı takılması	Sistem Birimi		4	1	2	8	4
		Sistem odası izolasyonun eksik olması	Yangın anında söndürme gazının yetersiz olması,maddi zarar, tüm bilgi işlem hizmetlerinin zarar görmesi, veri kaybı	4	1	3	12					4	1	1	4	8
		Su baskını (binanın doğa şartlarına yetersiz oluşu)	Tüm bilgi işlem hizmetlerinin devre dışı kalması,önemli maddi zarar, kurum prestijinin zarar görmesi	5	2	2	20	C	Odanın 1 üst kata taşınması	Sistem Birimi		5	1	3	15	5
		Deprem,Yangın	Tüm bilgi işlem hizmetlerinin devre dışı kalması,önemli maddi zarar, kurum prestijinin zarar görmesi	5	1	1	5								0	5
103	Kadıköy Kampüsü Sistem odası	Fiziki güvenlik yetersizliği	Cihazların çalınması ya da zarar görmesi,yetkisiz erişim, veri kaybı.tüm bilgi işlem hizmetlerinin devre dışı	4	1	2	8								0	8
		Sistem Odası su baskını	Tüm bilgi işlem hizmetlerinin devre dışı kalması,önemli maddi zarar, kurum prestijinin zarar görmesi	4	1	1	4								0	4
		Deprem,Yangın	Tüm bilgi işlem hizmetlerinin devre dışı kalması,önemli maddi zarar, kurum prestijinin zarar görmesi	4	1	1	4								0	4
104	Mecidiyeköy Kampüsü Sistem odası	Fiziki güvenlik yetersizliği	Cihazların çalınması ya da zarar görmesi,yetkisiz erişim, veri kaybı.tüm bilgi işlem hizmetlerinin devre dışı	4	1	2	8								0	8
		Sistem Odası su baskını	Tüm bilgi işlem hizmetlerinin devre dışı kalması,önemli maddi zarar, kurum prestijinin zarar görmesi	4	1	1	4								0	4
		Deprem,Yangın	Tüm bilgi işlem hizmetlerinin devre dışı kalması,önemli maddi zarar, kurum prestijinin zarar görmesi	4	1	1	4								0	4
105	Ağ dağıtım Kabinleri kesintisiz güç kaynakları	Periyodik bakım eksikliği	Elektrik kesintisinde bölgesel oalrak tüm bilgi işlem hizmetlerine daha kısa süre destek vermesi veya hiç verememesi, cihazın arızalanması	3	2	3	18	C	Yıllık bakım sözleşmelerinin yapılması	Sistem Birimi		3	2	3	18	0
106	Projeksiyon Cihazları	Periyodik bakım eksikliği	Cihazın arızalanması	3	1	1	3								0	3
		Fiziki güvenlik yetersizliği	Cihazların çalınması ya da zarar görmesi	3	1	1	3								0	3
		Cihazın uzun süre açık bırakılması	Cihaz lamba ömrünün azalması	2	3	3	18	C	Cihazın otomatik kapanma özelliği devreye alınacak	Sistem Birimi		2	2	3	12	6
107	Personel	Kritik personel seçiminde hatalı davranılması ya da yedeğinin bulundurlumaması	Hizmetin aksaması, bilgi hırsızlığı, maddi zarar, kurum prestijinin zarar görmesi	4	1	2	8								0	8
		Donanımların veya yazılımların yanlış kullanılması	Veri kaybı, personel hataları	3	1	2	6								0	6

		İşe alımda yetersiz özgeçmiş incelemesi ve doğrulaması	Veri kaybı, kasten zarar verme	4	1	2	8								0	8
108	Tuzla Kampüsü	Fiziki güvenlik yetersizliği	Kontrolsüz giriş, yetkisiz erişim,bilgi ve cihaz hırsızlığı	4	1	2	8								0	8
109	Kadıköy MYO Binası	Fiziki güvenlik yetersizliği	Kontrolsüz giriş, yetkisiz erişim,bilgi ve cihaz hırsızlığı	4	1	2	8								0	8
110	Mecidiyeköy Enstitü Binası	Fiziki güvenlik yetersizliği	Kontrolsüz giriş, yetkisiz erişim,bilgi ve cihaz hırsızlığı	4	1	2	8								0	8
111	IK Yazılımı	Kaynak kodlardaki açıklıklar	Yetkisiz kullanım, öğrenci işlemlelerinin aksaması, bilgi hırsızlığı, maddi kayıp,kurum prestijinin zarar görmesi	3	1	2	6								0	6
		Şifre yönetimi yetersizliği	Yetkisiz kullanım, öğrenci işlemlelerinin aksaması, bilgi hırsızlığı, maddi kayıp,kurum prestijinin zarar görmesi	3	1	2	6								0	6
		Erişim izinlerinin yanlış verilmesi	Yetkisiz kullanım, öğrenci işlemlelerinin aksaması, bilgi hırsızlığı, maddi kayıp,kurum prestijinin zarar görmesi	3	1	2	6								0	6
		Dışardan firma desteği	Verilerin silinmesi ya da bilgi hırsızlığı	4	2	2	16	C	yedeklerin alınması ve firma ile yapılan sözlemeye gizlilik tahhüt maddesi eklenmesi	Sistem Birim/İnsan Kaynakları		4	1	2	8	8
112	Diş Hastanesi Yazılımı	Kaynak kodlardaki açıklıklar	Yetkisiz kullanım, öğrenci işlemlelerinin aksaması, bilgi hırsızlığı, maddi kayıp,kurum prestijinin zarar görmesi	3	1	2	6								0	6
		Şifre yönetimi yetersizliği	Yetkisiz kullanım, öğrenci işlemlelerinin aksaması, bilgi hırsızlığı, maddi kayıp,kurum prestijinin zarar görmesi	3	1	2	6								0	6
		Erişim izinlerinin yanlış verilmesi	Yetkisiz kullanım, öğrenci işlemlelerinin aksaması, bilgi hırsızlığı, maddi kayıp,kurum prestijinin zarar görmesi	3	1	2	6								0	6
		Dışardan firma desteği	Verilerin silinmesi ya da bilgi hırsızlığı	4	2	2	16	C	yedeklerin alınması ve firma ile yapılan sözlemeye gizlilik tahhüt maddesi eklenmesi	Sistem Birim/Diş hastanesi Md.lüğü		4	1	2	8	8
113	Diş Hastanesi Sunucuları	Şifre yönetimi yetersizliği	İşletim sistemi hizmetlerinin ve mali işlemlerin aksaması, bilgi hırsızlığı, maddi kayıp,kurum prestijinin zarar görmesi	4	1	3	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	1	1	4	8
		İşletim sistemi açıklıkları ve hataları	İşletim sisteminin çökmesi ve hasta kayıt işlem sürecinin aksaması	3	1	2	6		Güncelleştirmelerin zamanında ve önce test ortamında yapılması						0	6
		Anti-virus yazılımının çalışmaması,zararlı yazılımlar	Sunucu hizmetlerinin devre-dışı kalması ve veri kaybı oluşması	4	1	3	12	C	3 aylık sistem kontrol çizelgesinde gözden geçirilmesi	Sistem Birimi		4	1	1	4	8

1. AMAÇ

Erişim Yönetim Prosedürü bilgiye erişimin denetlenmesi, bilgi sistemlerine yetkisiz erişimin engellenmesi, hizmetlerin korunması, yetkisiz işlemlerin tespit edilmesi ve uzaktan çalışma ortamlarında bilgi güvenliğinin sağlanması gibi kritik konuları kapsamaktadır.

2. KAPSAM

Bu prosedür Okan Üniversitesi bünyesindeki erişim faaliyetlerini kapsar.

3. SORUMLULUK

Bilgi Güvenliği Yönetim Temsilcisi tüm erişim yönetim prosedürünün uygulanmasından sorumludur.

4. TANIMLAR

Active Directory: Etki alanı içindeki bilgisayar ve kullanıcı hesaplarının tutulduğu sistemdir.
DHCP(Dynamic Host Configuration Protocol)**:** Basit olarak sistemdeki bilgisayarlara IP adreslerini ve buna ek olarak değişik parametreleri atamak için kullanılan servistir.
OKIM: Okan Kurumsal İletişim Merkezi Programı
GKS: Geçiş Kontrol Sistemi
VLAN: Sanal Yerel Alan Ağı
Firewall: Güvenlik duvarı, tek noktadan erişim denetimi ile ağı dışarıdaki kullanıcıların istifadesine belirli izinler oranında eriştiren ve böylece dışarıdan gelebilecek yetkisiz erişim veya saldırıları önleyebilen bir sistemdir.
Switch: Bilgisayarların ve diğer ağ öğelerinin birbirlerine bağlanmasına olanak veren ağ donanımlarıdır
DMZ (Demilitarized Zone): Bir kuruluşun dış servislerini içeren ve bu servisleri daha büyük güvensiz bir ağa (genellikle internet) maruz bırakan fiziksel veya mantıksal bir alt ağdır.
Kerberos : Açık bir ağda güvenli kimlik denetimini sağlamak için şifreleme teknolojisini ve hakem olarak üçüncü bir tarafı kullanan sistem.

5. UYGULAMA

5.1. Erişim politikası

Erişim için iş ve güvenlik gereksinimlerini temel alan PO.BİS.004 İnternet Erişim ve Kullanım Politikası ve PO.BİS.010 Ağ Kullanım Politikası' nda BGYS politikaları yazılmış ve yıllık olarak gözden geçirilmektedir.

5.2. Kullanıcı erişim yönetimi

Amaç: Bilgi Sistemlerine yetkisiz erişimlerin engellenmesidir.

5.2.1. Kullanıcı Kaydı

5.2.1.1. İnsan Kaynakları Direktörlüğü, turnike geçiş kontrol sistemi (GKS), personelin etki alanı, e-posta, OKİM, kullanıcı hesabı oluşturulması ve silinmesi taleplerini bilgi işleme e-posta ile bildirir. Bilgi işlem de hesap bilgilerini e-posta ile IK' na ve ilgili personele bildirir.

5.2.1.2. Öğrenci Bilgi Sistemi, İnsan Kaynakları Bilgi Sistemi, Mali İşler Bilgi Sistemi kullanıcı hesapları ilgili müdürlüğün kontrolünde yetkili personel tarafından

yönetilmektedir.

5.2.1.3. Öğrenci e-posta hesapları talep edilmeksizin, öğrenci kaydı esnasında Öğrenci İşleri tarafından oluşturulur. Öğrenci mezun olduktan sonra otomatik olarak kapanır.

5.2.2. Ayrıcalık yönetimi

5.2.2.1. OKIM, GKS programı kullanıcı hesapları için yetki ayrıcalıkları talepleri İnsan Kaynakları tarafından bilgi işleme bildirilir.

5.2.2.2. Yerel yönetici yetkisi almak isteyen kullanıcılar FR.BİS.008 Yerel Yönetici Yetki Formu'nu doldurarak bilgi işleme başvururlar, Sistem Birim Yöneticisi başvuruyu güvenlik ve sistemin uyumluluğu açısından inceledikten sonra uygun olup olmadığına karar verir.

5.2.2.3. Özel port ve web sitesi erişimi açtırmak isteyen kullanıcılar FR.BİS.007 Ağ Erişim-İnternet-Port ve Web Sitesi Talep Formu'nu doldurarak bilgi işleme başvurur, Sistem Birim Yöneticisi başvuruyu güvenlik ve sistemin uyumluluğu açısından inceledikten sonra uygun olup olmadığına karar verir.

5.2.3. Kullanıcı parola yönetimi

Parola yönetimi PR.BİS.008 Parola Prosedürü' ne göre yapılır.

5.2.4. Kullanıcı erişim haklarının gözden geçirilmesi

Yönetim adına Bilgi Güvenliği ekibi, kullanıcıların erişim haklarını düzenli aralıklarla yapılan kontrollerde gözden geçirir.

5.3. Kullanıcı sorumlulukları

5.3.1. Parola kullanımı

Parolaların seçiminde ve kullanımında belirlenen politikalar otomatik olarak sistem tarafından kullanıcılara uygulanmaktadır. Kullanıcılar şifrelerini PR.BİS.008 Parola Prosedürü göre oluşturup, kullanmaktan sorumludur.

5.3.2 Gözetimsiz kullanıcı teçhizatı

6.3.2.1 Sistem tarafından bilgisayarların 10 dk. sonra parola korumalı ekran koruyucusuna geçmesi sağlanmaktadır.

6.3.2.2 Kullanıcılar işleri bittiği zaman bilgisayar ve diğer cihazları kapatırlar.

5.3.3 Temiz masa ve temiz ekran politikası

Kağıtlar ve taşınabilir depolama ortamları ve bilgi işleme olanakları için PO.BİS.0012 Temiz Masa ve Temiz Ekran Politikası kullanılmaktadır.

5.4. Ağ erişimi

5.4.1. Ağ hizmetlerinin kullanımına ilişkin politika

5.4.1.1. Kullanıcıların sadece kullanımlarına yetki verilen hizmetlere erişime sahip olması için Active Directory Windows kimlik doğrulama sistemi kullanılır.

5.4.1.2. PO.BİS.009 Ağ Yönetim ve PO.BİS.010 Ağ Kullanım Politikaları' nda ilgili hususlar belirtilmiştir

5.4.2 Dış bağlantılar için kullanıcı kimlik doğrulama

5.4.2.1 Dış bağlantılar için kullanıcı kimlik doğrulama işlemi Firewall üzerinde oluşturulan kullanıcı hesapları ile sağlanır.

5.4.3 Ağlarda Cihaz Kimliği Belirleme

5.4.3.1. Yeni bir Ağ anahtarı veya kablosuz ağ cihazı sisteme dahil edilirken, bulunduğu konuma göre isimlendirilip, etiketlenir ve fiziksel adresleri ve seri numaraları ile envantere kaydedilir.

5.4.3.2. Bilgisayar ve diğer donanımlar sisteme dahil edilirken birimlere ait isimlendirme listesi LS.BİS.008 İsim Listesi 'ne göre isimlendirilir ve envantere kaydedilir.

5.4.3.3. Otomatik IP kullanan cihazların fiziksel adresleri cihaz kimliği belirleme metodu olarak kullanılır.

5.4.4 Uzak tanı ve yapılandırma portu koruma

5.4.4.1 Uzak tanı ve yapılandırma portlarına erişimler kısıtlanmış ve şifre koruması uygulanmıştır.

5.4.5 Ağlarda ayrım

5.4.5.1 Ağlarda, bilgi hizmetlerinin, kullanıcıların ve bilgi sistemlerinin gruplarını ayırmak amacıyla farklı VLAN' lar oluşturulmuştur.

5.4.5.2 VLAN' lar Omurga switch üzerinde tanımlanmaktadır ve IP adresi dağıtımı DHCP tarafından yönetilmektedir.

5.4.5.3 Yeni VLAN tanımları sistem yöneticisi tarafından omurga switch üzerinde tanımlanır ve otomatik IP dağıtılacaksa DHCP üzerinde yeni Scope açılarak hizmete sunulur.

5.4.6 Ağ bağlantı Kontrolü

5.4.6.1 Okan Üniversitesi internet ortamından erişilen sistemleri uygulamaların gereksinimlerine uygun olarak sınırlandırılmaktadır.

5.4.6.2 DMZ'de www.okan.edu.tr adresinden yayın yapan kurumsal web sitesi, mail.okan.edu.tr adresinden yayın yapan kurumsal e-posta servisi *.okan.edu.tr subdoaminlerinde yayın yapan web siteleri ve kurumsal uygulama sunucuları için gerekli port erişimleri açılmıştır.

5.4.6.3 Portlarda meydana gelen her hareket firewall tarafından kayıt altına alınmaktadır.

5.4.6.4 Yeni açılacak olan internet servisleri yada uygulamaları için gerekli port tanımları firewall kuralları ile sistem yöneticisi tarafından yapılmaktadır.

5.4.7 Ağ yönlendirme

5.4.7.1 VLAN'lar arası haberleşme omurga switch üzerinde tanımlanan erişim listeleri ile bilgisayar bağlantılarının ve bilgi akışlarının erişim politikasını ihlal etmemesini sağlamak için yönetilmektedir.

5.4.7.2 Erişim yetkisi isteyen kullanıcılar FR.BİS.007 Ağ Erişim-İnternet Port ve Web Sitesi

Talep Formu'nu doldurarak bilgi işleme başvurur.

5.5 İşletim sistemi erişim

5.5.1 Güvenli oturum açma prosedürleri

5.5.1.1. İşletim sistemlerine erişim etki alanı kullanıcı adı ve şifresi ile sağlanmaktadır.

5.5.1.2. Girilen şifre, şifreli olarak etki alanı denetleyici sunucusuna gönderilir ve kontrol edilerek sisteme giriş izni verilir.

5.5.1.3. Etki alanına bağlı olmayan bilgisayarlarda sınırlı yerel kullanıcı acı ve şifresi ile oturum açılır.

5.5.2 Kullanıcı kimlik tanımlama ve doğrulama

Tüm kullanıcılar yapılan işlemlerin sonradan sorumlu bireyler kapsamında izlenmesi için active directory üzerinden benzersiz (isim.soyisim) bir kimlik alır ve bir kullanıcının öne sürdüğü kimliğini ispatlamak için kerberos kimlik doğrulama tekniği kullanılır.

5.5.3 Parola yönetim sistemi

Parola yönetim sistemleri PR.BİS.008 Parola Prosedüründe tanımlanmıştır.

5.5.4 Oturum zaman aşımı

Web tabanlı uygulamalar için etkin olmayan oturumlar 10 dakikalık hareketsizlik süresinden sonra kapatılır. Windows uygulamalarında zaman aşımı otomatik değildir. Programı kapatmak kullanıcının sorumluluğundadır.

5.5.5 Bağlantı süresinin sınırlandırılması

Bağlantı sürelerinde sınırlandırmalar, yüksek riskli uygulamalara ek güvenlik sağlamak için kullanılmaktadır. Kullanıcıların çok riskli bilgi içeren noktalarda gerek görülürse bağlantı süresi sınırlandırılır.

5.6 Uygulama ve bilgi erişim

5.6.1 Bilgi erişim kısıtlaması

Kullanıcılar ve destek personeli tarafından bilgi ve uygulama sistem işlevlerine erişim, tanımlanmış erişim politikasına uygun olarak kısıtlanmaktadır.

5.6.2 Hassas sistem yalıtımı

Okan Üniversitesi için her bilgi mahrem ve hassas olduğu kabul edilerek, sistemlerimiz dış dünyadan Firewall ve IPS güvenlik cihazları ile korunmaktadır. PR.BİS.007 Kötü Niyetli Yazılımlara Karşı Koruma Prosedürü 'nde ilgili hususlar belirtilmiştir.

5.7 Uzaktan çalışma

5.7.1. Okan Üniversitesi dışından bilgi sistemlerine bağlanmak için SSL VPN kullanılır.

5.7.2. Kişisel ya da hizmet aldıkları firma için uzaktan bağlantı talebinde bulunan kullanıcılar FR.BİS.009 Uzak Erişim Talep Formu' nu doldurarak bilgi işleme başvururlar.

5.7.3. SSL VPN bağlantısı cep telefonları, tablet PC'ler, masaüstü ve dizüstü bilgisayarlarda çalışabilmektedir.

5.7.4. Firewall üzerinde açılan VPN erişim adresine bağlanılarak VPN kullanıcı adı ve şifresi ile sisteme giriş yapılır.

5.7.5. İlk girişten sonra bilgisayara bir defalığına bir program yüklenecektir. Bu programın yüklenebilmesi için pop-up engelleyicisine izin verilmeli ve bu kurulum sırasında kuruluma onay verilmelidir.

5.7.6. VPN bağlantısı sağlandıktan sonra yetki verilen uygulama veya sunucuya , yetki verildiği düzeyde erişim yapılabilir.

5.7.7. Periyodik olarak yapılan kontrollerde, üniversiteden ilişiği kesilmiş veya görevi değişmiş kullanıcı veya firma hesapları ile kaldırılmalıdır.

6. KAYITLAR

-Yerel Yönetici Yetki Formu FR.BİS.008
-Ağ Erişim-İnternet Port ve Web Sitesi Talep Formu FR.BİS.007

7. REVİZYONLAR

1. AMAÇ

Okan Üniverstesi bünyesinde oluşturulan Yönetim Sistemleri doğrultusunda, bilgi işleme olanaklarının doğru ve güvenli işletimini sağlamak

2. KAPSAM

Oluşturulan Yönetim Sistemi içerisinde tüm birim çalışanlarını kapsar.

3. SORUMLULUK

Bu prosedürün uygulanmasından tüm birimler, hazırlanmasından ve kontrolünden Bilgi Güvenliği Ekibi sorumludur

4. TANIMLAR

Aktif Dizin: Etki alanı içindeki bilgisayar ve kullanıcı hesaplarının tutulduğu sistemdir.

Firewall: Güvenlik Duvarı, tek noktadan erişim denetimi ile ağı dışarıdaki kullanıcıların istifadesine belirli izinler oranında eriştiren ve böylece dışarıdan gelebilecek yetkisiz erişim veya saldırıları önleyebilen bir sistemdir.

vCenter: Sanallaştırma Programı Adı

5. UYGULAMA

5.1 Operasyonel prosedürler ve sorumluluklar

5.1.1 İşletim prosedürleri

İşletim prosedürleri int.okan.edu.tr paylaşımında tüm kullanıcıların erişimine açılmıştır. Bilgi Güvenliği Yönetim Temsilcisi ilgili sistemlerin işletim prosedürlerini temin eder ve gerektiğinde güncellenmesi talimatını verir.

5.1.2 Değişim yönetimi

Bilgi işleme olanakları ve sistemlerinde olan değişiklikler PR.BİS.016 Bilgi Sistemleri Edinim Geliştirme Bakım Ve Uyum Prosedürüne göre kontrol edilmektedir.

5.1.3 Görev ayrımları

Kuruluşun varlıklarının yetkisiz veya farkında olmadan değiştirilme ya da kötüye kullanılma fırsatlarını azaltmak için, görevler ve sorumluluk alanları görev tanımlarında yazılmıştır.

5.1.4 Geliştirme, test ve işletim olanaklarının ayrımı

5.1.4.1. Geliştirme, test ve işletim olanakları, işletilen sisteme yetkisiz erişim veya değişiklik risklerini azaltmak için ayrılmaktadır.

5.1.4.2. Öğrenci Bilgi Sistemi için yazılımsal değişiklikleri önce test sisteminde danışman firma tarafından yapılır ve uygunluğu Öğrenci İşleri Müdürü tarafından onaylandıktan sonra danışman firma tarafından canlı sisteme taşınılır

5.1.4.3. Muhasebe Yönetim Sistemi için yazılımsal değişiklikleri önce test sisteminde danışman firma tarafından yapılır ve uygunluğu Mali İşler Müdürü tarafından onaylandıktan sonra danışman firma tarafından canlı sisteme taşınılır.

5.1.4.4. Web sitesinde kullanıcıların sadece kendi üniteleri ile ilgili değişiklik yapma yetkisi vardır. Yazılımsal ve data değişiklikleri önce test sisteminde yapılır ve uygunluğu Yazılım Birim yöneticisi tarafından onaylandıktan sonra bu personel tarafından canlı web sitesine taşınılır.

5.1.5. Otorite İletişim Yöntemleri

Otorite İletişim Yöntemleri e-posta ve OKİM(Okan İletişim Merkezi) ile yapılmakta olup, iletişim kayıtları tutulmaktadır.

5.2 Üçüncü Taraf Hizmet Sağlama Yönetimi

Amaç: Üçüncü taraf hizmet sağlama anlaşmalarıyla uyumlu olarak uygun bilgi güvenliği ve hizmet dağıtımı seviyesi gerçekleştirmek ve sürdürmek.

5.2.1 Hizmet sağlama

5.2.1.1 Hizmet tanımları üçüncü taraflarla yapılacak sözleşmelerde detaylandırılır.

5.2.1.2 Üçüncü taraflar ile yapılan sözleşmelerde gizlilik ve güven ile ilgili taahhütler yer alır.

Sözleşmelere eklenecek taahhüt maddesi aşağıdaki gibidir.

GİZLİLİK TAAHHÜDÜ

İşbu sözleşmede aksi yazılı olarak belirtilmediği sürece, Taraflar arasında görüşmeler yapıldığı veya Taraflar arasındaki işbu Sözleşme veya diğer sözleşmelerin mevcut olduğu bilgisi ve tarafların niyetleri de dâhil olmak üzere, ÜNİVERSİTE'nin işbu Sözleşme veya Taraflar arasında akdedilen her türlü sözleşme ve/veya iş nedeniyle bu Sözleşme'nin imzalanmasından önce veya sonra edindiği ÜNİVERSİTE ile doğrudan yada dolaylı olarak ilgili, yazılı, sözlü, görsel, işitsel ve/veya herhangi bir formdaki her türlü veri, bilgi ve belge Gizli Bilgi sayılacaktır.

Ancak, gizlilik yükümlülüğü olmadığı ÜNİVERSİTE tarafından yazılı olarak belirtilmek suretiyle Taraflarca birbirlerine verilen, işbu Sözleşme'nin imzalanmasından önce kamuya mal olmuş bulunan, işbu Sözleşmenin imzalanmasından sonra Sözleşme'nin ihlali sonucunu doğurmaksızın kamuya mal olan veya bilginin ifşa edildiği tarihten önce diğer tarafça bilinen veya bağımsız olarak geliştirilen ve bu şekilde bilindiği veya geliştirildiği yazılı belge ile kanıtlanabilen bilgiler Gizli Bilgi kapsamına girmez.

İşbu sözleşme kapsamında diğer taraf,
-Gizli Bilgi'yi uygun şekilde almayı ve büyük bir gizlilik içinde korumayı,
-Gizli Bilgi'yi Taraflar arasındaki hukuki ilişkinin amacının gerçekleştirilmesi dışında, her ne surette olursa olsun doğrudan veya dolaylı olarak başkaca hiç bir amaç için kullanmayacağını,
-Gizli Bilgi'yi diğerinin yazılı izni olmadan ve mahkeme kararı, istisna olmak kaydıyla, hangi suretle olursa olsun üçüncü şahıs ya da kurumlara açıklamayacağını ve üçüncü şahıslarca kullanımına ve/veya kopya edilmesine izin vermeyeceğini,
-Gizli Bilgi'nin istihdam ettiği personel, vekiller, ilgili taraf adına hareket eden gerçek veya tüzel kişiler tarafından da korunacağını, Sözleşmeden doğan yükümlülüklerin yerine getirileceğini ve aksi halde doğacak sonuçlardan bizzat sorumlu olacağını,
-ilgili tarafın Mahkeme kararı, kanun, tüzük, yönetmelik uyarınca Gizli Bilgi'yi açıklamak zorunda kalması halinde, aksine hareket yürürlükteki mevzuat gereği men edilmedikçe, durumu karşı tarafa derhal yazılı olarak bildireceğini ve mahkeme kararı veya mevzuatın gerektirdiği asgari açıklamayı yaparken verilen bilgilerin gizli kalması için gereken özeni göstereceğini

İlgili tarafın talebi halinde Gizli Bilgi'nin orjinalini, kopyalarını, diğer reprodüksiyonlarını ve özetlerini (diğer tarafça hazırlanmış olsun veya olmasın),gerekli tüm belgeleri derhal iade edeceğini,

İlgili tarafın, işbu Sözleşme'de yer alan yükümlülüklerini ihlal etmesi halinde diğer tarafın ihlal eden taraf aleyhine ihtiyati tedbir dahil her türlü kanun yollarına başvurmak ve sair her türlü hukuki ve fiili tedbirleri almak hakkını haiz bulunduğunu gayrı kabili rücu kabul ve taahhüt eder.

5.2.1.3 Hizmet tanımları ve koşulları hizmeti talep eden birim tarafından belirlenir ve Bilgi Güvenliği Yönetim Temsilcisi tarafından kontrol edilir.

5.2.1.4 Hizmet tanımları, gizlilik ve güvenlik koşullarının yer aldığı anlaşmalar hizmeti sunacak üçüncü taraf tarafından onaylanır.

5.2.1.5 Hizmeti talep eden birim, üçüncü tarafça sağlanan hizmetin gerçekleştirilmesini sözleşmelerde detaylandırıldığı şekli ile takip eder.

5.2.1.6 Üçüncü taraf hizmet sağlayıcısı, sağlanan hizmet ile ilgili bilgi ve dokümantasyonu hizmet talebi yapan birim ile paylaşır ve hizmetin işletilmesi ile ilgili eğitimi verir.

5.2.1.7 Hizmetin işletilmesi hizmet talebi yapan birim tarafından sağlanır.

6.2.2 Üçüncü Taraf Hizmetleri İzleme ve Gözden Geçirme

6.2.2.1. Üçüncü tarafa sağlanan hizmetler, sözleşmelerde tanımlandığı şekli ile sağlanır.

6.2.2.2. Sözleşmelerde yer alan maddeler BGYS politikaları çerçevesinde oluşturulur ve uygulanır.

6.2.2.3. Üçüncü tarafa sağlanan hizmetler, raporlar ve kayıtlar düzenli olarak talebi yapan birim tarafından izlenir, gözden geçirilir ve denetimler gerçekleştirilir.

6.2.3 Üçüncü Taraf Hizmetlerdeki Değişiklikleri Yönetme

Üçüncü taraf hizmet koşullarında değişiklik olması durumunda, ilgili iş sistemleri ve süreçlerin kritikliğini ve risklerin yeniden değerlendirmesini hesaba katarak, değişiklik süreci hizmeti talep eden birim tarafından yönetilir.

6.3 Sistem Planlama ve Kabul

Amaç: Sistem başarısızlıkları riskini en aza indirmek.

6.3.1 Kapasite Planlama

6.3.1.1. Her yıl düzenli olarak Bilgi İşlem Müdürü, Bilgi İşlem Yöneticisi/Md.Yrd.'nın ve birim yöneticilerinin katıldığı bir toplantıda bir sonraki yıl için gerekli sistem performansını sağlamak, yeni sistemler ile mevcut sistemi geliştirmek, mevcut kaynakların kullanımı izlemek ve iyileştirmek için bir sonraki seneye kapasite gereksinimleri ortaya çıkarılır.

6.3.1.2. Gereksinimleri karşılamak için projeler oluşturulur ve projelerin mümkünse demo çalışması mutlaka yaptırıldıktan sonra bütçe planına eklenir.

6.3.2 Sistem Kabulü

6.3.2.1. Yeni bilgi sistemleri, sistem yükseltmeleri ve yeni sürümler için kabul kriterleri proje şartnamesinde belirlenir.

6.3.2.2. Proje şartnamesine uygun olarak yapılan projeden sonra geçici kabul ve kabul öncesinde sistem(ler)e ilişkin uygun testler bilgi işlem tarafından ilgili firma ile beraber gerçekleştirilir.

6.3.2.3. Testlerden başarı ile geçen projeler kabul edilir.

6.4 Kötü Niyetli ve Mobil Koda Karşı Koruma

Amaç: Yazılım ve bilginin bütünlüğünü korumak.

6.4.1 Kötü Niyetli Koda Karşı Kontroller

Kötü niyetli koda karşı korunmak için saptama, önleme ve kurtarma kontrolleri Kötü Niyetli Yazılımlara Karşı Koruma Prosedürüne göre gerçekleştirilir.

6.4.2 Mobil koda karşı kontroller

Mobil kod uygulaması yapılmamaktadır.

6.5 Yedekleme

Amaç: Bilgi ve bilgi işleme olanaklarının bütünlüğünü ve kullanılabilirliğini sağlamak.

6.5.1 Bilgi Yedekleme

Bilgi ve yazılımlara ait yedekleme kopyaları PR.BİS.014 Yedekleme Prosedürüne göre alınmakta ve bu yedekleme politikasına uygun şekilde muhafaza edilmektedir.

6.6 Ağ Güvenliği Yönetimi

Amaç: Ağdaki bilginin ve destekleyici alt yapının korunmasını sağlamak.

6.6.1 Ağ Kontrolleri

Tehditlerden korunmak ve iletilmekte olan bilgi dahil ağı kullanan sistemler ve uygulamalar için güvenliği sağlamak amacıyla Okan Üniversitesi ağı Firewall ve Saldırı Engellemi Sistemi ile korunmaktadır.

6.6.2 Ağ Hizmetleri Güvenliği

Ağ hizmetleri güvenliği, "PR.BİS.001 Ağ ve Sistem Yönetim Prosedürü ve PO.009 Ağ Yönetimi Politikası'nda tanımlanmıştır.

6.7 Ortam İşleme

Amaç: Varlıkların yetkisiz ifşa edilmesi, değiştirilmesi, kaldırılması veya yok edilmesini ve iş faaliyetlerinin kesintiye uğramasını önlemek.

6.7.1 Taşınabilir Ortam Yönetimi

Hırsızlık ve yetkisiz kişilerin erişimine karşı taşınabilir bilgisayarlarda işletim sistemi erişimi etki alanı kullanıcı adı ve şifresi ile sağlanmaktadır. Taşınabilir bilgisayar ve usb disklerde ÇOK GİZLİ kategorisine giren belge saklanmaması kullanıcı sorumluğundadır.

ÇOK GİZLİ kategorisine giren yazılı belgeler, cihazlar, diskler, kasetler, kilitli dolaplarda saklanır.

6.7.2 Ortamın Yok Edilmesi

Taşınabilir , masa üstü bilgisayarlar ve sunucuların arızalanması durumunda cihaza boş disk

takılarak teknik servise gönderilir.

Diskin gönderilmesi zorunlu olduğu durumlarda disk üzerine 3 kere yazma metodu kullanılarak silindikten sonra gönderilir .Cihazların elden çıkarılması durumunda disk parçalanarak imha edildikten sonra depoya geri dönüşüm için teslim edilir. İmha işlemleri Donanım, sistem birim yöneticileri ve bilgi işlem uzmanından oluşan 3 kişilik heyet tarafından FR.BİS.015 İmha Formu doldurularak kayıt altına alınır.

6.7.3 Bilgi İşleme Prosedürleri

Bu tür taşınılabilir ortamlarda bulunan bilgileri yetkisiz ifşa etmeye ya da kötüye kullanmaya karşı korumak için kullanıcı personel gerekli güvenlik tedbirlerini alır.

6.7.4 Sistem Dokümantasyonu Güvenliği

Sistem dokümantasyonu aktif dizin kullanıcı hesabı ile kimlik doğrulama yapılarak sağlanmaktadır. Böylelikle yetkisiz erişime karşı korunmaktadır.

6.8 Bilgi Değişimi

Bilgi Değişimi şu anda uygulanmamaktadır.

6.9 Elektronik ticaret hizmetleri

Elektronik ticaret mevcut değildir.

6.10 İzleme

Amaç: Yetkisiz bilgi işleme faaliyetlerini algılamak.

6.10.1 Denetim kaydetme

6.10.1.1. İnternet ve sunucular üzerindeki kullanıcı faaliyetleri, ayrıcalıkları ve bilgi güvenliği olayları log (crypto log) sunucu'da ve her sunucu üzerinde olay kaydedicisinde tutulmaktadır. Yazılımlar üzerindeki kullanıcı faaliyetleri yazılımın kendi takip aracı ile yapılmaktadır.İnternet kayıtları istenildiği takdirde verilmek üzere yasal süre olan 6 ay saklanmaktadır.

6.10.2 Sistem kullanımını izleme

6.10.2.1. Sunucu kullanımını izlemek için vmware vCenter uygulaması kullanılır. Bu uygulama ile sistem üzerinde sanal makinelerde ihtiyaç olan donanım kaynakları belirlenebilir ve yeterli kaynağın olması durumunda kaynak eklemesi yapılabilir. Sistemlere erişim her sistemin kendi olay kaydedicisi üzerinden takip edilmektedir.

6.10.2.2. Uygulama bazında sistem kullanımını görmek için uygulamaların kendi izleme yazılımlarından faydalanılır.

6.10.3 Kayıt bilgisinin korunması

Kayıt olanakları ve kayıt bilgisi yetkisiz erişime karşı Erişim Prosedürüne göre korunur.

6.10.4 Operatör kayıtları

Sistemin açılma kapanma zamanı, kayıt girişi yapan personelin kimlik bilgileri, işlem kayıtları kullanılan sistemin günlük kaydedicisinde tutulur.

6.10.5 Hata kaydı

Kullanıcılar tarafından bildirilen ve sistemde oluşan hatalar , bu hataların giderilme yolları ve düzeltici tedbirler LS.BİS.011 Hata Takip Listesi'nde ilgili birim yöneticileri tarafından kayıt altına alınır.

6.10.6 Saat senkronizasyonu

Okan üniversitesi etki alanındaki tüm ilgili bilgi işleme sistemlerinin saatleri, Microsoft time server ile senkronize edilir.

7. KAYITLAR

- İmha Formu FR.BİS.015
- Hata Takip Listesi LS.BİS.011

8. REVİZYONLAR

15 Nisan 2015 tarihinde Rev01 olarak güncellendi.

1. AMAÇ

Bu prosedürün amacı Okan Üniversitesi Bilgi Güvenliği Yönetim Sistemi kapsamında ağ güvenliği, ağ ve sistem yönetimi ve ağ cihazları işletimi hakkında kuralları oluşturmaktır.

2. KAPSAM

Bu prosedür Okan Üniversitesi bilgi işlem ağı ve sistemi hizmetlerini kullanan bütün personel ve öğrencileri kapsar.

3. SORUMLULUK

Bu prosedürün uygulanmasından Bilgi İşlem Müdürlüğü, denetim ve takibinden BGYS ekibi sorumludur.

4. TANIMLAR

BGYS: Bilgi Güvenliği Yönetim Sistemi
VLAN: Sanal yerel alan ağı
İnternet: Geniş alan ağı
İntranet: Yerel alan ağı
Port: Sanal,yazılımsal bağlantı noktası
Active Directory: Etki alanı içindeki bilgisayar ve kullanıcı hesaplarının tutulduğu sistemdir.
Domain: Etki alanı, dizin sistemiyle yönetilen ağ sistemine domain adı verilir
VPN (Virtual Private Network - Sanal Özel Ağ): Bu ağı kullanacak bir Firewall ile iki uç arasında bir kanal oluşturmak ve bu kanala girecek verilerin şifrelenmiş paketler halinde seyahatini sağlayarak yetkisiz kişilerin kullanımına engel olma sistemidir.
Güvenlik Duvarı (Firewall): Güvenlik duvarı, tek noktadan erişim denetimi ile ağı dışarıdaki kullanıcıların istifadesine belirli izinler oranında eriştiren ve böylece dışarıdan gelebilecek yetkisiz erişim veya saldırıları önleyebilen bir sistemdir.
Switch: Bilgisayarların ve diğer ağ öğelerinin birbirlerine bağlanmasına olanak veren ağ donanımıdır.
Community String: Aktif ağ cihazları hakkında bilgi toplanırken cihazlar arasında kullanılan anahtardır.

5. UYGULAMA

5.1 Sunucu ve ağ cihazlarının iş sürekliliğini sağlamak ve performans ölçümünü yapmak için kullanılan izleme yazılımlarının raporları bilgi işlem personeline ilgili yazılım tarafından gönderilir. Bilgi işlem personeli ilgili raporları takip eder, olağan dışı durumların nedenini araştırır ve gerekli tedbirlerin alınmasını sağlar.

5.2 Kullanıcı bilgisayarlarının ve cihazlarının LS.BİS.001 Sanal Ağ Listesi'ne göre sisteme erişmesi sağlanır.

5.3 Ağ cihazları ve sunucu erişim adresleri, ağa ait konfigürasyon bilgileri, SNMP community stringleri ve şifreleri bilgi işlem personeli tarafından sadece erişimi yetkilendirilmiş sunucu ve yedekleme alanlarında bulundurulur.

5.4 Bütün ağ cihazları ve sunuculara ait envanter bilgileri (IP,Seri-No,Konum,Marka/Model) envanter yönetim sisteminde güncel olarak kayıt altına alınır.

5.5 Ağ anahtarına uzaktan erişim sadece Telnet protokolü ile şifreli olarak sağlanır.

5.6 Her konfigürasyon değişikliğinden önce ağ cihazları konfigürasyonlarının mutlaka yedeği alınır.

5.7 Kullanıcı cihazlarının bağlı olduğu switch portlarında kimlik doğrulama protokolü uygulanır.

5.8 Active Directory kullanıcı kayıtları yapılırken, kullanıcıya ait imza bilgileri eksiksiz olarak doldurulur ve kayıt oluşturma bilgileri bir dokümana kaydedilir.

5.9 Personel e-posta hesapları kapatılırken, önce 1 ay süre ile devre dışı bırakılır daha sonra silinir ve silme tarihi bir dokumana kaydedilir.

Hazırlayan	Onaylayan
BGYS Ekip Lideri	Yönetim Temsilcisi

5.10 Etki alanına dahil edilecek bilgisayarların isimleri daha önceden belirlenmiş isim standardında olmalıdır, standart dışı bilgisayarlar etki alanından silinir.

5.11 Active Directory'de kullanıcı ve bilgisayarlara uygulanan grup politikaları tüm sisteme uygulanmadan önce mutlaka test ortamında çalıştırılmalıdır.

5.12 Kullanıcı ve bilgisayar hesapları bağlı oldukları birimin Active directory organizasyon ünitesi altında tutulmalıdır.

5.13 3 aydan fazla süre kullanılmayan bilgisayar hesapları ile 6 aydan fazla kullanılmayan kullanıcı hesaplarının sistem tarafından otomatik devre dışı bırakılması sağlanır.

5.14 Kullanıcı bilgisayarlarında standart yerel yönetici kullanıcı adı devre dışı bırakılır. Farklı bir yerel kullanıcı adı oluşturularak yönetici grubuna dahil edilir. Kullanıcılar bilgisayarlarda standart kullanıcı grubundadır.

5.15 Tuzla kampüsü Kadıköy ve Mecidiyeköy kampüslerine VPN bağlantısı ile kriptolu olarak bağlanmaktadır.

5.16 Okan dosya sunucusu üzerinde Departman' lar için klasörlere erişim sadece departmanın güvenlik grubuna verilir.

5.17 Bilgi Sistemleri ağ, cihaz ve yazılımları en az 3 ayda bir Sistem ve Yazılım Birim Yöneticisi tarafından kontrol edilir, FR.BİS.016 Sistem Kontrol Formu doldurularak kayıt altına alınır.

5.18 Sunucu güncelleştirmeleri 3 ayda bir Sistem ve Yazılım Birimi tarafından FR.BİS.021 Sunucu Güncelleştirme Takip Formu doldurularak kayıt altına alınır.

6. KAYITLAR

Sistem Kontrol Formu	FR.BİS.016
Sunucu Güncelleştirme Takip Formu	FR.BİS.021

7. REVİZYONLAR

19 Haziran 2015 tarihinde Rev01 olarak güncellendi.

Hazırlayan	Onaylayan
BGYS Ekip Lideri	Yönetim Temsilcisi

PO.BİS.003 PERSONEL GÜVENLİĞİ POLİTİKASI

1. AMAÇ

Üniversitenin bilgi varlıklarının güvenliğinin sağlanması, çalışanlarının bu konuya duyarlı olması, bilinç seviyeleri, kendilerine verilen yetki ve sorumlulukları iyi anlamaları ve yerine getirmeleriyle çok yakından bağlantılıdır.

İlgili personelin seçimi, sorumluluk ve yetkilerinin atanması, eğitilmesi ve iş akdinin feshi gibi konuların bilgi güvenliği ile ilgili boyutunun ne şekilde ele alınacağını bu politika belirler.

2. KAPSAM

Personel Güvenlik Politikası, tüm idari, akademik ve sözleşmeli personeli kapsamaktadır.

3. POLİTİKA

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

3.2 Yetkisi olmayan personelin, üniversitedeki gizli ve çok gizli bilgileri görmesi veya elde etmesi yasaktır.

3.3 Bilgi sistemlerinde sorumluluk verilecek kişinin özgeçmişi araştırılmalı, beyan edilen akademik ve profesyonel bilgiler teyit edilmeli, karakter özellikleriyle ilgili tatmin edici düzeyde bilgi sahibi olmak için iş çevresinden ve dışından referans sorulması sağlanmalıdır.

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

3.5 Akademik ve İdari personelin gizlilik taahhütleri ve internet erişimi yasal sorumlulukları hizmet sözleşmesinde bulunmaktadır.

3.6 Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenmelidir.

3.7 İş tanımı değişen veya üniversiteden ayrılan kullanıcılar, bilgi işlem departmanına Insan Kaynakları tarafından bildirilmeli ve erişim hakları revize edilmeli veya silinmelidir.

3.8 Üniversite bilgi sistemlerinin işletilmesinden sorumlu personelin, konularıyla ilgili teknik bilgi düzeyini güncel tutması çalışma sürekliliği açısından önemli olduğundan, eğitim planlamaları periyodik olarak yapılmalı, bütçe ayrılmalı, eğitimlere katılım sağlanmalı ve eğitim etkinliği değerlendirilmelidir.

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

3.10 Kritik süreçler tek bir çalışana bağlı bırakılmamalı ve silsile yolu üzerinde, her kritik süreç için o sürece hakim bir çalışan daha bulundurulmalıdır.

3.11 Çalışanlar kendi işleri ile ilgili olarak bilgi güvenliği sorumlulukları, riskler, görev ve yetkileri hakkında periyodik olarak eğitilmelidir. Yeni işe başlayan personele bu eğitim İnsan Kaynakları oryantasyon eğitimi içinde verilmelidir.

PO.BİS.004 İNTERNET ERİŞİM VE KULLANIM POLİTİKASI

1.AMAÇ

Üniversitenin güvenli internet erişimi için sahip olması gereken standartları belirlemektir.

2.KAPSAM

İnternetin uygun olmayan kullanımı, kurumun yasal yükümlülükleri, kapasite kullanımı ve kurumsal imajı açısından istenmeyen sonuçlara neden olabilir. Bilerek ya da bilmeyerek bu türden olumsuzluklara neden olunmaması ve internetin kurallarına, etiğe ve yasalara uygun kullanımının sağlanmasını amaçlanmaktadır. Bu politika Okan Üniversitesi'nin bütün kullanıcılarını kapsamaktadır.

3.POLİTİKA

Bütün kullanıcılar ve Sistem yöneticileri aşağıdaki internet erişim ve kullanım yönteminden dışarıya çıkmamalıdır.

3.1 Kurumun bilgisayar ağı erişim ve içerik denetimi yapan bir ağ güvenlik duvarı üzerinden internete çıkacaktır. Ağ güvenlik duvarları kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır. Ağın dışından ağın içine erişimin denetimi buradan yapılır. Güvenlik duvarı aşağıda belirtilen hizmetlerle birlikte çalışarak ağ güvenliğini sağlayabilmelidir.

3.2 Kurumun ihtiyacı doğrultusunda içerik filtreleme sistemleri kullanılır. İstenilmeyen siteler yasaklanır.

3.3 Kurumun ihtiyacı doğrultusunda saldırı tespit ve önleme sistemi kullanılır. Saldırı tespit ve önleme sistemi (IPS); şüpheli olayları, nüfuz ve saldırıları tespit etmeyi hedefleyen bir sistemdir. IPS, şüpheli durumlarda e-posta veya sms gibi yöntemlerle sistem yöneticisini uyarabilmektedir.

3.4 Anti-virüs gateway sistemleri kullanılır. İnternete giden veya internetten gelen bütün trafik virüslere karşı taranır.

3.5 Ancak yetkilendirilmiş sistem yöneticileri, internette bütün servisleri kullanma hakkına sahiptir. (ftp,telnet)

3.6 Genel ahlak anlayışına aykırı, suç teşkil eden internet sitelerine girilemez ve dosya indirimi yapılamaz.

3.7 Üçüncü şahısların kurum internetini kullanmaları HotSpot sistemi ile sağlanır.HotSpot; Cep telefonuna SMS göndererek kimlik doğrulaması yapan sistemdir.

3.8 Kablolu ve kablosuz internet erişiminde öğrenci ve tüm personelin internete erişimleri kimlik doğrulama sistemi kullanılarak sağlanır.

3.9 Öğrenci, tüm personel ve üçüncü şahısların internete çıkışları 5651 sayılı kanuna göre kayıt altına alınır ve bu kayıtlar en az 6 ay süreyle saklanır. Yasa maddelerine aykırı hareket eden kullanıcı yasal olarak bizzat kendisi sorumludur.

PO.BİS.010 AĞ KULLANIM POLİTİKASI

1. AMAÇ

Okan Üniversitesi ağ hizmetlerini kullanan tüm kullanıcılara uygulanan kuralları tanımlamaktır.

2. KAPSAM

Bu politika Okan Üniversitesindeki tüm kullanıcıları kapsamaktadır.

3. UYGULAMA

Yerel Alan Ağı, Okan Üniversitesi dahilinde bölüm, birim, bina ve kampüs düzeyinde bilişim kaynaklarını bir ağ yapısı ile birbirine bağlayan ve internet erişimini sağlayan ağdır. Okan Üniversitesi öğrencilerine, idari, akademik ve sözleşmeli personeline internet ve yerel alan ağı hizmeti vermektedir. Bu hizmetin kullanım önceliği idari faaliyetler ve eğitim amaçlı araştırma ve geliştirme faaliyetler içindir. Ağ güvenliğinin sağlanması ve daha etkin kullanımı için tüm kullanıcıların aşağıda belirtilen kurallara uymaları gerekmektedir.

3.1 Okan Üniversitesi İnternet ve Yerel Alan Ağına, ticari olan veya olmayan, ücret karşılığı ya da ücretsiz, yetki verilmemiş herhangi bir üçüncü kişi veya kuruluşun erişimi sağlanamaz.

3.2 Okan Üniversitesi İnternet ve Yerel Alan Ağını kullanan bölüm veya birimler bu kaynakların kullanımı ile ilgili sorumluluğu üstlenmiş sayılırlar. Kullanıcıların yarattığı giriş ve çıkış trafiğinden sorumludurlar. Bu konuda sorun yaşandığında Bilgi Güvenliği Ekibin'den gelen uyarıları değerlendirip, aykırı ve istenmeyen trafiği yaratan kullanıcı (personel veya öğrenci) uyarılmalıdır.

3.3 Bölüm veya birimler Bilgi İşlem'in binalarda kurduğu kablolama sistemi, ağ erişim cihazları ve diğer teçhizat üzerinde yazılım veya donanım düzeyinde değişiklikler yapmamalı, ihtiyaç durumunda Bilgi İşlem ile irtibata geçerek gerekli değişiklikler karşılıklı bilgilendirme ve onay sonucunda yapılmalıdır.

3.4 Okan Üniversitesi İnternet ve Yerel Alan Ağı aşağıdaki amaçlar için kullanılamaz:

3.4.1.Rastgele ve alıcının istemi dışında e-posta göndermek (SPAM iletiler).

3.4.2 Başka bir kullanıcının e-posta adresini, o kullanıcının izni olmadan mesaj gönderme amacıyla kullanmak.

3.4.3 Uçtan uca dosya paylaşım programlarını Blgi İşlem'in izni dışında kurmak ve kullanmak.

3.5.4 Bilgi İşlem hizmetlerinin kalitesini düşürecek veri trafiği oluşturmak.

3.5.5 Başkalarının telif haklarını ihlal edici konumda olan materyali (yazı, makale, kitap, film, müzik eserleri gibi) iletmek/yayınlamak/dağıtmak.

PO.BİS.012 TEMİZ MASA TEMİZ EKRAN POLİTİKASI

1. AMAÇ

Normal çalışma süresince ve dışında bilgiye yetkisiz erişim, bilgi kaybı ve hasarı risklerini azaltmak amacıyla kâğıtlar ve depolama ortamları ve kişisel bilgisayarlar için gerekli şartları tanımlamak.

2. KAPSAM

Bu politika kurumun tüm çalışanlarını kapsamaktadır.

3. UYGULAMA

3.1 Ulaşılması istenmeyen bilgi ya da belgeler kullanılmadığında uygun kilitli dolaplarda muhafaza edilir.

3.2 Ağa bağlı bilgisayarlar başıboş olduklarında oturum açık olarak bırakılmazlar. Masasından ayrılan personel ekran kilidi tuşlarına basarak ağ oturumunu otomatik olarak kilitler.

3.3 Hassas ve önemli iş bilgileri ya da belgeleri, gerekmedikleri zamanda özellikle de büro boş olduğunda, kilitlenir.

3.4 Gelen ve giden faks mesajları ve çıktısı alınan belgeler faks ve yazıcı makinelerinde başıboş bırakılmaz.

EK F UYGULANABİLİRLİK BİLDİRGESİ
KONTROL HEDEFLERİ VE KONTROLLER

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
A.5.	**Bilgi Güvenlik Politikaları**						
A.5.1	**Bilgi güvenliği için yönetimin yönlendirmesi**						
A.5.1.1	Bilgi güvenliği için politikalar	Bir dizi bilgi güvenliği politikaları, yönetim tarafından tanımlanmalı, onaylanmalı ve yayınlanarak çalışanlara ve ilgili dış taraflara bildirilmelidir.	Evet	YGG Toplantısı, Duyuru E-postaları, ISO klasörü	Yılda bir kez	Üst Yönetim Temsilcisi, BG ekip Lideri	PO.BİS.001, BGYSEK
A.5.1.2	Bilgi güvenliği için politikaların gözden geçirilmesi	Bilgi güvenliği politikaları, belirli aralıklarla veya önemli değişiklikler ortaya çıktığında sürekli uygunluk ve etkinliği sağlamak amacıyla gözden geçirilmelidir.	Evet	BGYS Ekibi ve YGG Toplantısı	Yılda bir kez	Üst Yönetim Temsilcisi, BG ekip Lideri	YGG Toplantısı, BGYS Ekibi Toplantısı
A.6	**Bilgi Güvenliği Organizasyonu**						
A.6.1	**İç Organizasyon**						
A.6.1.1	Bilgi güvenliği rolleri ve sorumlulukları	Tüm bilgi güvenliği sorumlulukları tanımlanmalı ve tahsis edilmelidir.	Evet	BGYS Ekibi Atama yazısı	Yılda bir kez	Üst Yönetim Temsilcisi, BG Ekip Lideri, Insan Kaynakları	Atama Yazıları(Bg Ekip Üyeleri, BG Ekip Lideri, BG Yönetim Temsilcisi), Görev Tanımları, Organizasyon Şeması
A.6.1.2	Görevlerin ayrılığı	Çelişen görevler ve sorumluluklar, yetkilendirilmemiş veya kasıtsız değişiklik fırsatlarını veya kurulus varlıklarının yanlış kullanımını azaltmak amacıyla ayrılmalıdır.	Evet	İç Denetimler	Yılda bir kez	Üst Yönetim Temsilcisi, BG Ekip Lideri, Insan Kaynakları	PR.BİS.006 Haberleşme ve İşletim Yönetimi Prosedürü, Görev Tanımları
A.6.1.3	Otoritelerle iletişim	Ilgili otoritelerle uygun iletişim	Evet	İç Denetimler	Yılda bir kez	Tüm Birimler, Üst Yönetim	E-mail ve OKIM Kayıtları, PR.BİS.006 Haberleşme ve İşletim Yönetimi Prosedürü

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
		kurulmalıdır.					
A.6.1.4	Özel ilgi grupları ile iletişim	Özel ilgi grupları veya diğer uzman güvenlik forumları ve profesyonel dernekler ile uygun iletişim kurulmalıdır.	Hayır	-------	--------	--------	----
A.6.1.5	Proje yönetiminde bilgi güvenliği	Proje yönetiminde, proje çeşidine bakılmaksızın bilgi güvenliği ele alınmalıdır.	Evet	İç Denetimler	Yılda bir kez	Tüm Birimler	Personel ve Taşeron Sözleşmeleri, PR.BİS.016 Bilgi Sistemleri Edinim, Geliştirme ve Bakım Prosedürü
A.6.2	**Mobil Cihazlar ve uzaktan çalışma**						
A.6.2.1	Mobil cihaz politikası	Mobil cihazların kullanımı ile ortaya çıkan risklerin yönetilmesi amacı ile bir politika ve destekleyici güvenlik önlemleri belirlenmelidir.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BİS.001 Ağ ve Sistem Yönetimi Prosedürü, PR.BİS.004 Erişim Yönetimi Prosedürü
A.6.2.2	Uzaktan çalışma	Uzaktan çalışma alanlarında erişilen, işlenen veya depolanan bilgiyi korumak amacı ile bir politika ve destekleyici güvenlik önlemleri uygulanmalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	Erişim Yönetimi Prosedürü (PR.BİS.004)
A.7	**İnsan Kaynakları Güvenliği**						
A.7.1	**İstihdam Öncesi**						
A.7.1.1	Tarama	Tüm işe alımlarda adaylar için, ilgili yasa, düzenleme ve etiğe göre ve iş gereksinimleri, erişilecek bilginin sınıflandırması ve alınan risklerle orantılı olarak geçmiş	Evet	İç Denetimler	Yılda bir kez	İnsan Kaynakları	PO.BİS.003 Personel Güvenliği Politikası, Adli Sicil Kayıtları, Görev Tanımları

EK F UYGULANABİLİRLİK BİLDİRGESİ
KONTROL HEDEFLERİ VE KONTROLLER

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
		doğrulama kontrolleri gerçekleştirilmelidir.					
A.7.1.2	İstihdam hüküm ve koşulları	Çalışanlar ve yükleniciler ile yapılan sözleşmeler kendilerinin ve kuruluşun bilgi güvenliği sorumluluklarını belirtmelidir.	Evet	İç Denetimler	Yılda bir kez	İnsan Kaynakları	PO.BİS.003 Personel Güvenliği Politikası, Hizmet Sözleşmesi, PR.BİS.004 Erişim Yönetimi Prosedürü
A.7.2	**Çalışma Esnasında**						
A.7.2.1	Yönetimin sorumlulukları	Yönetim, çalışanlar ve yüklenicilerin, kuruluşun yerleşik politika ve prosedürlerine göre bilgi güvenliğini uygulamalarını istemelidir.	Evet	İç Denetimler	Yılda bir kez	Üst Yönetim	BGYSEK, PO.BİS.002 Bilgi Güvenliği Politikası
A.7.2.2	Bilgi güvenliği farkındalığı, eğitim ve öğretimi	Kuruluştaki tüm çalışanlar ve ilgili olduğu durumda, yükleniciler, kendi iş, fonksiyonları ile ilgili, kurumsal politika ve prosedürlere ilişkin uygun farkındalık eğitim ve öğretimini ve bunların düzenli güncellemelerini almalıdırlar.	Evet	İç Denetimler	Yılda bir kez	İnsan Kaynakları	PO.BİS.003 Personel Güvenliği Politikası, PR.BİS.012 Varlık Yönetim Prosedürü, İnsan Kaynakları Eğitim Planları
A.7.2.3	Disiplin Prosesi	Bir bilgi güvenliği ihlal olayını gerçekleştiren çalışanlara yönelik önlem almak için resmi ve bildirilmiş bir disiplin prosesi olmalıdır.	Evet	İç Denetimler	Yılda bir kez	İnsan Kaynakları	PO.BİS.003 Personel Güvenliği Politikası, Hizmet Sözleşmesi, Disiplin Yönetmeliği

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
A.7.3	**İstihdamın sonlandırılması ve değiştirilmesi**						
A.7.3.1	Istihdam sorumluluklarının sonlandırılması veya değiştirilmesi	Istihdamın sonlandırılması veya değiştirilmesinden sonra geçerli olan bilgi güvenliği sorumlulukları ve görevleri tanımlanmalı, çalışan veya yükleniciye bildirilmeli ve yürürlüğe konulmalıdır.	Evet	İç Denetimler	Yılda bir kez	İnsan Kaynakları	İlişik Kesme Formu
A.8	**Varlık Yönetimi**						
A.8.1	**Varlıkların Sorumluluğu**						
A.8.1.1	Varlıkların envanteri	Bilgi ve bilgi işleme olanakları ile ilgili varlıklar belirlenmeli ve bu varlıkların bir envanteri çıkarılmalı ve idame ettirilmelidir.	Evet	BGYS Ekibi Toplantısı	Yılda bir kez	BGYS Ekibi	Varlık Yönetim Prosedürü (PR.BİS.012) Varlık Envanteri Listesi (LS.BİS.002) Varlık Sınıfları Listesi (LS.BİS.003)
A.8.1.2	Varlıkların sahipliği	Envanterde tutulan tüm varlıklara sahip atamaları yapılmalıdır.	Evet	BGYS Ekibi Toplantısı	Yılda bir kez	BGYS Ekibi	Varlık Yönetim Prosedürü (PR.BİS.012) Varlık Envanteri Listesi (LS.BİS.002) Varlık Sınıfları Listesi (LS.BİS.003)
A.8.1.3	Varlıkların kabul edilebilir kullanımı	Bilgi ve bilgi işleme tesisleri ile ilgili bilgi ve varlıkların kabul edilebilir kullanımına dair kurallar belirlenmeli, yazılı hale getirilmeli ve uygulanmalıdır.	Evet	BGYS Ekibi Toplantısı	Yılda bir kez	BGYS Ekibi	Varlık Yönetim Prosedürü (PR.BİS.012) Varlık Envanteri Listesi (LS.BİS.002) Varlık Sınıfları Listesi (LS.BİS.003)
A.8.1.4	Varlıkların iadesi kullanımı	Tüm çalışanlar ve dış tarafların kullanıcıları, istihdamlarının, sözleşme veya anlaşmalarının	Evet	İç Denetimler	Yılda bir kez	Mali İşler	İlişik Kesme Formu

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
		sonlandırılmasının ardından ellerinde olan tüm kurumsal varlıkları iade etmelidirler.					
A.8.2	**Bilgi Sınıflandırma**						
A.8.2.1	Bilgi sınıflandırması	Bilgi, yasal şartlar, değeri, kritikliği ve yetkisiz ifşa veya değiştirilmeye karşı hassasiyetine göre sınıflandırılmalıdır.	Evet	İç Denetimler	Yılda bir kez	BGYS Ekibi	BGYSEK, Bilgi Sınıflandırma Tanımlama Listesi(LS.BİS.009)
A.8.2.2	Bilgi etiketlemesi	Bilgi etiketleme için uygun bir prosedür kümesi kuruluş tarafından benimsenen sınıflandırma düzenine göre geliştirilmeli ve uygulanmalıdır.	Hayır	----	---	---	---
A.8.2.3	Varlıkların kullanımı	Varlıkların kullanımı için prosedürler, kuruluş tarafından benimsenen sınıflandırma düzenine göre geliştirilmeli ve uygulanmalıdır.	Evet	İç Denetimler	Yılda bir kez	Üst Yönetim, BGYS Ekibi	BGYSEK, PR.BIS.012 Varlık Yönetim Prosedürü
A.8.3	**Ortam İşleme**						
A.8.3.1	Taşınabilir ortam yönetimi	Taşınabilir ortam yönetimi için prosedürler kuruluş tarafından benimsenen sınıflandırma düzenine göre uygulanmalıdır.	Evet	İç Denetimler	Yılda bir kez	Tüm Birimler	PR.BIS.006 Haberleşme ve Işletim Yönetimi Prosedürü
A.8.3.2	Ortamın yok edilmesi	Ortam artık ihtiyaç kalmadığında resmi prosedürler kullanılarak güvenli bir şekilde yok	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BIS.006 Haberleşme ve Işletim Yönetimi Prosedürü

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
		edilmelidir.					
A.8.3.3	Fiziksel ortam aktarımı	Bilgi içeren ortam, aktarım sırasında yetkisiz erişim, kötüye kullanım ve bozulmaya karşı korunmalıdır.	Evet	İç Denetimler	Yılda bir kez	Tüm Birimler İşlem	PR.BIS.006 Haberleşme ve Işletim Yönetimi Prosedürü
A.9	**Erişim Kontrolü**						
A.9.1	**Erişim Kontrollünün İş Gereklilikleri**						
A.9.1.1	Erişim kontrol politikası	Bir erişim kontrol politikası, iş ve bilgi güvenliği şartları temelinde oluşturulmalı, yazılı hale getirilmeli ve gözden geçirilmelidir.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem, İnsan Kaynakları, Mali İşler, Öğrenci İşleri	PR.BIS.004 Erişim Yönetimi Prosedürü
A.9.1.2	Ağlara ve ağ hizmetlerine erişim	Kullanıcılara sadece özellikle kullanımı için yetkilendirildikleri ağ ve ağ hizmetlerine erişim verilmelidir.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BIS.004 Erişim Yönetimi Prosedürü
A.9.2	**Kullanıcı Erişim Yönetimi**						
A.9.2.1	Kullanıcı kaydetme ve kayıt silme	Erişim haklarının atanmasını sağlamak için, resmi bir kullanıcı kaydetme ve kayıt silme prosesi uygulanmalıdır.	Evet	İç Denetimler	Yılda bir kez	İnsan Kaynakları, Bilgi İşlem, Mali İşler, Öğrenci İşleri	PR.BIS.004 Erişim Yönetimi Prosedürü
A.9.2.2	Kullanıcı erişimine izin verme	Tüm kullanıcı türlerine tüm sistemler ve hizmetlere erişim haklarının atanması veya iptal edilmesi için resmi bir kullanıcı erişim izin prosesi	Evet	İç Denetimler	Yılda bir kez	İnsan Kaynakları, Bilgi İşlem	PR.BIS.004 Erişim Yönetimi Prosedürü

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
		uygulanmalıdır.					
A.9.2.3	Ayrıcalıklı erişim haklarının yönetimi	Ayrıcalıklı erişim haklarının tahsis edilmesi ve kullanımı kısıtlanmalı ve kontrol edilmelidir.	Evet	İç Denetimler	Yılda bir kez	İnsan Kaynakları, Bilgi İşlem	PR.BIS.004 Erişim Yönetimi Prosedürü
A.9.2.4	Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi	Gizli kimlik doğrulama bilgisinin tahsis edilmesi, resmi bir yönetim prosesi yoluyla kontrol edilmelidir.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BIS.004 Erişim Yönetimi Prosedürü, BGYSEK
A.9.2.5	Kullanıcı erişim haklarının gözden geçirilmesi	Varlık sahipleri kullanıcıların erişim haklarını düzenli aralıklarla gözden geçirmelidir.	Evet	İç Denetimler	Yılda bir kez	Tüm Birimler	PR.BIS.004 Erişim Yönetimi Prosedürü, BGYSEK
A.9.2.6	Erişim haklarının kaldırılması veya düzenlenmesi	Tüm çalışanların ve dış taraf kullanıcılarının bilgi ve bilgi işleme olanaklarına erişim yetkileri, istihdamları, sözleşmeleri veya anlaşmaları sona erdirildiğinde kaldırılmalı veya bunlardaki değişiklik üzerine düzenlenmelidir.	Evet	İç Denetimler	Yılda bir kez	İnsan Kaynakları, Bilgi İşlem	PR.BIS.004 Erişim Yönetimi Prosedürü
A.9.3	**Kullanıcı Sorumlulukları**						
A.9.3.1	Gizli kimlik doğrulama bilgisinin kullanımı	Kullanıcıların, gizli kimlik doğrulama bilgisinin kullanımında kurumsal uygulamalara uymaları şart koşulmalıdır.	Evet	İç Denetimler	Yılda bir kez	Tüm Personel,İnsan Kaynakları, Bilgi İşlem	PR.BIS.004 Erişim Yönetimi Prosedürü, BGYSEK, Eğitimler

EK F UYGULANABİLİRLİK BİLDİRGESİ
KONTROL HEDEFLERİ VE KONTROLLER

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
		.					
A.9.4	**Sistem ve Uygulama Erişim Kontrolü**						
A.9.4.1	Bilgiye erişimin kısıtlanması	Bilgi ve uygulama sistem fonksiyonlarına erişim, erişim kontrol politikası doğrultusunda kısıtlanmalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BİS.004 Erişim Yönetimi Prosedürü, PO.BİS.008 Sunucu Güvenlik Politikası, PO.BİS.009 Ağ Yönetim Politikası, PO.BİS.010 Ağ Kullanım Politikası
A.9.4.2	Güvenli oturum açma prosedürleri	Erişim kontrol politikası tarafından şart koşulduğu yerlerde, sistem ve uygulamalara erişim güvenli bir oturum açma prosedürü tarafından kontrol edilmelidir.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BİS.004 Erişim Yönetimi Prosedürü, PO.BİS.008 Sunucu Güvenlik Politikası, PO.BİS.009 Ağ Yönetim Politikası, PO.BİS.010 Ağ Kullanım Politikası, Etki Alanı Kullanıcı hesapları
A.9.4.3	Parola yönetim sistemi	Parola yönetim sistemleri etkileşimli olmalı ve yeterli güvenlik seviyesine sahip parolaları temin etmelidir.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem, Mali İşler, Öğrenci İşleri, İnsan Kaynakları	PR.BİS.008 Şifre Prosedürü
A.9.4.4	Ayrıcalıklı destek programlarının kullanımı	Sistem ve uygulamaların kontrollerini geçersiz kılma kabiliyetine sahip olabilen destek programlarının kullanımı kısıtlanmalı ve sıkı bir şekilde kontrol edilmelidir.	Hayır	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BİS.002 Bakım Prosedürü, PR.BİS.004 Erişim Yönetimi Prosedürü, PO.BİS.008 Sunucu Güvenlik Politikası, PO.BİS.009 Ağ Yönetim Politikası, PO.BİS.010 Ağ Kullanım Politikası
A.9.4.5	Program kaynak koduna erişim	Program kaynak koduna erişim	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PO.BİS.013 Yazılım Geliştirme Politikası

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
	kontrolü	kısıtlanmalıdır.					
A.10	**Kriptografi**						
A.10.1	**Kriptografik Kontroller**						
A.10.1.1	Kriptografik kontrollerin kullanımına ilişkin politika	Bilginin korunması için kriptografik kontrollerin kullanımına dair bir politika geliştirilmeli ve uygulanmalıdır.	Hayır	---	---	---	---
A.10.1.2	Anahtar yönetimi	Kriptografik anahtarların kullanımı, korunması ve yaşam süresine dair bir politika geliştirilmeli ve tüm yaşam çevirimleri süresince uygulanmalıdır.	Hayır	---	---	---	---
A.11	**Fiziksel ve Çevresel Güvenlik**						
A.11.1	**Güvenli Alanlar**						
A.11.1.1	Fiziksel güvenlik sınırı	Hassas veya kritik bilgi ve bilgi işleme olanakları barındıran alanları korumak için güvenlik sınırları tanımlanmalı ve kullanılmalıdır.	Evet	BGYS Ekibi Toplantısı	Yılda bir kez	BGYS Ekibi	PR.BİS.005 Fiziki ve Çevre Güvenliği Prosedürü
A.11.1.2	Fiziksel giriş kontrolleri	Güvenli alanlar sadece yetkili personele erişim izni verilmesini temin etmek için uygun giriş kontrolleri ile korunmalıdır.	Evet	İç Denetimler	Yılda bir kez	BGYS Ekibi, İdari İşler, Mali İşler, İnsan Kaynakları,	PR.BİS.005 Fiziki ve Çevre Güvenliği Prosedürü

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
						Öğrenci İşleri	
A.11.1.3	Ofislerin, odaların ve tesislerin güvenliğinin sağlanması	Ofisler, odalar ve tesisler için fiziksel güvenlik tasarlanmalı ve uygulanmalıdır.	Evet	İç Denetimler	Yılda bir kez	İdari İşler	PR.BIS.005 Fiziki ve Çevre Güvenliği Prosedürü
A.11.1.4	Dış ve çevresel tehditlere karşı koruma	Doğal felaketler, kötü niyetli saldırılar veya kazalara karşı fiziksel koruma tasarlanmalı ve uygulanmalıdır.	Evet	İç Denetimler	Yılda bir kez	Üst yönetim	PR.BIS.005 Fiziki ve Çevre Güvenliği Prosedürü, Acil Durum Planları
A.11.1.5	Güvenli alanlarda çalışma	Güvenli alanlarda çalışma için prosedürler tasarlanmalı ve uygulanmalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem, Mali işler, İnsan Kaynakları, Öğenci İşleri	PR.BIS.005 Fiziki ve Çevre Güvenliği Prosedürü
A.11.1.6	Teslimat ve yükleme alanları	Yetkisiz kişilerin tesise giriş yapabildiği, teslimat ve yükleme alanları gibi erişim noktaları ve diğer noktalar kontrol edilmeli ve mümkünse yetkisiz erişimi engellemek için bilgi işleme olanaklarından ayrılmalıdır.	Hayır	---	---	---	---
A.11.2	**Teçhizat**						
A.11.2.1	Teçhizat yerleştirme ve koruma	Teçhizat, çevresel tehditlerden ve tehlikelerden ve yetkisiz erişim fırsatlarından kaynaklanan riskleri azaltacak şekilde yerleştirilmeli ve korunmalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem, Yapı İşleri	Fiziki ve Çevre Güvenliği Prosedürü (PR.BİS.005), Bakım Prosedürü (PR.BİS.002), Kötü Niyetli Yazılımlara Karşı Koruma
A.11.2.2	Destekleyici altyapı	Teçhizat destekleyici altyapı	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem,	Fiziki ve Çevre Güvenliği Prosedürü

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
	hizmetleri	hizmetlerindeki hatalardan kaynaklanan enerji kesintileri ve diğer kesintilerden korunmalıdır.				Yapı İşleri	(PR.BİS.005)
A.11.2.3	Kablo güvenliği	Veri veya destekleyici bilgi hizmetlerini taşıyan enerji ve telekomünikasyon kabloları, dinleme, girişim oluşturma veya hasara karşı korunmalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem, Yapı İşleri	Fiziki ve Çevre Güvenliği Prosedürü (PR.BİS.005)
A.11.2.4	Teçhizat bakımı	Teçhizatın bakımı, sürekli erişilebilirliğini ve bütünlüğünü temin etmek için doğru şekilde yapılmalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem, Yapı İşleri	PR.BİS.006 Haberleşme ve Işletim Yönetimi Prosedürü
A.11.2.5	Varlıkların taşınması	Teçhizat, bilgi veya yazılım ön yetkilendirme olmaksızın kuruluş dışına çıkarılmamalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem, Mali İşler	BGYSEK, Cihaz Teslim Formu (FR.BİS.004), Erişim Kısıtlamaları
A.11.2.6	Kuruluş dışındaki teçhizat ve varlıkların güvenliği	Kuruluş dışındaki varlıklara, kuruluş yerleşkesi dışında çalışmanın farklı riskleri de göz önünde bulundurularak güvenlik uygulanmalıdır.	Hayır	---	-----	----	----
A.11.2.7	Teçhizatın güvenli yok edilmesi veya tekrar kullanımı	Depolama ortamı içeren teçhizatların tüm parçaları, yok etme veya tekrar kullanımdan önce tüm hassas verilerin ve lisanslı yazılımların kaldırılmasını veya güvenli bir	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	Haberleşme ve İşletim Yönetimi Prosedürü (PR.BİS.006)

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
		şekilde üzerine yazılmasını temin etmek amacıyla doğrulanmalıdır.					
A.11.2.8	Gözetimsiz kullanıcı teçhizatı	Kullanıcılar, gözetimsiz teçhizatın uygun şekilde korunmasını temin etmelidir.	Evet	İç Denetimler	Yılda bir kez	Tüm Birimler	PR.BIS.004 Erişim Yönetimi Prosedürü
A.11.2.9	Temiz masa temiz ekran politikası	Kâğıtlar ve taşınabilir depolama ortamları için bir temiz masa politikası ve bilgi işleme olanakları için bir temiz ekran politikası benimsenmelidir.	Evet	İç Denetimler	Yılda bir kez	Tüm Birimler	Temiz Masa Temiz Ekran Politikası (PO.BİS.012)
A.12	**İşletim Güvenliği**						
A.12.1	**İşletim Prosedürleri ve Sorumlulukları**						
A.12.1.1	Yazılı işletim prosedürleri	Işletim prosedürleri yazılı hale getirilmeli ve ihtiyacı olan tüm kullanıcılara sağlanmalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	Haberleşme ve İşletim Yönetimi Prosedürü (PR.BİS.006),
A.12.1.2	Değişiklik yönetimi	Bilgi güvenliğini etkileyen, kuruluş, iş, prosesleri, bilgi işleme olanakları ve sistemlerdeki değişiklikler kontrol edilmelidir.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	Bilgi Sistemleri Edinim, Geliştirme ve Bakım Prosedürü (PR.BİS.016), Donanım Değişim Kontrol Geçerleme ve Doğrulama Formu (FR.BİS.012), Yazılım Sistemleri Devreye Alma Geliştirme Ve Kontrol Formu(FR.BİS.013)
A.12.1.3	Kapasite yönetimi	Kaynakların kullanımı izlenmeli, ayarlanmalı ve gerekli sistem performansını temin etmek için gelecekteki kapasite gereksinimleri ile ilgili	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	Bilgi Sistemleri Edinim, Geliştirme ve Bakım Prosedürü (PR.BİS.016), Donanım Değişim Kontrol Geçerleme ve Doğrulama Formu (FR.BİS.012), Yazılım Sistemleri Devreye Alma Geliştirme Ve Kontrol Formu(FR.BİS.013)

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
		kestirimler yapılmalıdır.					
A.12.1.4	Geliştirme, test ve işletim ortamlarının birbirinden ayrılması	Geliştirme, test ve işletim ortamlar, yetkisiz erişim veya işletim ortamlarında değişiklik risklerinin azaltılması için birbirinden ayrılmalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PO.BİS.013 Yazılım Geliştirme Politikası, PO.BİS.09 Ağ Yönetim Politikası
A.12.2	**Kötücül Yazılımlardan Koruma**						
A.12.2.1	Kötücül yazılımlara karşı kontroller	Kötücül yazılımlardan korunmak için tespit etme, engelleme ve kurtarma kontrolleri uygun kullanıcı farkındalığı ile birlikte uygulanmalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BİS.007 Kötü Niyetli Yazılımlara Karşı Koruma Prosedürü
A.12.3	**Yedekleme**						
A.12.3.1	Bilgi yedekleme	Bilgi, yazılım ve sistem imajlarının yedekleme kopyaları alınmalı ve üzerinde anlaşılmış bir yedekleme politikası doğrultusunda düzenli olarak test edilmelidir.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BİS.014 Yedekleme Prosedürü
A.12.4	**Kaydetme ve İzleme**						
A.12.4.1	Olay kaydetme	Kullanıcı işlemleri, kural dışılıklar, hatalar ve bilgi güvenliği olaylarını kaydeden olay kayıtları üretilmeli, saklanmalı ve düzenli olarak gözden geçirilmelidir.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem, Mali İşler, Öğrenci İşleri, İnsan Kaynakları	PR.BİS.006 Haberleşme ve İşletim Yönetimi Prosedürü
A.12.4.2	Kayıt bilgisinin	Kaydetme olanakları ve kayıt	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem,	PR.BİS.006 Haberleşme ve İşletim

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
	korunması	bilgileri kurcalama ve yetkisiz erişime karşı korunmalıdır.				Mali İşler, Öğrenci İşleri, İnsan Kaynakları	Yönetimi Prosedürü
A.12.4.3	Yönetici ve operatör kayıtları	Sistem yöneticileri ve sistem operatörlerinin işlemleri kayıt altına alınmalı, kayıtlar korunmalı ve düzenli olarak gözden geçirilmelidir.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem, Mali İşler, Öğrenci İşleri, İnsan Kaynakları	PR.BİS.006 Haberleşme ve İşletim Yönetimi Prosedürü
A.12.4.4	Saat senkronizasyonu	Bir kuruluş veya güvenlik alanında yer alan tüm ilgili bilgi işleme sistemlerinin saatleri tek bir referans zaman kaynağına göre senkronize edilmelidir.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	Erişim Yönetimi Prosedürü (PR.BİS.004)
A.12.5	**İşletimsel Yazılımın Kontrolü**						
A.12.5.1	İşletimsel sistemler üzerine yazılım kurulumu	İşletimsel sistemler üzerine yazılım kurulumunun kontrolü için prosedürler uygulanmalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PO.BİS.002 Bilgi Sistemleri Genel Kullanım Politikası, PR.BİS.004 Erişim Yönetimi Prosedürü
A.12.6	**Teknik Açıklık Yönetimi**						
A.12.6.1	Teknik açıklıkların yönetimi	Kullanılmakta olan bilgi sistemlerinin teknik açıklıklarına dair bilgi, zamanında elde edilmeli kuruluşun bu tür açıklıklara karşı zafiyeti değerlendirilmeli ve ilgili riskin ele alınması için uygun tedbirler alınmalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BİS.001 Ağ ve Sistem Yönetimi Prosedürü, PR.BİS.010 Ölçüm Yöntemleri Ve Kontrolleri Prosedürü, Firewall, IPS, Anti Virus Programı, Kullanıcı Erişim Yetki Kısıtlamaları

EK F UYGULANABİLİRLİK BİLDİRGESİ
KONTROL HEDEFLERİ VE KONTROLLER

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
A.12.6.2	Yazılım kurulumu kısıtlamaları	Kullanıcılar tarafından yazılım kurulumuna dair kurallar oluşturulmalı ve uygulanmalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PO.BİS.002 Bilgi Sistemleri Genel Kullanım Politikası, PR.BIS.004 Erişim Yönetimi Prosedürü
A.12.7	**Bilgi Sistemleri Tetkik Hususları**						
A.12.7.1	Bilgi sistemleri tetkik kontrolleri	İşletimsel sistemlerin doğrulanmasını kapsayan tetkik gereksinimleri ve faaliyetleri, iş proseslerindeki kesintileri asgariye indirmek için dikkatlice planlanmalı ve üzerinde anlaşılmalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	Bilgi Sistemleri Edinim, Geliştirme ve Bakım Prosedürü (PR.BİS.016), Donanım Değişim Kontrol Geçerleme ve Doğrulama Formu (FR.BİS.012), Yazılım Sistemleri Devreye Alma Geliştirme Ve Kontrol Formu(FR.BİS.013)
A.13	**Haberleşme Güvenliği**						
A.13.1	**Ağ Güvenliği Yönetimi**						
A.13.1.1	Ağ kontrolleri	Sistemlerdeki ve uygulamalardaki bilgiyi korumak amacıyla ağlar yönetilmeli ve kontrol edilmelidir.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BIS.001 Ağ ve Sistem Yönetimi Prosedürü, PO.BİS.009 Ağ Yönetim Politikası, PO.BİS.010 Ağ Kullanım Politikası
A.13.1.2	Ağ hizmetlerinin güvenliği	Tüm ağ hizmetlerinin güvenlik mekanizmaları, hizmet seviyeleri ve yönetim gereksinimleri tespit edilmeli ve hizmetler kurulus, içinden veya dış kaynak yoluyla sağlanmış olsun olmasın, ağ hizmetleri anlaşmalarında yer almalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BIS.001 Ağ ve Sistem Yönetimi Prosedürü, PO.BİS.009 Ağ Yönetim Politikası, PO.BİS.010 Ağ Kullanım Politikası
A.13.1.3	Ağlarda ayrım	Ağlarda, bilgi hizmetleri, kullanıcıları ve bilgi sistemleri	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BIS.004 Erişim Yönetimi Prosedürü

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
		grupları ayrılmalıdır.					
A.13.2	**Bilgi Transferi**						
A.13.2.1	Bilgi transfer politikaları ve prosedürleri	Tüm iletişim olanağı türlerinin kullanımıyla bilgi transferini korumak için resmi transfer politikaları, prosedürleri ve kontrolleri mevcut olmalıdır.	Hayır	--	--	--	--
A.13.2.2	Bilgi transferindeki anlaşmalar	Anlaşmalar, kuruluş ve dış taraflar arasındaki iş bilgileri'nin güvenli transferini ele almalıdır.	Hayır	--	--	--	--
A.13.2.3	Elektronik mesajlaşma	Elektronik mesajlaşmadaki bilgi uygun şekilde korunmalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BİS.003 E-Posta Prosedürü, PO.BİS.005 E-Posta Politikası
A.13.2.4	Gizlilik ya da ifşa etmeme anlaşmaları	Bilginin korunması için kuruluşun ihtiyaçlarını yansıtan gizlilik ya da ifşa etmeme anlaşmalarının gereksinimleri tanımlanmalı, düzenli olarak gözden geçirilmeli ve yazılı hale getirilmelidir.	Evet	İç Denetimler	Yılda bir kez	Hukuk Müşavirliği	PR.BİS.006 Haberleşme ve İşletim Yönetimi Prosedürü, Güvenlik Taahhüdü Maddesi.
A.14	**Sistem temini, geliştirme ve bakımı**						
A.14.1	**Bilgi Sistemlerinin Güvenlik Gereksinimleri**						
A.14.1.1	Bilgi güvenliği gereksinimleri analizi ve belirtimi	Bilgi güvenliği ile ilgili gereksinimler, yeni bilgi sistemleri gereksinimlerine veya var olan bilgi sistemlerinin iyileştirmelerine dâhil	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BİS.001 Ağ ve Sistem Yönetimi Prosedürü, PO.BİS.009 Ağ Yönetim Politikası, PO.BİS.010 Ağ Kullanım Politikası, PO.BİS.004 İnternet Erşim ve Kullanım Politikası

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
		edilmelidir.					
A.14.1.2	Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması	Halka açık ağlar üzerinden geçen uygulama hizmetlerindeki bilgi, hileli faaliyetlerden, sözleşme ihtilafından ve yetkisiz ifşadan ve değiştirmeden korunmalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BİS.001 Ağ ve Sistem Yönetimi Prosedürü, PO.BİS.009 Ağ Yönetim Politikası, PO.BİS.010 Ağ Kullanım Politikası, PO.BİS.004 İnternet Erşim ve Kullanım Politikası
A.14.1.3	Uygulama hizmet işlemlerinin korunması	Uygulama hizmet işlemlerindeki bilgi eksik iletim, yanlış yönlendirme, yetkisiz mesaj değiştirme, yetkisiz ifşayı, yetkisiz mesaj çoğaltma ya da mesajı yeniden oluşturmayı önlemek için korunmalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BİS.010 Ölçüm Yöntemleri Ve Kontrolleri Prosedürü, PO.BİS.011 Veritabanı Güvenlik Politikası, PO.BİS.Sunucu Güvenlik Politikası
A.14.2	**Geliştirme ve Destek Süreçlerinde Güvenlik**						
A.14.2.1	Güvenli geliştirme politikası	Yazılım ve sistemlerin geliştirme kuralları belirlenmeli ve kuruluş içerisindeki geliştirmelere uygulanmalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PO.BİS.013 Yazılım Geliştirme Politikası, PR.BİS.013 Yazılım Geliştirme ve Sistem Yönetimi Prosedürü
A.14.2.2	Sistem değişiklik kontrolü prosedürleri	Geliştirme yaşam döngüsü içerisindeki sistem değişiklikleri resmi değişiklik kontrol prosedürlerinin kullanımı ile kontrol edilmelidir.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BİS.016 Bilgi Sistemleri Edinim, Geliştirme ve Bakım Prosedürü.
A.14.2.3	İşletim platformu değişikliklerden sonra	İşletim platformları değiştirildiğinde, kurumsal	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BİS.016 Bilgi Sistemleri Edinim, Geliştirme ve Bakım Prosedürü.

EK F UYGULANABİLİRLİK BİLDİRGESİ
KONTROL HEDEFLERİ VE KONTROLLER

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
	uygulamaların teknik gözden geçirmesi	işlemlere ya da güvenliğe hiçbir kötü etkisi olmamasını sağlamak amacıyla iş için kritik uygulamalar gözden geçirilmeli ve test edilmelidir.					
A.14.2.4	Yazılım paketlerindeki değişikliklerdeki kısıtlamalar	Yazılım paketlerine yapılacak değişiklikler, gerek duyulanlar hariç önlenmeli ve tüm değişiklikler sıkı bir biçimde kontrol edilmelidir.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BİS.016 Bilgi Sistemleri Edinim, Geliştirme ve Bakım Prosedürü, Donanım Değişim Kontrol Geçerleme ve Doğrulama Formu (FR.BİS.012), Yazılım Sistemleri Devreye Alma Geliştirme Ve Kontrol Formu(FR.BİS.013)
A.14.2.5	Güvenli sistem mühendisliği prensipleri	Güvenli sistem mühendisliği prensipleri belirlenmeli, yazılı hale getirilmeli ve tüm bilgi sistemi uygulama çalışmalarına uygulanmalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BİS.016 Bilgi Sistemleri Edinim, Geliştirme ve Bakım Prosedürü. BGYS Tüm Politikaları
A.14.2.6	Güvenli geliştirme ortamı	Kuruluşlar tüm sistem geliştirme yaşam döngüsünü kapsayan sistem geliştirme ve bütünleştirme girişimleri için güvenli geliştirme ortamları kurmalı ve uygun bir şekilde korumalıdır.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BİS.016 Bilgi Sistemleri Edinim, Geliştirme ve Bakım Prosedürü, PR.BİS.013 Yazılım Geliştirme ve Sistem Yönetimi Prosedürü
A.14.2.7	Dışarıdan sağlanan geliştirme	Kuruluş dışarıdan sağlanan sistem geliştirme faaliyetini denetlemeli ve izlemelidir.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BİS.016 Bilgi Sistemleri Edinim, Geliştirme ve Bakım Prosedürü, PR.BİS.013 Yazılım Geliştirme ve Sistem Yönetimi Prosedürü, Donanım Değişim Kontrol Geçerleme ve Doğrulama Formu

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
							(FR.BİS.012), Yazılım Sistemleri Devreye Alma Geliştirme Ve Kontrol Formu(FR.BİS.013)
A.14.2.8	Sistem güvenlik testi	Güvenlik işlevselliğinin test edilmesi, geliştirme süresince gerçekleştirilmelidir.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BIS.010 Ölçüm Yöntemleri Ve Kontrolleri Prosedürü
A.14.2.9	Sistem kabul testi	Kabul test programları ve ilgili kriterler, yeni bilgi sistemleri, yükseltmeleri ve yeni versiyonları için belirlenmelidir.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BIS.010 Ölçüm Yöntemleri Ve Kontrolleri Prosedürü, PR.BIS.016 Bilgi Sistemleri Edinim, Geliştirme ve Bakım Prosedürü
A.14.3	**Test Verisi**						
A.14.3.1	Test verisinin korunması	Test verisi dikkatli bir şekilde seçilmeli, korunmalı ve kontrol edilmelidir.	Evet	İç Denetimler	Yılda bir kez	BGYS Ekibi	PR.BIS.016 Bilgi Sistemleri Edinim, Geliştirme ve Bakım Prosedürü
A.15	**Tedarikçi İlişkileri**						
A.15.1	**Tedarikçi İlişkilerinde Bilgi Güvenliği**						
A.15.1.1	Tedarikçi ilişkileri için bilgi güvenliği politikası	Tedarikçinin kuruluşun varlıklarına erişimi ile ilgili riskleri azaltmak için bilgi güvenliği gereksinimleri tedarikçi ile kararlaştırılmalı ve yazılı hale getirilmelidir.	Evet	İç Denetimler	Yılda bir kez	Üst Yönetim	YGG Toplantıları, PR.BIS.006 Haberleşme ve Işletim Yönetimi Prosedürü
A.15.1.2	Tedarikçi anlaşmalarında güvenliği ifade etme	Kuruluşun bilgisine erişebilen, bunu işletebilen, depolayabilen, iletebilen veya kuruluşun bilgisi için bilgi teknolojileri altyapı bileşenlerini temin edebilen	Evet	İç Denetimler	Yılda bir kez	Hukuk Müşavirliği	PR.BIS.006 Haberleşme ve Işletim Yönetimi Prosedürü

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
		tedarikçilerin her biri ile anlaşılmalı ve ilgili tüm bilgi güvenliği gereksinimleri oluşturulmalıdır.					
A.15.1.3	Bilgi ve iletişim teknolojileri tedarik zinciri	Tedarikçiler ile yapılan anlaşmalar, bilgi ve iletişim teknolojileri hizmetleri ve ürün tedarik zinciri ile ilgili bilgi güvenliği risklerini ifade eden şartları içermelidir.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BİS.006 Haberleşme ve İşletim Yönetimi Prosedürü, PR.BİS.016 Bilgi Sistemleri Edinim, Geliştirme ve Bakım Prosedürü
A.16	**Bilgi Güvenliği İhlal Olayı Yönetimi**						
A.16.1	**Bilgi Güvenliği İhlal Olaylarının ve İyileştirmelerinin Yönetimi**						
A.16.1.1	Sorumluluklar ve prosedürler	Bilgi güvenliği ihlal olaylarına hızlı, etkili ve düzenli bir yanıt verilmesini sağlamak için yönetim sorumlulukları ve prosedürleri oluşturulmalıdır.	Evet	İç Denetimler	Yılda bir kez	BGYS Ekip Lideri	PR.BİS.009 BG Olay Yönetim Prosedürü
A.16.1.2	Bilgi güvenliği olaylarının raporlanması	Bilgi güvenliği olayları uygun yönetim kanalları aracılığı ile olabildiğince hızlı bir şekilde raporlanmalıdır.	Evet	İç denetimler	Yılda bir kez	Tüm Personel	PR.BİS.009 BG Olay Yönetim Prosedürü
A.16.1.3	Bilgi güvenliği açıklıklarının raporlanması	Kuruluşun bilgi sistemlerini ve hizmetlerini kullanan çalışanlardan ve yüklenicilerden, sistemler veya hizmetlerde gözlenen veya şüphelenilen herhangi bir bilgi güvenliği açıklığına dikkat etmeleri ve	Evet	İç denetimler	Yılda bir kez	Tüm Personel	PR.BİS.009 BG Olay Yönetim Prosedürü

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
		bunları raporlamaları istenmelidir.					
A.16.1.4	Bilgi güvenliği olaylarında değerlendirme ve karar verme	Bilgi güvenliği olayları değerlendirilmeli ve bilgi güvenliği ihlal olayı olarak sınıflandırılıp sınıflandırılmayacağına karar verilmelidir.	Evet	İç denetimler	Yılda bir kez	BGYS Ekibi	PR.BIS.009 BG Olay Yönetim Prosedürü
A.16.1.5	Bilgi güvenliği ihlal olaylarına yanıt verme	Bilgi güvenliği ihlal olaylarına, yazılı prosedürlere uygun olarak yanıt verilmelidir.	Evet	İç denetimler	Yılda bir kez	BGYS Ekibi	PR.BIS.009 BG Olay Yönetim Prosedürü
A.16.1.6	Bilgi güvenliği ihlal olaylarından ders çıkarma	Bilgi güvenliği ihlal olaylarının analizi ve çözümlemesinden kazanılan tecrübe gelecekteki ihlal olaylarının gerçekleşme olasılığını veya etkilerini azaltmak için kullanılmalıdır.	Evet	BGYS Ekibi Toplantısı	Yılda iki kez	BGYS Ekibi	PR.BIS.009 BG Olay Yönetim Prosedürü
A.16.1.7	Kanıt toplama	Kuruluş, kanıt olarak kullanılabilecek bilginin teşhisi, toplanması, edinimi ve korunması için prosedürler tanımlamalı ve uygulamalıdır.	Evet	İç denetimler	Yılda iki kez	BGYS Ekibi	PR.BIS.009 BG Olay Yönetim Prosedürü,
A.17	**İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları**						
A.17.1	**Bilgi Güvenliği Sürekliliği**						
A.17.1.1	Bilgi güvenliği sürekliliğinin	Kuruluş, olumsuz durumlarda, örneğin bir kriz ve felaket boyunca, bilgi güvenliği ve bilgi	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BIS.015 İş Sürekliliği Prosedürü, PL.BIS.002 İş Sürekliliği Planı, FR.BIS.014 Tatbikat Değerlendirme

EK F UYGULANABİLİRLİK BİLDİRGESİ
KONTROL HEDEFLERİ VE KONTROLLER

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
	planlanması	güvenliği yönetimi sürekliliğinin gereksinimlerini belirlemelidir.					Formu
A.17.1.2	Bilgi güvenliği sürekliliğinin uygulanması	Kuruluş, olumsuz bir olay süresince bilgi güvenliği için istenen düzeyde sürekliliğin sağlanması için prosesleri, prosedürleri ve kontrolleri kurmalı, yazılı hale getirmeli, uygulamalı ve sürdürmelidir.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	PR.BIS.015 İş Sürekliliği Prosedürü, PL.BIS.002 İş Sürekliliği Planı, FR.BIS.014 Tatbikat Değerlendirme Formu
A.17.1.3	Bilgi güvenliği sürekliliği'nin doğrulanması, gözden geçirilmesi ve değerlendirilmesi	Kuruluş, oluşturulan ve uygulanan bilgi güvenliği sürekliliği kontrollerinin, olumsuz olaylar süresince geçerli ve etkili olduğundan emin olmak için belirli aralıklarda doğruluğunu sağlamalıdır.	Evet	İş Sürekliliği Tatbikatı	Yılda bir kez	Bilgi İşlem	B PR.BIS.015 İş Sürekliliği Prosedürü, PL.BIS.002 İş Sürekliliği Planı, FR.BIS.014 Tatbikat Değerlendirme Formu
A.17.2	**Yedek Fazlalıklar**						
A.17.2.1	Bilgi işleme olanaklarının erişilebilirliği	Bilgi işleme olanakları, erişilebilirlik gereksinimlerini karşılamak için yeterli fazlalık ile gerçekleştirilmelidir.	Evet	İç Denetimler	Yılda bir kez	Bilgi İşlem	B PR.BIS.015 İş Sürekliliği Prosedürü, PL.BIS.002 İş Sürekliliği Planı, FR.BIS.014 Tatbikat Değerlendirme Formu
A.18	**Uyum**						
A.18.1	**Yasal ve Sözleşmeye tabii gereksinimlerle uyum**						
A.18.1.1	Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri	Ilgili tüm yasal mevzuat, düzenleyici, sözleşmeden doğan şartları ve kuruluşun bu gereksinimleri karşılama	Evet	Mevzuatlar, İç denetimler	Sürekli	BG Ekip Lideri	BGYSEK

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
	tanımlama	yaklaşımı her bilgi sistemi ve kuruluşu için açıkça tanımlanmalı, yazılı hale getirilmeli ve güncel tutulmalıdır.					
A.18.1.2	Fikri mülkiyet hakları	Fikri mülkiyet hakları ve patentli yazılım ürünlerinin kullanımı üzerindeki yasal, düzenleyici ve anlaşmalardan doğan şartlara uyum sağlamak için uygun prosedürler gerçekleştirilmelidir.	Evet	İç denetimler	Yılda bir kez	BG Yönetim Temsilcisi	BGYSEK
A.18.1.3	Kayıtların korunması	Kayıtlar kaybedilmeye, yok edilmeye, sahteciliğe, yetkisiz erişime ve yetkisiz yayımlamaya karşı yasal, düzenleyici, sözleşmeden doğan şartlar ve iş şartlarına uygun olarak korunmalıdır.	Evet	İç Denetimler	Yılda bir kez	BG Yönetim Temsilcisi, Bilgi İşlem	BGYSEK
A.18.1.4	Kişi tespit bilgisinin gizliliği ve korunması	Kişiyi tespit bilgisinin gizliliği ve korunması uygulanabilen yerlerde ilgili yasa ve düzenlemeler ile sağlanmalıdır.	Evet	İç Denetimler	Yılda bir kez	BGYS Ekibi	
A.18.1.5	Kriptografik kontrollerin düzenlemesi	Kriptografik kontroller tüm ilgili sözleşmeler, yasa ve düzenlemelere uyumlu bir şekilde kullanılmalıdır.	Hayır	--	--	--	--

EK F UYGULANABİLİRLİK BİLDİRGESİ
KONTROL HEDEFLERİ VE KONTROLLER

MAD.NO	KONTROL HEDEFİ	KONTROL	UYGULANABİLİR	KONTROL YÖNTEMİ	KONTROL SIKLIĞI	SORUMLU	REFERANS
A.18.2	**Bilgi Güvenliği Gözden Geçirmeleri**						
A.18.2.1	Bilgi güvenliğinin bağımsız gözden geçirmesi	Kuruluşun bilgi güvenliğine ve uygulamasına(örn. bilgi güvenliği için kontrol hedefleri, kontroller, politikalar, prosesler ve prosedürler) yaklaşımı belirli aralıklarla veya önemli değişiklikler meydana geldiğinde bağımsız bir şekilde gözden geçirilmelidir.	Evet	BGYS Ekibi Toplantısı,	Yılda iki kez	BGYS Ekibi	İç Denetim Planı, BGYSEK
A.18.2.2	Güvenlik politikaları ve standartları ile uyum	Yöneticiler kendi sorumluluk alanlarında bulunan, bilgi işleme ve prosedürlerin, uygun güvenlik politikaları, standartları ve diğer güvenlik gereksinimleri ile uyumunu düzenli bir şekilde gözden geçirmelidir.	Evet	BGYS Ekibi Toplantısı,YGG	Yılda iki kez	BGYS Ekibi	İç Denetim Planı, BGYSEK
A.18.2.3	Teknik uyum gözden geçirmesi	Kuruluşun bilgi güvenliği politika ve standartları ile uyumu için bilgi sistemleri düzenli bir şekilde gözden geçirilmelidir.	Evet	BGYS Ekibi Toplantısı	Yılda bir kez	Bilgi İşlem	İç Denetim Planı, BGYSEK Prosedürü (PR.BİS.004)

EK G SİSTEM KONTROL FORMU

Cihaz/Program ve Yapılacak Kontroller	Açıklama	Kontrolü Yapan Adı-Soyadı	Tarih	İmza
Firewall				
Kurallar				
Kullanıcı Adı/Şifre				
Yedekleme				
Güncelleme				
Uzak Erişim Yetkileri				
Donanımsal Durumu				
Lisans				
IPS				
Kullanıcı Adı/Şifre				
Yedekleme				
Güncelleme				
Donanımsal Durumu				
Lisans				
Crypto-LOG				
Kullanıcı Adı/Şifre				
Yedekleme				
Donanımsal Durumu				
Güncelleme				

Lisans				
Omurga Switch				
Erişim Listeleri (Access List)				
Kullanıcı Adı/Şifre				
Donanımsal Durumu				
Yedekleme				
Kenar Switch				
Kullanıcı Adı/Şifre				
Port Kimlik Doğrulama				
Donanımsal Durumu				
Yedekleme				
Kablosuz Ağ Kontrol Cihazları (WLC-CryptoSPOT)				
Kullanıcı Adı/Şifre				
Yedekleme				
Donanımsal Durumu				
Güncelleme				
Yedekleme Cihazı				
Kullanıcı Adı/Şifre				
Donanımsal Durumu				
Güncelleme				
Okan ve OkanStd PDC/ ADC Sunucu				
Kullanıcı Adı/Şifre				
Erişim Yetkileri				
Güncelleme				

E-Posta Sunucuları				
Kullanıcı Adı/Şifre				
Erişim Yetkileri				
Güncelleme				
Muhasebe Sunucusu				
Kullanıcı Adı/Şifre				
Erişim Yetkileri				
Güncelleme				
OBS Sunucusu				
Kullanıcı Adı/Şifre				
Erişim Yetkileri				
Güncelleme				
Kurum Websitesi/Web Sunucu/Veritabanı/				
Kullanıcı Adı/Şifre				
Erişim Yetkileri				
Dosya Sunucu Kullanıcı Dosyaları				
Kullanıcı Adı/Şifre				
Erişim Yetkileri				
Sanallaştırma Sunucuları-Tuzla/UZEM/Kadıköy				
Donanımsal Durumu (Disk, Güç Kaynağı)				
Güncelleme (Sanallaştırma Platformu)				
Alarm ve Yangın Söndürme Sistemleri-Tuzla/Kadıköy/Mecidiyeköy Sistem Odası ve Tuzla Arşiv Odası				
Gaz Sistemi Durumu				
Kuru Tip Söndürme Cihazı Durumu				

HAZIRLAYAN BG EKİP LİDERİ			