YÜKSEKÖĞRETİM KURULU
BAŞKANLIĞI

2023 YILI

T.C.
AĞRI İBRAHİM ÇEÇEN ÜNİVERSİTESİ

BİLGİ İŞLEM DAİRE BAŞKANLIĞI

BİRİM FAALİYET RAPORU

İÇİNDEKİLER

BİRİM / ÜST YÖNETİCİ SUNUŞU

Kamu yönetiminin geliştirilmesi ve vatandaş odaklı, kaliteli, etkili v hızlı hizmet sunabilen; esneklik, saydamlık, katılımcılık, hesap verme sorumluluğu, öngörülebilirlik gibi çağdaş kavramları benimsemiş bir anlayışa, yapıya ve işleyişe dayanan bir sisteme dönüştürülmesi gerekli kılınmıştır. 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu'nun yayınlanmasıyla beraber veri ve bilgiye dayalı bir yönetimin gerekliliği, kaynakların etkin bir şekilde kullanılıp kullanılmadığının izlenmesi ihtiyacı söz konusu olmuştur. Bunun sonucu olarak hazırlanan faaliyetlerimiz ve projelerimiz sorumlu olan birilerin ilgili olduğu kanun ve yönetmelik çerçevesinde önceliklere göre planlanmış olup, idari ve mali kaynaklarımız ilgili kanunlar ve yönetmeliklerin hükümlerine göre kullanılacaktır.

Üniversitemize ait tüm birimlerin Bilgi Teknolojileri konularında ki ihtiyaçlarının güvenli, kaliteli ve ekonomik olarak karşılanmasını sağlamak için çalışmak öncelikli amacımızdır.

Bu amaçla Bilgi İşlem Daire Başkanlığı birim faaliyet raporu 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunun 41' inci maddesine dayanılarak, Maliye Bakanlığı tarafından düzenlenen kamu idarelerince hazırlanacak faaliyet raporu hakkında yönetmelik gereğince hazırlanmıştır.

Adı Soyadı : Ömer OKUCU

Unvanı : Daire Başkan V.

İmza

I- GENEL BİLGİLER

A. Misyon ve Vizyon

Misyon

Üniversitemiz akademik ve idari birimler ile öğrencilerin ihtiyaç duyacağı bilişim hizmetleri ve servislerinin karşılanmasında, mevcut ve doğacak ihtiyaçlara sorunsuz cevap veren, sürekliliği olan yazılımsal ve donanımsal çözümleri üretmek, temin etmek ve bu amaçla yeni bilişim teknolojilerini üniversitemize kazandırarak, kontrol ve koordinasyon yoluyla etkin ve verimli bir şekilde kullanımı ve devamlılığını sağlamaktır.

Vizyon

Bilişim teknolojileri konusundaki gelişmeleri yakından izleyerek üniversitemizin teknolojik alt yapısını sürekli geliştirmek, tüm birimlerde yaygın olarak faydalanılmasını sağlamak, bilişim hizmetlerinin yürütülmesinde ve paydaşlarına sunumunda teknolojik alt yapısı ve hizmet kalitesi açısından ülkemizin önde gelen ve teknolojik gelişmişliği açısından tercih edilen üniversiteleri arasında olmaktır

B. Yetki, Görev ve Sorumluluklar

Başkanlığımız, üniversitenin bilgisayar, kablolu ve kablosuz internet hizmetleri , bilgi sistemleri desteği, işletim sistemi ve Office 365, teknik servis, mail, web sayfası, siber güvenlik altyapısı, telefon ve santral, kamera altyapısı, bilgi güvenliği , kvkk , grafik tasarım ve baskı, online eğitim altyapı hizmetlerini yürüten idari faaliyet birimidir. Başkanlık olarak en güncel teknolojileri takip ederek tüm personel ve öğrencilerimize eğitim ve akademik çalışmalarında optimum yarar sağlayacak şekilde planlanan hizmetleri sunmakla yükümlüdür. Tüm kullanıcılarına en son bilişim teknolojilerini kullanarak çağdaş hizmet vermeye gayret etmekte; üniversite öğrenci ve personeli ile tüm birimlere e-posta, web, mobil erişim, sunucu, yazılım, teknik servis ve ofis hizmetleri sunmaktadır.

Başkanlığımız sorumluluğunda sunulan internet ve web hizmetleri ile üniversitemizin yurt içi ve dışına tanıtımı en olgun düzeyde sağlanmakta gerçekleştirdiğimiz yazılım üretme, bakım ve teknik servis hizmetleri ile üniversitemiz ve devlet bütçesinde önemli oranda tasarruf sağlarken, idari işleyişin şeffaf ve düzenli olmasına da büyük katkı sağlamaktadır.

Verilen hizmetlerin kalite ve verimini arttırmak amacıyla yürütülen ve geliştirilmeye çalışılan faaliyetlerimiz ana hatları ile şunlardır:

Sunucu Yönetimi ve Konfigürasyonları

Kurumun ihtiyaç duyduğu uygulamaların çalıştırılabilmesi için sunucu kurulum ve yapılandırma işlemlerini yerine getirmek. (Mail Sunucusu,EBYS, PDKS ve yemekhane uygulama sunucusu, Öğrenci İşleri Otomasyonu, Kütüphane Otomasyonu ve Açık Erişim Sistemleri İşlemleri , Nas sunucu kurulumu ve konfigürasyonu ,Storage yapılandırma ve yönetme , uzaktan eğitim merkezi sunucu işlemleri , Sanal Sunucu İşlemleri gibi ihtiyaca binaen oluşabilecek diğer talepler ile bunlarda yaşanan sorunların giderilmesi noktasında sunulan hizmetleri yönetmek.

Kablolu ve Kablosuz İnternet Hizmetleri

Üniversitemizdeki öğrenciler ve tüm birimlerimizin internet hizmetinden faydalanması için kablosuz cihazların kurulum ve yapılandırma işlemleri

Tubitak-Ulakbim Hizmetleri İnternet Alt yapısı sunulması işlemleri

İnternet bağlantı hızının arttırılması ve Tubitak Ulakbim hizmetlerinin kurumumuzda kullanılması Networkümüzü kullanan tüm cihazların oluşturmuş olduğu veri trafiğini grafike edip, Ulakbime göndermek.

Firewall Konfigürasyonu ve Yönetimi
Üniversitemizin network güvenliğini yapılandırma işlemleri, kurum içine dışarıdan erişim ve dışarıya kurum içinden erişim noktalarının yapılandırılması

Eduroam Hizmeti
Uluslararası akademik internet hizmetinin sunulması ve bu ağdaki kurumlara dolaşım serbestliği sunulması

Proxy Hizmetinin Sunulması
Kurumdışındaki personelin kurum içinde sunulan hizmetlerden faydalanması için proxy sunucu kurulumu ve konfigürasyon işlemleri

Switch Konfigürasyonları (Ağ kurulum işlemleri)
Mevcut ve yeni kurulan kurum binalarına network altyapsını sağlamak üzere switch kurulum vekonfigürasyonunun yapılması (Patch Panel Sorunlarının giderilmesi, Bina içi kablo sorunları nın çözülmesi RJ-45 sonlandırma işlemleri)

Ağ üzerinden çalışan tüm servislerin iş sürekliliğin sağlanması, kesintiler yaşanmaması için gerekli çalışmalar yapmak

Bilişim güvenliği konusunda prosedür , politika ve talimatlar vb. gibi çalışmalar yapmak.

Siber güvenlik çalışmalarını yürütmek.

Binalar arasındaki fiber optik hatları planlamak, fiber sonlandırma, katlar arası fiber yapısını , binalardaki ağ yapılarını (sistem odası , kabinler , kablolama altyapısı, kablosuz ağ vb.) yönetimini yapmak.

E-posta , Dns , Dhcp, Log Analizi ve Yönetimi , Vekil Sunucu , Sanallaştırma Teknollojilerini , Alan Yönetiminin Yönetimini sağlamak.

Sanallaştırma, Depolama, arşivleme, storage ve yedekleme sistemlerini yönetmek.

Uzaktan eğitim, Bap Otomasyonu, Kartlı Geçiş Kontrol sistemleri, Harcama noktaları, Ebys, Obs, Personel Yönetim Sistemi gibi sunucu üzerinde çalışan kurumumuzun bilgi sistemlerinin ihtiyaç duyduğu altyapı desteğini sağlamak.

İp Telefon ve İp Fax sistemlerini yönetmek

İp güvenlik kamerasına ait sunucu , ağ ve depolama hizmetlerini yürütmek

Üniversitemiz genelinde kullanılan lisanslı yazılımların, lisans sunucularının yönetimlerini yapmak

Sunucu ve ağ cihazları ile ilgili felaket senaryoları oluşturmak, düzenli olarak yedek almak.

Vpn uzaktan erişim ve port yetkilendirmelerini yönetmek

Uygulama sunucularının veritabanlarını yönetmek

Some – Bome olaylarına müdahale ve gerekli koordinasyonu sağlamak

Kurumumuzun envanterinde yer alan ağ cihazlarının İp Mac adresi bilgilerini hazır bulundurmak.

Tüm ağ topolojisini haritalandırmak, kritik bilgi sistemlerinin varlık envanterini çıkarmak.

Binalarda hizmet veren anahtarların switch – port etiketlendirme çalışmalarını yürütmek.

Bilginin gizliliği, bütünlüğü ve erişilebilirliğinin sağlanması ve kişisel mahremiyetin korunması noktasında gerekli tedbirleri almak.

Ağ trafik analizinin yapılması, ağ trafiğini olumsuz etkileyen nedenlerin tespit edilmesi, ağ trafiğinin kalitesini etkileyen, istenmeyen trafik oluşturarak sistemin çalışırlılığını bozan kullanıcıların tespit edilmesi

Saldırı tespit sistemleri, FKM, bilişim alanındaki güvenlik ile ilgili yenilikleri, antivirüs politikaları ile ilgili gerekli çalışmaları koordine etmek devreye alınmasını sağlamak

İp adreslerinin organizasyonunu sağlamak, sınıflandırmak, ağları alt ağlara ayırmak.

Kurumda bilgi güvenliği politikalarının uygulanmasını, SOME ve USOM'la koordinasyonu sağlamak.

Mevzuattan kaynaklanan insan kaynakları güvenliğinin sağlanması, bilgi güvenliğinin sağlanması, denetim kayıtları tutulması, lisanslı yazılım kullanılması vb. bilgi güvenliği önlemleri alınması

Manyetik kart vb. kimlik doğrulama yöntemleri vb. gibi kontrol yöntemleri ile sistem odalarının güvenliği sağlanmalıdır. Sistem odalarının sıcaklık, nem vb. çevresel şartları sağlanmalı, yangın, sel vb. olaylara karşı önlemler alınması

En az iki yılda bir kez bilgi sistemlerine açıklık analizi ve sızma testi yaptırılması, elde edilen sonuçlar uyarınca düzeltmelerin gerçekleştirilmesi ve sürecin yönetmesi

Tespit edilen ihtiyaçlar doğrultusunda gerekli bütçenin planlanması, analitik bütçe kodlarına aktarılacak parayı kalem bazında sınıflandırmak.

Kamu harcama ve Muhasebe Bilişim sistemi üzerinden (KBS)

Taşınır Mal Yönetim Sistemi Uygulamalarının (TKYS) birim içinde takip edilmesi, uygulanması

Taşınır Mal yönetim sistemi kapsamında TKYS Sistemi üzerinde marka tanımları , ölçü birim tanımlama işlemleri , firma ve malzeme ek özellik tanımlamaları , ambar tanımlama ,Taşınır Kod listesi malzeme tanımlamaları , istek birimi tanımlama , kişi tanımlamaları , rol ve yetki atamaları , yerleşim birimi tanımlamaları , taşınır mal giriş ve çıkış işlemleri , satın alma , bağış yardım alma , devir alma, iade işlemleri , envanter giriş işlemleri ile devretme suretiyle çıkış işlemi , ambarlar arası devir işlemi, satış ve kayıttan düşme işlemleri , onaylı ve onaysız tiflerin düzeltilmesi işlemleri , zimmet işlemleri , zimmete verme zimmet iadesi yapma , mevcut ambardaki ürünlerin listesini ve raporlama seçeneklerinin kullanılması , taşınır istek talepleri ve bu taleplerin karşılanması , defterler ve cetveller ,tutanaklar , ambar devir

işlemleri ,, sayım ve yıl sonu iş ve işlemleri , yıll sonu kapatma işlemlerini TKYS sistemi üzerinden yürütmek.

Gelen- giden evrak kayıt, evrakların dosyalanması, sınıflandırılması, arşiv işlerinin yürütülmesi kurum içi ve dışı yazışmaların takibini resmi yazışma kurallarına göre yapmak.

İhtiyaç duyulan malzemelerin temini ve tesipinin yapılması, onay işlemlerinin takibi, tekliflerin verilmesi ve alınması, piyasa araştırmasının yapılması, uygun teklifin kabul edilmesi, mal ve hizmetin teslim alınması, teslim alınan mal ve hizmetin muayene ve kabul komisyonu işlemleri, taşınır kayıt sistemine işlenmesi, ve ödemesinin yapılmasının muhasebeleştirilmesi işlemlerini yürütmek.

Birim personellerinin kişisel ve özlük bilgilerininin düzenlenmesi, izin, rapor, görevlendirme, vb. gibi kayıtların tutulması ve dosyalanması.

Otomasyon bilgi sistemlerinin yıllık bakım anlaşmaları için bütçe hazırlamak, ve ödemeler ile ilgili tüm süreçleri takip etmek.

Birim personellerinin yolluk ödemelerini gerçekleştirmek.

Avans işlemlerini takip etmek, kapatmak.

İhale sürecini ve tüm işlemlerini yürütmek.

Kısmı Zamanlı çalışanların puantajlarının hazırlanması, ödeme yapılacak ilgili birime gönderilmesi.

Birim çalışanlarının mesai çizelgelerini hazırlamak ve ilgili birimlerlerce ödemenin yapılmasını sağlamak, takip etmek

Birim faaliyetlerinin dökümantasyon işlemlerini koordine etmek (talimatlar hazırlama, prosedürler belirleme, politikalar oluşturma koordine etme).

Birim faaliyet raporunun hazırlanması

İç Kontrol Standartları Uyum eylem planının hazırlanmasını takip etmek

Birim stratejik planının hazırlanması

Birimde göreve başlayan personellerin sigortalı işe giriş bildirgelerinin hazırlanması, sigorta giriş ve çıkış işlemlerinin yürütülmesi

Birimin randevu, ziyaret, toplantı, günlük programı, ulaşım, iletişim, vb. gibi sekreterya hizmetlerini yürütmek.

Sms ileti merkezi yönetimi
Elektronik Belge yönetim sistemi kullanıcılarına gerekli eğitimin verilmesi, Birim ebys sorumluları aracılığıyla sistemin üniversite bünyesinde kullanılabilir durumda olmasını sağlamak yaşanan sorunlara çözüm üretmek

Kamu Sertifikasyon merkezi nitelikli elektronik sertifika iş ve işlemleri Ebys e-imza süreçleri ve bunların yönetimini sağlamak

Güvenlik sözcüğü sıfırlama işlemleri
Sürücü yükleme işlemleri
Java ve kullancı hesabı denetim ayarları
Nitelikli elektronik sertifika ıslak imzalı başvuru formunun dolduruluması
Başvuru erişim parolası işlemleri
E-imza flash ı kilit çözme
Pin puk bilgisi öğrenme işlemleri
Ebys sistemi kullanıcı desteği kullanıcı ekleme-çıkarma vekalet, izin talep formu, Dilekçe oluşturma, sayfa ile ilgili ayarlamalar yapma
E-imza flash kayıp ve tekrar başvuru işlemleri
Ebys sistemi kullanım kılavuzu oluşturma, Sistem Ayarları, sistem konfigürasyonu, evrak tanımları, kep ayaları, ocr ayarları, kurum haberleri, menü işlemleri, portal arayüz yönetimi, arşiv işlemleri, standart dosya planı ve saklama sürelerinin tanımlanması, evrak şablonları, entegrasyon ayarları gibi sistemin arka planını yönetmek işlevsel hale getirmek.
Nes Raporlama Arayüzü sayfası üzerinden Nes Kullanım sürelerini takip etmek ve gerekli önbaşvuru işlemleri yapmak.

Üniversitemiz web sayfası ve alt birim sayfalarında yayınlanan duyuru, ders, vize, final, bütünleme programı ve haber duyuruları, personel alım ilanları, haberleri ve etkinliklerin yayınlanması

Üniversitemiz dışındaki kurumların bilimsel amaçlı duyurularını ilgili sayfalarda yayınlamak

Birimlerimizden gelen ve tüm idari ve akademik personelin bilgilendirilmesi istenen duyuruların toplu posta yoluyla iletilmesi

Üniversitemiz web sayfalarının kategori, içerik, sayfa yönetimi güncellemelerini yapmak ve destek sağlamak

Kullanıcılara ait web sayfasında bulunan personel bölümünü güncel ve dinamik tutulması; akademik personel bürosundan gelen atama, ayrılma ve ünvan değişikliklerini elektronik ortamda güncellemek.

Akademik personelin web sayfalarını güncellemede karşılaştıkları sorunları çözmeye çalışmak. Güncellemeyi bazen bizzat yaparak, Filezilla Ftp programının bağlantı ayarları hakkında bilgi verip güncellemeyi yapmak.

Üniversitemiz Yönetim Kurulu ve Senato listelerinde yapılan değişiklikleri web sayfasında güncellemek.

Ana sayfamızda yer alan kongre, sempozyum, panel ve etkinlik duyurularının yapılması

Web Sayfası Oluşturma
Ünivesitemiz bünyesinde faaliyet gösteren idari ve akademik birimlerin web sayfalarının içeriğinin oluşturulması ve teslim edilmesi

Web Sayfası İçerik Yönetimi (Duyuru, Haber,Fotoğraf galerisi,)

Web sayfasında yayınlanılacak duyuru , haber etkinlikler ve web arayüzü oluşturulması

Web İletişim araçlarının servise sunulması

Üniversite bünyesindeki tüm birimlerin iletişim formları, elektronik listeleri, telefon rehberi vb. hizmetlerin sunulması

Web sayfası birim yöneticisi eğitimi ve şifre işlemleri bütün birim web sayfalarının oluşturulmasından sonra her birim bünyesinde görevlendirilen web birim sorumlusu aracılığyla ilgili birimin web hizmetlerinin sağlanması için eğitim verilmesi tarafına şifre oluşturulması

Grafik Tasarım ve Baskı Hizmeti
Ünivestemiz tarafından düzenlenen sempozyum, etkinlik, kongre ve diğer etkinlikler ile ilgili hizmet verilecek diğer işlerin logoların, afişlerinin, tasarımlarının hazırlanması

Personel Devam Takip Kontrol Sistemi Yönetim Ve Kurulum Işlemleri
Personel giriş ve çıkış işlemlerinin kontrol edilebilmesi için idari ve akademik birimler bazında belirlenen yöneticilere parola oluşturulması, bunların yaşayacak oldukları sistem ile ilgili sıkıntılarına çözüm üretilmesi ve yeni kurulan birimlere kart okuyucuların monte edilmesi devreye alınması ve yaşanan sorunların giderilmesi

Personel Kimlik Kartı Tanımlama Işlemleri
Personel Kimlik kartlarının PDKS sistemi kapsamında kullanılabilir hale getirilmesi için formatlanması, sisteme tanımlanması
Turnike sistemlerinin kontrol edilmesi, kurulması veya değiştirilmesi

Yemekhane bünyesinde bulunan turnikler ile ilgili ouşan sorunları gidermek, sistemin her daim çalışabilir durumda olmasını sağlamak.

Hgs Kurulum İşlemleri
Hızlı Geçiş Güvenlik sistemi bünyesinde ilgili yerlere sistemin devreye alınması, kurulum işlemleri arızalı kartların değişimi

Turnike sistemlerinin kontrol edilmesi, kurulması veya değiştirilmesi
Yemekhane bünyesinde bulunan turnikler ile ilgili ouşan sorunları gidermek, sistemin her daim çalışabilir durumda olmasını sağlamak.

Nakit Yükleme Kioskları sorunlarına destek sağlamak

Kurumsal E-Posta Açma Ve Kapama Işlemleri
Üniversitemizde göreve başlayan idari ve akademik personellerin hepsine kurumsal mail adresleri tanımlanması

Mail Adresi parola sıfırlama işlemleri

Talep doğrultusunda kullanıcıların şifre bilgilerinin güncellenmesi

E-mail kullanım klavuzu oluşturmak, mail sisteminin aktif olarak kullanılabilmesi için gerekli Altyapı ve eğitim bilgilendirme desteğini sağlamak.

Dağıtım grupları oluşturmak, tüm kuruma bir mail adresiyle mail gönderilmesini sağlamak.

Office 365 kurulum ve lisans desteği sağlamak

Kamera kayıtlarının görüntü talebi işlemleri ,Cd ye aktarımları

Kamera sistemi bilgisayardan izleme talepleri

Kamera sistemi kurulum talepleri

Kamera arızaları Bakım ve onarım talepleri

Kamera kayıtlarının geçmiş tarihli verilerine erişim talebi

Telefon arızaları

Telefon Kurulumları

Telefon Kablosu Çakma işlemi

Reji odalarının kilit altında tutulması,

Ses sistemleri ve donanımlarının (bilgisayar, mikser, mikrofon, hoparlörler, kürsü; internet, ses ve görüntü kabloları ve ara parçaları, vb.) çalıştırılması, etkinliklerde kullanılması,

Salonların internet bağlantısının sürekliliğinin sağlanması,

Etkinlikler öncesinde prova ve test işlemlerinin yürütülmesi,

Etkinlikler sırasında program sonuna kadar takibinin yapılması,

Etkinlikler sonunda da kapatılıp güvenlik altına alınması,

Diğer zamanlarda sistem ve donanımlarının sürekli hizmete hazır tutulması amacıyla bakım ve destek çalışmalarının yapılması,

Sistem arızaların ve eksikliklerin tespit edilerek başkanlık makamına sözlü ve yazılı olarak bildirilmesi,

Ünivesitemiz idari ve akademik personellerinin bilgisayarlar ile ayrıca laboratuvar bünyesinde kurulu olan bilgisayar ve çevre birimlerinin (bilgisayar , yazıcı, tarayıcı ,projeksiyon, Led Tv, Akıllı Tahta , sistem formatlama , yazılım kurulum işlemleri bakım ,onarım ve güncelleme ve destek işlemleri ,

Bilgisayar Kurulum Hizmetleri (Format ve Sistem Bileşenleri Kurulumu)

Donanım Arızaları ve Yazılımdan kaynaklanan hataların giderilmesinde kullanıcı desteği

Üniversitemizdeki birimlerden gelen talepler doğrultusunda alımı yapılacak bilgisayar ve sarf malzemeler için teknik şartname hazırlanması

Talimatlar hazırlamak , (Bilgisayar ve bileşenlerinin kullanımı ile ilgili talimatlar)

Talep doğrultusunda teknik şartname hazırlamak , teknik şartname desteği vermek

Kültür ve Kongre Merkezi bünyesinde düzenlenen seminer , konferans, vb. etkinlerde salonun kullanılabilir durumda olmasını sağlamak.

C. İdareye İlişkin Bilgiler

Başkanlığımız kurum organizasyon yapısında Genel Sekreterlik Makamına bağlı olarak çalışır.
Ağrı İbrahim Çeçen Üniversitesi Bilgi İşlem Dairesi Başkanlığı 2007 yılında faaliyetine başlamıştır. Başkanlığımız çalışmalarını, Ağrı İbrahim Çeçen Üniversitesi'ni iyi yönetilen bir üniversite haline getirmek için çalışmaktadır. Yapılan çalışmaların tamamı merkezi bilgi sistemine eklenerek genişletilmektedir.
Bilgi İşlem Daire Başkanlığı, üniversitemiz Kongre ve Kültür Merkezi binasında bulunmaktadır.
Başkanlık en güncel teknolojileri takip ederek tüm öğrenci ve personelimize eğitim ve akademik çalışmalarında optimum yarar sağlayacak şekilde planlanan hizmetleri sunmakla yükümlüdür. Yaklaşık 13.000 öğrenci ve 1.000 personelle en son bilişim teknolojilerini kullanarak çağdaş hizmet vermeye gayret etmekte Üniversite öğrenci ve personeli ile tüm birimlere e-posta, web, mobil erişim, sunucu, yazılım, teknik servis ve ofis hizmetleri sunmaktadır. Başkanlığımız sorumluluğunda verilen internet ve web hizmetleri ile Üniversitemizin yurt içi ve dışına tanıtımı üst düzeyde sağlanmakta, gerçekleştirdiğimiz yazılım, bakım ve teknik servis hizmetleri ile Üniversitemiz ve devlet bütçesinde önemli oranda tasarruf sağlarken, idari işleyişin şeffaf ve düzenli olmasına da büyük katkı sağlamaktadır.

1.2. Eğitim Alanları

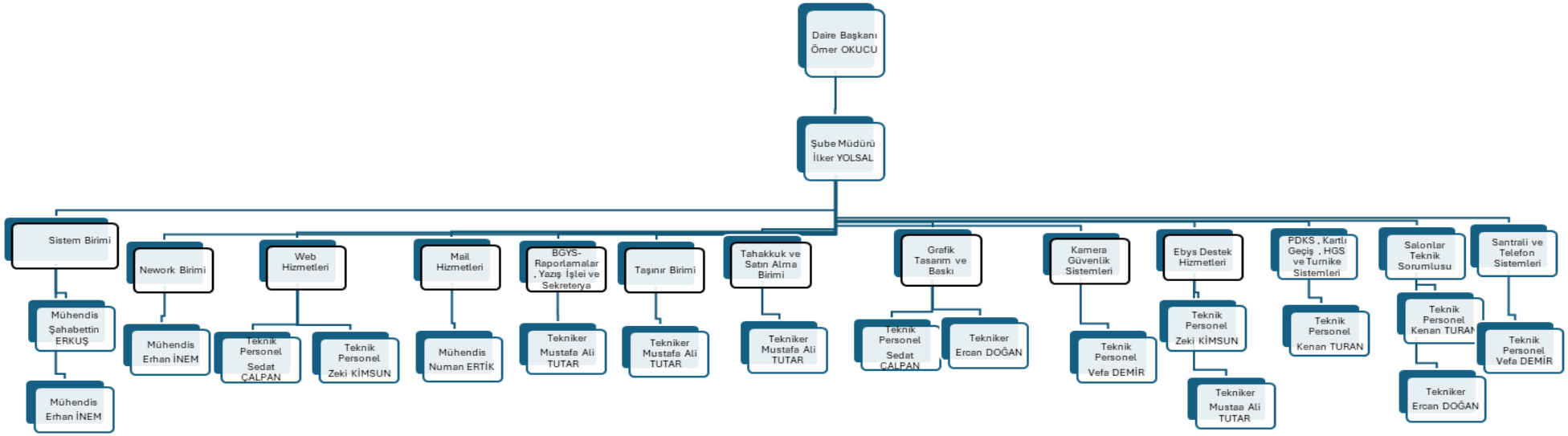
Eğitim Alanı Sayıları

Eğitim Alanı		**Kapasite 0–50**	**Kapasite 51–75**	**Kapasite 76–100**	**Kapasite 101–150**	**Kapasite 151–250**	**Kapasite 251-Üzeri**	**Toplam**
Amfi								
Sınıf								
Atölye			1					1
Diğer (……..)								
Laboratuvarlar	**Eğitim Laboratuvarları**							
	Sağlık Laboratuvarları							
	Araştırma Laboratuvarları							
	Diğer (……)							
TOPLAM			1					1

1.5. Toplantı ve Konferans Salonu Sayıları

Toplantı ve Konferans Salonu Sayıları

	Kapasitesi					
	0–50	51–75	76–100	101–150	151–250	251+
Toplantı Salonu	1					1
Seminer Salonu						
Konferans Salonu	3					3
Toplam	4					4


Daire Başkanı
Ömer OKUCU
Şube Müdürü
İlker YOLSAL
Sistem Birimi
Mühendis
Şahabettin
ERKUŞ
Mühendis
Erhan İNEM
Nework Birimi
Mühendis
Erhan İNEM
Web
Hizmetleri
Teknik
Personel
Sedat
ÇALPAN
Teknik
Personel
Zeki KİMSUN
Mail
Hizmetleri
Mühendis
Numan ERTİK
BGYS-
Raporlamalar
, Yazış İşlei ve
Sekreterya
Tekniker
Mustafa Ali
TUTAR
Taşınır Birimi
Tekniker
Mustafa Ali
TUTAR
Tahakkuk ve
Satın Alma
Birimi
Tekniker
Mustafa Ali
TUTAR
Grafik
Tasarım ve
Baskı
Teknik
Personel
Sedat
ÇALPAN
Tekniker
Ercan DOĞAN
Kamera
Güvenlik
Sistemleri
Teknik
Personel
Vefa DEMİR
Ebys Destek
Hizmetleri
Teknik
Personel
Zeki KİMSUN
Tekniker
Mustaa Ali
TUTAR
PDKS , Kartlı
Geçiş , HGS
ve Turnike
Sistemleri
Teknik
Personel
Kenan TURAN
Salonlar
Teknik
Sorumlusu
Teknik
Personel
Kenan TURAN
Tekniker
Ercan DOĞAN
Santrali ve
Telefon
Sistemleri
Teknik
Personel
Vefa DEMİR

3- Bilgi ve Teknolojik Kaynaklar

3.1. Teknolojik Kaynaklar

Teknolojik Kaynaklar	2023 (Adet)
Masaüstü Bilgisayar	**14**
Dizüstü Bilgisayar	22
Tablet Bilgisayar	3
Ekranlar	24
Tutucular	4
Projeksiyon Cihazları	3
Yazıcılar	8
Tarayıcılar	4
Fotokopi Makinesi	-
Faks Makinesi	-
Switch (Anahtarlar)	37
Televizyon	8
Kart Okuyucu	6
Baskı Makinesi	-
Access Point Kablosuz Erişim Cihazı Modemler	7
Sabit Telefon	9
Fotoğraf Makinesi	-
Kesintisiz Güç Kaynağı	1
Dijital Kameralar, Sabit Kameralar, Güvenlik Kameraları	9
Ağ Cihazları Kabini	4
Dijital Kayıt Sistemleri , Kamera Kayıt Sistemleri	3
Patch Panel	9
Gbig Modüller	29
Harici Harddisk	2
Üç Kollu Turnike (İç Ortam)	1
Kiosk Sistemler	1
Fiber Ek Aleti (Fujikira)	1
Yüz Tanıma Cihazı	1
Ağ Kontrol Cihazı	1
Fiber Işık Kaynağı	2
Firewall Chechpoint T-150	1
Palo Alto 3410 Donanım Cihazı	1
TOPLAM	**224**

3.2. Kullanılan yazılımlar

Birim Adı	Kullanılan Yazılım Programları
Bilimsel Araştırma Projeleri Birimi	Bap otomasyon sistemi
Yapı İşleri ve Teknik Daire Başkanlığı	Oska e hakediş ve yaklaşik maliyet programi
Yapı İşleri ve Teknik Daire Başkanlığı	Amp kurumsal hakediş ve yaklaşik maliyet program
Öğrenci İşleri ve Sks Daire Başkanlığı	Öğrenci konseyi seçim otomasyonu
Bilgi İşlem Daire Başkanlığı	Annual maintanence renewal expired - veam backup@replication standart for vmware
Bilgi İşlem Daire Başkanlığı	Annual maintanence renewal expired - fee waived veeam backup@replication standart for vmware
UZEM	Arcgis for destop advanced concurrent use educational Teaching lab pk 31 pack license
UZEM	Adobe connect platinium spt. Rnwl lisans
UZEM	Adobe connect tam plt.-spt rnwl
UZEM	Adobe connect named host edu yazilim lisansi
UZEM	Adobe connect plt.spt.named host 12 m
UZEM	Maadle tier 2. Spt rnwl
Öğrenci İşleri Daire Başkanlığı	Karekod ve ders program yazilim entegrasyonu
Bilgi İşlem Daire Başkanlığı	Annual basic maintenance renewel - Veeam backup@replication standart for wmvare
Bilgi İşlem Daire Başkanlığı	Monthly basic maintenance renewal - Veeam backup@ veeam backup@ replication sdantart for wmware- education only
Bilgi İşlem Daire Başkanlığı	2 additional years of basic maintenance prepaid for Veeam backup@replication standart for wmware
Ebys Sistemi çatısı altında Tüm Birimler ve Yazı İşleri Şube Müdürlüğü	E- yazişma paketi ve kep entegrasyonu sistemi
Bilgi İşlem Daire Başkanlığı – Tüm Birimleri kapsıyor	Ov-premium wilcard ssl sertifa yazilimi
Bilgi İşlem Daire Başkanlığı	Dwc-2000 d-link dwc 2000 wireless controller
Bilgi İşlem Daire Başkanlığı	Dwc-2000 - ap128 d-link ek lisans
Bilgi İşlem Daire Başkanlığı	Fortinet fortigate 600 d Ağ güvenik duvari yazilimi (firewall)
Bilgi İşlem Daire Başkanlığı	Aruba 7210 kit/3y kablosuz ağ kontrol cihazi
Bilgi İşlem Daire Başkanlığı	Ağ yönetim yazilimi (imc)
Bilgi İşlem Daire Başkanlığı - Tüm Birimleri kapsıyor	Desktop education
Bilgi İşlem Daire Başkanlığı - Tüm Birimleri kapsıyor	Windows server ca
Bilgi İşlem Daire Başkanlığı - Tüm Birimleri kapsıyor	Exchange std. Cal

Bilgi İşlem Daire Başkanlığı- Tüm Birimleri kapsıyor	Share point std. Cal
Bilgi İşlem Daire Başkanlığı- Tüm Birimleri kapsıyor	Sccm client ml
Bilgi İşlem Daire Başkanlığı- Tüm Birimleri kapsıyor	Lyne std. Cal
Bilgi İşlem Daire Başkanlığı- Tüm Birimleri kapsıyor	System center endpoint protection (antivirüs)
Bilgi İşlem Daire Başkanlığı- Tüm Birimleri kapsıyor	Office pro plus
Bilgi İşlem Daire Başkanlığı- Tüm Birimleri kapsıyor	Sql server standart core edition
Bilgi İşlem Daire Başkanlığı- Tüm Birimleri kapsıyor	Windows server datacenter core
Öğrenci İşleri Daire Başkanlığı	Öğrenci işleri bilgi sistemi
Bilgi İşlem Daire Başkanlığı – Tüm Birimleri Kapsıyor	Elektronik belge yönetim sistemi
Personel Daire Başkanlığı	Personel özlük işleri otomasyonu
Strateji Geliştirme Daire Başkanlığı	Ek ders otomasyon sistemi
Sağlık Kültür ve Spor Daire BAşkanlığ ı	Yemekhane sistemi yönetim modülü
Sağlık Kültür ve Spor Daire Başkanlığı	Fitness spor salonu uygulama yazilimi
Bilgi İşlem Daire Başkanlığı – BUYAMER	Web sitesi
Bilgi İşlem Daire Başkanlığı	Gözcü takip erken uyari sistemi- sistem odasi
Bilgi İşlem Daire Başkanlığı , Basın ve Halkla İlişkiler	Sms paket hizmeti
Personel Daire Başkanlığı ve Bilgi İşlem Daire Başkanlığı	Ebys -personel otomasyonu izin entegrasyonu
Kütüphane ve Dokümantasyon Daire Başkanlığı	Kütüphane otomasyonu (Yordam)
Kütüphane ve Dokümantasyon Daire Başkanlığı	Vidobu (video veritabani lisansi)
Kütüphane ve Dokümantasyon Daire Başkanlığı	Scifinder (veritabani lisansi)
Merkezi Araştırma ve Uygulama Laboratuvarı	Kartli geçiş sistemi- merlab
Merkezi Araştırma ve Uygulama Laboratuvarı	Numune kabul otomasyonu
Kütüphame ve Dokümantasyon Daire Başkanlığı	Rfid kitap ödünç iade sistemi Sciencefinder vidobu Ebscohost Emerald primier e-journa Jstor archive journal content Ieee Mendeley Nature journals ithenticate Proquest dissertations&theses Ovid-lww Scopus Web of science wiley Turnitin Taylor&francis Springerlink

	Sciencedirect
Kütüphane ve Dokümantasyon Daire Başkanlığı	Hiperkitap Veritabanı
Kütüphane ve Dokümantasyon Daire Başkanlığı	E-Osmanlıca Veritabanı
Kütüphane ve Dokümantasyon Daire Başkanlığı	Kelime-X Veritabanı
Bilgi İşlem Daire Başkanlığı	Personel devam takip kontrol sistemi
Öğrenci İşleri Daire Başkanlığı	Ösym e-kilavuz sistemi
İş Sağlığı ve Güvenliği Birimi	Iş sağliği ve güvenliği kayit, takip ve izleme programi
KBS	Bütünleşik kamu mali yönetim bilişim sistemi
	Tübitak tts sistemi
HYS	Kamu personeli harcamalari yönetim sistemi
Döner Sermaye İşletme Müdürlüğü	Döner sermaye Muhasebe otomasyon sistemi (dmis)
E-Devlet	Kamu elektronik bordro sistemi (e-bordro)
Öğrenci İşleri Daire Başkanlığı	Elektronik kamu bilgi yönetim sistemi (kaysis)
Kütüphane ve Dokümantasyon Daire Başkanlığı	Kütüphaneler arasi işbirliği sistemi (kits)
Kütüphane ve Dokümantasyon Daire Başkanlığı	Türkiye belge sağlama sistemi (tübess)
Kütüphane ve Dokümantasyon Daire Başkanlığı	Ulusal toplu katalog (to-kat)
İdari ve Mali İşler Daire Başkanlığı	Telefon santrali yönetim sistemi ve sunucusu (telesis)
Personel Daire Başkanlığı	Yükseköğretim kurulu ortak veritabani (yöksis)
Bilgi İşlem Daire Başkanlığı	Sophos (Mail , Firewall, Yeni nesil saldırı önleme tespit sistemi)
Bilgi İşlem Daire Başkanlığı	Squid proxy yazilimi
Bilgi İşlem Daire Başkanlığı	Sql server -my sql veritabani sunucusu
Bilgi İşlem Daire Başkanlığı	Office 365- Microsoft Teams
TKYS Bilgi Sistemi	Taşinir kayit kontrol sistemi
SAY 2000 Bilgi Sistemi Strateji Geliştirme Daire Başkanlığı	Say 2000i maaş sistemi
Strateji Geliştirme Daire Başkanlığı	E-bütçe
Strateji Geliştirme Daire bAşkanlığı	Kamu hesaplari bilgi sistemi
Meslek Yüksekokulu	Datasoft muhasebe programi
Öğrenci İşleri Daire Başkanlığı –Erasmus – Farabi	Bologna otomasyonu
Personel Daire Başkanlığı	Devlet personel başkanliği e-uygulama
Personel Daire Başkanlığı	Kimlik paylaşim sistemi
Konuk Evi	Konukevi misafir takip sistemi

E-Devlet – Personel Daire Başkanlığı	Sgk hizmet takip programi(hitap)
Bilgi İşlem Daire Başkanlığı	Kurumsal e-posta sistemi –zimbra e-posta yöneticisi
Uzem	Adobe connect
Uzem	Moodle
Uzem	Atom
Uzem	Sekoku – optik okuma programi
Uzem	Aiçuzem soru hazirlama ve kontrol programi
Uzem	Soru kitapçiği üretme programi
Uzem	Portal – sinav değerlendirme, sonuçlandirma ve giriş dokümani alma
Fen Edebiyat Fakültesi – Coğrafya Bölüm Başkanlığı	Gis (geographical information system) / esri firmasi – 10.2 sürümü –coğrafyabilgi sistemi fen edebiyat
Konuk Evi	Egm güvenlik sistemi (https://kbs.egm.gov.tr) – sks konuk evi
Öğrenci İşleri Daire Başkanlığı	Yatay Geçiş Başvuru ve değerlendirme sistemi
Konuk Evi	Otel programi (akinsoft otel s4.03.16) sks konuk evi –
Bilgi İşlem Daire Başkanlığı	Antivirüs Programı – Securitu Essential
Öğrenci İşleri Daire Başkanlığı	Tıp Fakültesi Modülü
Öğrenci İşleri Daire Başkanlığı	Yabancı Uyruklu Öğrenci Modülü
Bilgi İşlem Daire Başkanlığı	Elektronik Mühür Entegrasyonu
Bilgi İşlem Daire Başkanlığı	Palo Alto 3410 Firewall Yazılımı
Bilgi İşlem Daire Başkanlığı	Logsign SIEM ve Log Yönetimi

3. Kütüphane Kaynakları

Kütüphane Kaynakları

Kaynak Türü	2021 Yılında Alınan Kütüphane Kaynakları			Toplam Kütüphane Kaynakları		
	Basılı	Elelktronik	Toplam	**Basılı**	Elelktronik	Toplam
Kitap sayısı	-			22		22
Basılı ve veri tabanında yer alan süreli yayın sayısı	-					
Abone olunan süreli yayın sayısı	-					
Abone olunan very tabanı sayısı	-					
Yazma Eser	-					
Toplam				22		22

4- İnsan Kaynakları

4.2. İdari Personel Kadro Dağılımı

İdari Personelin Yıllar İtibariyle Kadro Dağılımı

	2022	**2023**
Genel İdare Hizmetleri	1	1
Sağlık Hizmetleri Sınıfı	0	
Teknik Hizmetleri Sınıf	4	4
Eğitim ve Öğretim Hizmetleri Sınıfı	2	2
Avukatlık Hizmetleri Sınıfı		
Din Hizmetleri Sınıfı		
Yardımcı Hizmetli	5	5

Toplam	**12**	**12**

4.2.1.Engelli İdari Personel Hizmet Sınıflarına Göre Dağılımı

Engelli Personelin Unvan ve Hizmet Sınıfına Göre Dağılımı

Hizmet Sınıfı	**Engelli Personel Sayısı**			**Toplam Personele Oranı(%)**
	K	**E**	**Toplam**	
Genel İdari Hizmetler				
Sağlık Hizmetleri Sınıfı				
Teknik Hizmetler Sınıfı				
Eğitim ve Öğretim Hizmetleri Sınıfı				
Avukatlık Hizmetleri Sınıfı				
Din Hizmetleri Sınıfı				
Yardımcı Hizmetler Sınıfı				
TOPLAM				

4.2.2.İdari Personelin Eğitim Durumu

İdari Personel Eğitim Durumu

	İlköğretim	**Lise**	**Ön Lisans**	**Lisans**	**Yüksek Lisans ve Doktora**	**TOPLAM**
Kişi Sayısı		2	4	4	2	12
Yüzde (%)		%16.66	%33.33	%33.33	%16.66	100

4.2.3. İdari Personelin Hizmet Süreleri
İdari Personel Hizmet Süresi

	1-3 Yıl		4-6 Yıl		7-10 Yıl		11-15 Yıl		16-20 Yıl	21-Üzeri			TOPLAM
	K	E	K	E	K	E	K	E	K	E	K	E	
Toplam Kişi Sayısı				**1**		**5**		**6**					**12**
Yüzde (%)	**%**	**%**		**%8.33**		**%41.66**		**%50**					**100**

4.2.4.İdari Personelin Yaş İtibariyle Dağılımı

İdari Personel Yaş İtibariyle Dağılımı

	21–25 Yaş		26–30 Yaş		31–35 Yaş		36–40 Yaş		41–50 Yaş		51-Üzeri		TOPLAM
	K	E	K	E	K	E	K	E	K	E	K	E	
Toplam Kişi Sayısı						**3**		**5**		**3**			**12**
Yüzde (%)						**%25**		**%41.66**		**%33.33**			**100**

5.2-İdari Hizmetler
Tespit edilen ihtiyaçlar doğrultusunda gerekli bütçenin planlanması, analitik bütçe kodlarına aktarılacak parayı kalem bazında sınıflandırmak.

Kamu harcama ve Muhasebe Bilişim sistemi üzerinden (KBS)Taşınır Mal Yönetim Sistemi Uygulamalarının (TKYS) birim içinde takip edilmesi, uygulanması

Taşınır mal yönetim sistemi kapsamında TKYS sistemi üzerinde marka tanımları , ölçü birim tanımlama işlemleri , firma ve malzeme ek özellik tanımlamaları , ambar tanımlama ,taşınır kod listesi malzeme tanımlamaları , istek birimi tanımlama , kişi tanımlamaları , rol ve yetki atamaları , yerleşim birimi tanımlamaları , taşınır mal giriş ve çıkış işlemleri , satın alma , bağış yardım alma , devir alma, iade işlemleri , envanter giriş işlemleri ile devretme suretiyle çıkış işlemi , ambaralar arası devir işlemi , satış ve kayıttan düşme işlemleri , onaylı ve onaysız tiflerin düzeltilmesi işlemleri , zimmet işlemleri , zimmete verme zimmet iadesi yapma , mevcut ambardaki ürünlerin listesini ve raporlama seçeneklerinin kullanılması , taşınır istek talepleri ve bu taleplerin karşılanması , defterler ve cetveller, tutanaklar , ambar devir işlemleri, sayım ve yıl sonu iş ve işlemleri , yıll sonu kapatma işlemlerini TKYS sistemi üzerinden yürütmek.

Gelen- giden evrak kayıt, evrakların dosyalanması, sınıflandırılması, arşiv işlerinin yürütülmesi kurum içi ve dışı yazışmaların takibini resmi yazışma kurallarına göre yapmak.

İhtiyaç duyulan malzemelerin temini ve tesipinin yapılması, onay işlemlerinin takibi, tekliflerin verilmesi ve alınması, piyasa araştırmasının yapılması, uygun teklifin kabul edilmesi, mal ve hizmetin teslim alınması, teslim alınan mal ve hizmetin muayene ve kabul komisyonu işlemleri, taşınır kayıt sistemine işlenmesi, ve ödemesinin yapılmasının muhasebeleştirilmesi işlemlerini yürütmek.

Birim personellerinin kişisel ve özlük bilgilerininin düzenlenmesi, izin, rapor, görevlendirme, vb. gibi kayıtların tutulması ve dosyalanması.

Otomasyon bilgi sistemlerinin yıllık bakım anlaşmaları için bütçe hazırlamak, ve ödemeler ile ilgili tüm süreçleri takip etmek.

Birim personellerinin yolluk ödemelerini gerçekleştirmek.

Avans işlemlerini takip etmek, kapatmak.

İhale sürecini ve tüm işlemlerini yürütmek.

Kısmı Zamanlı çalışanların puantajlarının hazırlanması, ödeme yapılacak ilgili birime gönderilmesi.

Birim çalışanlarının mesai çizelgelerini hazırlamak ve ilgili birimlerlerce ödemenin yapılmasını sağlamak, takip etmek

Birim faaliyetlerinin dökümantasyon işlemlerini koordine etmek (talimatlar hazırlama, prosedürler belirleme, politikalar oluşturma koordine etme).

Birim faaliyet raporunun hazırlanması

İç Kontrol Standartları Uyum eylem planının hazırlanmasını takip etmek

Birim stratejik planının hazırlanması

Birimde göreve başlayan personellerin sigortalı işe giriş bildirgelerinin hazırlanması, sigorta giriş ve çıkış işlemlerinin yürütülmesi

Birimin randevu, ziyaret, toplantı, günlük programı, ulaşım, iletişim, vb. gibi sekreterya hizmetlerini yürütmek.

5.3-Diğer Hizmetler

Birim tarafından 2023 yılında görev alanına giren faaliyetler dışında yapmış olduğu herhangi bir çalışma bulunmamaktadır.

6- Yönetim ve İç Kontrol Sistemi

İç Kontrol çalışmaları kapsamında 2023 yılı kapsamında birimimiz sorumluluğundaki tüm iş ve işlemler akademik ve idari birimlerimizin ihtiyaç ve taleplerine cevap verecek ölçüde birim içi belirlenen görev dağılım çizelgeleri, yazılı prosedür ve kanunlar göz önüne alınarak yürütülmüştür. Bu çerçevede birim içi etik kurallar oluşturulmuş ve personele duyurulmuştur. İç Kontrol el kitabı üniversitemiz web anasayfasında yayınlanmıştır. Birim websayfasında iç kontrol için menü oluşturularak ilgili belge ve bilgilere erişim sağlanmıştır. Hassas görevler ve envanterleri, risk belirleme ve analiz çalışmaları yapılmıştır. Bununla birlikte birimimizde gerçekleşen yazışmalar EBYS üzerinden yürütülmekte olup; arşivleme işi bu sistem üzerinden yürütülmektedir. Birimimize ait misyon ve vizyon hazırlanarak sayfamızda yayınlanmıştır. Görev dağılım tabloları oluşturularak her hizmet alanının görev ve sorumluluk alanı tespit edilmiş ve personele duyurulmuştur. Tahakkuk ve taşınır işlemleri ilgili kanun ve yönetmelikler çerçevesinde Strateji Geliştirme Daire Başkanlığıyla iletişim halinde yürütülmektedir. İş akış süreçleri belirlenmiş, her alt birim kendi göreviyle ilgili risk belirleme çalışmalarını gerçekleştirmiştir. Herhangi bir sebeple yaşanan işten ayrılma durumlarında standart iş devir formları hazırlanarak işin sürekliliği sağlanmıştır. Bununla beraber Yönetim Bilgi Sistemi ile ilgili çalışmalar sürdürülmekte; kurumumuza ait bilgi ve belgelerin daha erişilebilir olması amacıyla geliştirilmeye çalışılmaktadır.

II- AMAÇ ve HEDEFLER

A. İdarenin Amaç ve Hedefleri

Faaliyet Raporunun GENEL BİLGİLER bölümünde "Misyon" ve "Vizyon" bölümünde yer alan tanımlara paralel olarak kurumsal iş verimliliği konusunda da çalışmalar yürütülmektedir. Başkanlığımızın öncelik verdiği amaç ve hedefler:

Bilgi İşlem Daire Başkanlığının kaynak verimliliği sağlayan bir birim olması. Parasal, zaman ve fiziki (mekan, donanım, sunucu v. b. kullanımı) kaynaklarda optimum kullanım sağlanması.

Üniversitemizin idari ve akademik birimlerinin ihtiyacı olan bilgisayar yazılımlarını güncellemek,

Bilişim Güvenliği İle İlgili Kullanıcı Politikası ve Bilgi Güvenliği Politikası hazırlamak,
"Kişisel Bilişim Güvenliği, Korunma Yöntemleri, TCK' nın Bilişim Güvenliği Yasaları ve Sorumluluklarımız, Kötü Amaçlı Yazılımlar ve Korunma Yöntemleri" içerikli bilinçlendirme etkinlikleri düzenlemek,

Kampus Genelinde kötü amaçlı yazılımların (virüs, trojen, solucan, turuva atı vb.) bulaşmış olduğu bilgisayarların tespiti

Üniversitede kullanılan bilişim sistemlerinin tespit ve geliştirilmesindeki katkı payımızı arttırmak.

Mevcut hizmetlerimizin, kullanıcıların değişen ihtiyaçlarına ve teknolojik gelişmelere göre iyileştirilmesi.

Hizmetlerimizden yararlanan kullanıcıların servislerimizden yararlanma oranını üst düzeye çıkarmak.

Üniversitemiz tüm birimlerinde görevlendirilen bilgi işlem sorumluları (koordinatörleri) ile iletişimi ve katılımlarının artırılarak kullanıcı sorunlarını daha hızlı çözülmesini sağlamak.

Başkanlık personelinin mesleki yeterlilik seminer ve eğitimlerine katılımını sağlamak.

Sürekli gelişen teknolojik, mesleki, sosyal ve çevre koşulları nedeniyle zaman içerisinde hizmet açısından yetersiz duruma düşmemek amacıyla personelimizi amaca yönelik seminer ve kurslara göndermek.

B. Temel Politikalar ve Öncelikler

Esas alınacak politika belgeleri kamu idaresinin faaliyet alanı ve içinde bulunduğu sektöre göre değişmektedir. Ancak örnek olması açısından aşağıdaki politika belgeleri sayılabilir.
Yükseköğretim Kurulu Başkanlığı Tarafından Hazırlanan "Türkiye'nin Yükseköğretim Stratejisi"
Kalkınma Planları ve Yılı Programı,
Orta Vadeli Program,
Orta Vadeli Mali Plan,
Bilgi Toplumu Stratejisi ve Eki Eylem Planı,
Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi (BİDGES)
5651 Sayılı internet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun
Kişisel Verilerin korunması hakkında kanun KVKK
Elektronik İmza Kanunu
İso 27001 BGYS Politikası
Ağ Yönetim Politikası
Bilgi Güvenliği Politikası
Ağ Cihazları Güvenliği Politikası
Antivirüs Politikası
E-Posta Politikası
Kablosuz İletişim Politikası
Veritabanı Güvenlik Politikası
Uzaktan Erişim Politikası
Sunucu Güvenlik Politikası
Son Kullanıcı Güvenliği Politikası
Parola Politikası
Kriz Acil Durum Yönetimi Politikası
Kimlik Doğrulama ve Yetkilendirme Politikası
İnternet Erişim ve Kullanım Politikası
Erişim Yöntemi ve Erişim Kayıtlarının Tutulması
Bilgisayar Ağı ve İnternet Kullanım Politikası
Bilgi Sistemleri Genel Kullanım Politikası
Bilgi Güvenliği ve İzleme ve Denetleme Yönetimi Politikası
Yönetimin Gözden Geçirme Prosedürü
Yasal Gereksinimlere Uyum Prosedürü

İş Akışı İş sürekliliği Yönetimi Prosedürü
İnsan Kaynakları ve Eğitim Prosedürü
İç Tetkik Prosedürü
Görevler Ayrılığı Prosedürü
Fiziksel ve çevresel güvenlik prosedürü
Düzeltici ve Önleyici Faaliyetler Prosedürü
Doküman ve Kayıtların Kontrolü Prosedürü
Bilgi Güvenliği İhlal Prosedürü
Bilgi Güvenliği Disiplin Kuralları Prosedürü
Asgari Güvenlik Kriterleri
Kurumsal Siber Güvenliğe Yönelik Tehditler

C. Diğer Hususlar

Tüm personelin bilgi güvenliği konusunda bilinçlendirilmesini sağlamak,

Yeni projelerin geliştirilmesi kapsamında ihtiyaç duyulan teknik altyapının güçlendirilmesi.

Cisco veya Microsoft Network kurslarının üniversitemizde de düzenlenmesi,

Üniversitemiz networkünün ve uygulamalarının penetrasyon (sızma testi) testlerini yaptırmak,

Teknik personelin sayısını ve niteliğini arttırmak

Öğrencilerin yaz stajı için birimimizde uygulamalı eğitime alınması (yazılım , network , teknik servis uygulamaları)

Kablolu ve kablosuz internetin bağlantı hızlarını arttırmak, altyapısal iyileştirmeler yapmak,

Bilgi İşlem hizmetlerinde yaşanan aksaklıkların kaynağında yok edilebilmesi için, akademik ve idari birimlerde bilgi işlem ile koordineli çalışacak teknik personelin bulunmasını sağlamak

Teknik personelin kurs, seminer vb. etkinliklerden yeterince yararlanabilmesini sağlamak,

Düzenli olarak uygulanacak Bilgi işlem memnuniyet anketi ve bu kapsamda yapılacak iyileştirmeler ile sunulan hizmetlerin kalitesini arttırmak

Felaket Kurtarma Merkezi kurmak (İkinci bir veri merkezi oluşturarak herhangi bir afet durumunda kurumun iş ve işleyişinin aksamadan devam etmesini sağlamak ve veri kayıplarını en aza indirmek),

İSO 27001 Bilgi Güvenliği Yönetim Sistemi Standardını üniversitemize kazandırmak, Dokumantasyon ve raporlama düzenini oluşturmak

Tüm kurum kullanıcılarını Kimlik Denetim Sistemine dâhil etmek,

Birim Ebys Sorumluları ve Birim Web Sorumluları ile aylık değerlendirmeler ve iyileştirme toplantıları düzenlemek

Bilişim kaynakları envanteri yazılımı ile mevcut kaynaklarımızın kontrolünü ve dağılımını kontrol edebilmek.

IP Telefon hizmetini hayata geçirmek,

Kartlı geçiş sistemlerimizi güçlendirmek,

Destek merkezi oluşturmak, Help desk, Yardım Masası, Sorun Havuzu , Bilgi Bankası

Yönetim Bilgi Sisteminin kurulması

Network Sistem Donanım altyapısının güçlendirilmesi

Tablo 31. Taşınır Malzeme Listesi

			2022	2023
253.01	**Tesisler Grubu**	ADET	1	1
253.02	**Makineler ve Aletler**	ADET	16	20
253.03	**Cihazlar ve Aletler**	ADET	7	7
253 HESAP TOPLAMI:			706.033,41	723.054,41
254.01	**Karayolu Taşıtları Grubu**	ADET	1	1
254 HESAP* TOPLAMI:			10.938,60	10.938,60
255.01	**Döşeme ve Mefruşat**	ADET	11	11
255.02	**Büro Makineleri Grubu**	ADET	250	287
255.03	**Mobilyalar Grubu**	ADET	148	148
255.07	**Kütüphane Demirbaşları**	ADET	22	22
255.10	**Güvenlik, Kontrol**	ADET	20	20
255.11	**Demirbaş Niteliğindeki**	ADET		
255.99	**Diğer Demirbaşlar**	ADET		
255 HESAP TOPLAMI:			**488**	7.036.409,79 TL

Tablo 35. Personel Sayısının Yıllara Göre Dağılımı (Tüm Birimler)

Personel Sınıfı	2018 Yılı	2019 Yılı	2020 Yılı	2021 Yılı	2022 Yılı	2023 Yılı
Akademik Personel		1	2	2	2	2
Yabancı Uyruklu Akademik Personel						
İdari Personel	6	8	6	6	6	5
Sürekli İşçi	3	3	4	4	4	5
TOPLAM	9	12	12	12	12	12

Tablo 45. İdari Personel Kadrolarının Hizmet Sınıflarına Göre Dağılımı (Tüm Birimler)			
	Dolu	**Boş**	**Toplam**
Genel İdari Hizmetler Sınıfı	3	4	7
Sağlık Hizmetleri Sınıfı			
Teknik Hizmetler Sınıfı	2	6	8
Eğitim ve Öğretim Hizmetleri Sınıfı			
Avukatlık Hizmetleri Sınıfı			
Yardımcı Hizmetli Sınıfı			
Toplam	**5**	**10**	**15**

	Tablo 49. 2023 Yılında Göreve Başlayan İdari Personel (Tüm Birimler)				
	Açıktan	**Nakil**	**Geçici Görevlendirme**	**Mahkeme Kararı**	**Toplam**
İdari Personel		2			2
TOPLAM		**2**			**2**

Tablo 50. 2023 Yılı Üniversitemizden Ayrılan İdari Personel Sayısı	
Emekli	-
İstifa	2
Ölüm	1
Nakil	-
Diğer	-
TOPLAM	**3**

III- FAALİYETLERE İLİŞKİN BİLGİ VE DEĞERLENDİRMELER

1-Bütçe Uygulama Sonuçları

1.1-Bütçe Giderleri

Ekonomik Sınıflandırmaya Göre Ödenek ve Harcama Miktarı (TL)

NO	GİDER TÜRLERİ	2023 YILI KBÖ	EKLENEN	DÜŞÜLEN	YILSONU ÖDENEĞİ	TOPLAM HARCAMA	HARCAMA ORANI
01	PERSONEL GİDERLERİ	1.629.000,00 TL	0	0	1.629.000,00 TL	1.481.183,11 TL	**%90.93**
02	SOSYAL GÜVENLİK KURUMLARINA DEVLET PRİMİ GİDERLERİ	275.000,00 TL	0	7696,00 TL	267304,00 TL	203056,86 TL	**%75.96**
03	MAL VE HİZMET ALIM GİDERLERİ	144100,00 TL	47100,00 TL	0	184100,00 TL	203350,32 TL	**%110.46**
05	CARİ TRANSFERLER	111.000,00 TL	0	0	110.000,00 TL	0	**%0**
06	SERMAYE GİDERLERİ	1.600.000 TL	5.400.000 TL	1.400.000,00 TL	5.600.000,00 TL	5.542.300,32 TL	**%98.97**
GENEL TOPLAM		**3.759.100,00 TL**	**5.447.100,00 TL**	**1.407.696,00 TL**	**7.790.404,00 TL**	**7.429.890,61 TL**	

Tablo 63. Ekonomik Sınıflandırmaya Göre Bütçe Gider Gerçekleşmeleri (I. Düzey)

(Tüm Birimler)

Kodu	Ödenek Türü	2022		
		KBÖ	Yılsonu Ödenek	Harcama
01	Personel Giderleri	1.629.000,00 TL	1.629.000,00 TL	1.481.183,11 TL
02	Sosyal Güvenlik Kurumlarına Devlet Primi Giderleri	275.000,00 TL	267.304,00 TL	203.056,86 TL
03	Mal Ve Hizmet Alım Giderleri	144.100,00 TL	184.100,00 TL	203.350,52 TL
04	Faiz Giderleri			
05	Cari Transferler	111.000,00 TL	111.000,00 TL	0,00 TL
06	Sermaye Giderleri	1.600.000,00 TL	5.600.000,00 TL	5.542.300,32 TL
07	Sermaye Transferleri			

08	Borç Verme			
09	Yedek Ödenekler			
Genel Toplam		**3.759.100,00 TL**	**7.791.404,00 TL**	**7.429.890,81 TL**

Tablo 64. Ekonomik Sınıflandırmaya Göre Bütçe Gider Gerçekleşmeleri (II. Düzey

EKONOMİK KODLAR		**2022 Yılı**		
KOD	**AÇIKLAMA**	**KBÖ**	**TOPLAM ÖDENEK**	**HARCAMA**
01.1	MEMURLAR	1.629.000,00 TL	1.629.000,00 TL	1.481.183,11 TL
01.2	SÖZLEŞMELİ PERSONEL			
01.3	İŞÇİLER			
01.4	GEÇİCİ SÜRELİ ÇALIŞANLAR			
01.5	DİĞER PERSONEL			
01	**PERSONEL GİDERLERİ**			
02.1	MEMURLAR	275.000,00 TL	267.304,00 TL	203.056,86 TL
02.2	SÖZLEŞMELİ PERSONEL			
02.3	İŞÇİLER			
02.4	GEÇİCİ SÜRELİ ÇALIŞANLAR			
02.5	DİĞER PERSONEL			
02	**SOSYAL GÜVENLİK KURUMLARINA DEVLET PRİMİ GİDERLERİ**			
03.1	ÜRETİME YÖNELİK MAL VE MALZEME ALIMLARI			
03.2	TÜKETİME YÖNELİK MAL VE MALZEME ALIMLARI	63.000,00 TL	103.000,00 TL	101.506,22 TL
03.3	YOLLUKLAR	12.000,00 TL	19.100,00 TL	15.501,00 TL
03.4	GÖREV GİDERLERİ			
03.5	HİZMET ALIMLARI	111.000,00 TL	111.000,00 TL	0,00 TL
03.6	TEMSİL VE TANITMA GİDERLERİ			
03.7	MENKUL MAL, GAYRİMADDİ HAK ALIM, BAKIM VE ONARIM G.	89.000,00 TL	89.000,00 TL	86.343,30 TL
03.8	GAYRİMENKUL MAL BAKIM VE ONARIM			

	GİDERLERİ			
03.9	TEDAVİ VE CENAZE GİDERLERİ			
03	**MAL VE HİZMET ALIM GİDERLERİ**			
04	**FAİZ GİDERLERİ**			
05.1	GÖREVLENDİRME GİDERLERİ			
05.2	HAZİNE YARDIMLARI			
05.3	KAR AMACI GÜTMEYEN KURULUŞLARA YAPILAN TRANSFER.			
05.4	HANE HALKINA YAPILAN TRANSFERLER			
05.5	DEVLET SOSYAL GÜVENLİK KURUMLARINDAN HANE HALKINA YAPILAN FAYDA ÖDEMELERİ			
05.6	YURTDIŞINA YAPILAN TRANSFERLER			
05.8	GELİRLERDEN AYRILAN PAYLAR			
05	**CARİ TRANSFERLER**			
06.1	MAMUL MAL ALIMLARI	500.000,00 TL	3.900.000,00 TL	3.891.158,01 TL
06.2	MENKUL SERMAYE ÜRETİM GİDERLERİ			
06.3	GAYRİ MADDİ HAK ALIMLARI	1.100.000,00 TL	1.700.000,00 TL	1.651.142,31 TL
06.4	GAYRİMENKUL ALIMLARI VE KAMULAŞTIRMASI			
06.5	GAYRİMENKUL SERMAYE ÜRETİM GİDERLERİ			
06.6	MENKUL MALLARIN BÜYÜK ONARIM GİDERLERİ			
06.7	GAYRİMENKUL BÜYÜK ONARIM GİDERLERİ			
06.8	STOK ALIMLARI			
06.9	DİĞER SERMAYE GİDERLERİ			
06	**SERMAYE GİDERLERİ**			
07	**SERMAYE TRANSFERLERİ**			
08	**BORÇ VERME**			
09	**YEDEK ÖDENEKLER**			

Tablo 66. Ekonomik Sınıflandırmaya Göre Gider Gerçekleşmeleri

Birimi	KBÖ	Toplam Ödenek	Gerçekleşme
Rektörlük Özel Kalem			
Genel Sekreterlik			
Strateji Geliştirme Daire Başkanlığı			
Yapı İşleri ve Teknik Daire Başkanlığı			
İdari ve Mali İşler Daire Başkanlığı			
Öğrenci İşleri Daire Başkanlığı			
Kütüphane ve Dokümantasyon Daire Başkanlığı			
Sağlık Kültür ve Spor Daire Başkanlığı			
Personel Daire Başkanlığı			
Bilgi İşlem Daire Başkanlığı	3.779.000,00 TL	7.818.404,00 TL	7.429.890,81 TL
Hukuk Müşavirliği			
Toplam	3.779.000,00 TL	7.818.404,00 TL	7.429.890,81 TL

Tablo 67. Fonksiyonel Sınıflandırmaya Göre Bütçe Gider Gerçekleşmeleri (Tüm Birimler)				
KOD	**Açıklama**	**KBÖ**	**Toplam Ödenek**	**Harcama**
01	PERSONEL GİDERLERİ	1.629.000,00 TL	1.629.000,00 TL	1.481.183,11 TL
02	SOSYAL GÜVENLİK KURUMLARINA DEVLET PRİMİ GİDERLERİ	275.000,00 TL	267.304,00 TL	203.056,86 TL
03	MAL VE HİZMET ALIM GİDERLERİ	144.100,00 TL	184.100,00 TL	203.350,52 TL
04	FAİZ GİDERLERİ			
05	CARİ TRANSFERLER	111.000,00 TL	111.000,00 TL	0,00 TL
06	SERMAYE GİDERLERİ	1.600.000,00 TL	5.600.000,00 TL	5.542.300,32 TL

B- Performans Bilgileri

V.1. Ağ ve Sistem Yönetim Hizmetleri

Bağlantı sayısı ve yoğunluğunun artmasıyla kurum internet bağlantı hızı ULAKNET aracılığıyla 1250 mbps'den 1500 mbps'ye yükseltilmiştir.

Firewall ; Kapsamlı ağ güvenliği sağlamak için gelişmiş teknolojilerin yapay zeka ile kombinasyonunu sağlayan Yeni Nesil Güvenlik Duvarı ile derin paket denetimleri, izinsiz giriş önleme ve tehdit istihbaratı sağlayan Palo Alto Firewall donanım cihazı ve yazılım paketi alınmıştır.

Logsign :

Ağ güvenliği için her sayıda ve her kaynaktan, istenen miktarda veriyi toplayarak saklayabildiği, yedekli bir veri gölü oluşturma imkanı sağlayan, veri gölü üzerinde gerçek zamanlı analizlerle zaafiyet veya tehdit, atak tespitine imkan veren Logsign Siem yazılımı tedarik edilmiştir.

Santral Altyapısı Güçlendirmesi

Yıl içerisinde yaşanan arıza ve oluşan ihtiyaçlar doğrultusunda Santral Anakartları, Santral Power ve Santral Lisans alımları ile altyapı güçlendirmeleri ve hizmet sürekliliği sağlanmıştır.

Ssl Sertifika lisans alımı ile kullanıcıları bilgilerinin üçüncü taraflarca ele geçirilmesine engel olan, kullanıcı bilgilerinin güvende olmasını sağlayan Ssl sertifika tedarik edilmiştir.

Zoom Lisans Alımı ile ; internet bağlantısı aracılığıyla sesli video konferans görüşmeleri, sohbet ve web seminerleri ve online toplantılar gerçekleştirilebilmesi için Zoom Yazılımı lisansı tedarik edilmiştir.

Öğrenci Yaşam merkezi ve Hobi Bahçeleri güvenlik tedbirleri için kamera konuşlandırılmıştır.

2023 yılında tüm birimlerimize hizmet veren bilgi sistemleri yazılımlarının bakım güncelleme revizyon ve destek hizmetlerinin sağlanması için , hizmet sürekliliği için sözleşmeler yenilenmiştir.

Kurumsal Faaliyetlerin yürütüldüğü bilgi sistemlerinin çalışmasını sürdürülebilir kılan felaket kurtarma merkezi yatırımları ile veri kaybı yaşanma riski ortadan kaldırılmıştır.

Ebys, Tekink Servis, Mail sistemi, Web Sitesi, Kartlı Geçiş Sistemleri, İnternet Sorunları , Grafik tasarım ve baskı hizmetleri, Dahili Telefon problemleri ve birim laboratuvarlarının eğitim öğretime hazırlanması ve süreç içerisinde müdahalelerde bulunması gibi yıl içerisinde gerçekleştirilmiş , çözüme kavuşturulmuş, destek sağlanmış faaliyetler aşağıda yer alan tabloda olduğu haliyle belirtilmiştir.

V.2. Birimler 2023 Yılı İşlem Yapılan Faaliyetler Toplamı

Faaliyet Adı (Yıllık)	Adet
Ebys Birimi Çözüme Kavuşturulan İş Talep Formu	390
Teknik Servis Birimi Çözüme Kavuşturulan İş Talep Formu	209
Mail Sistemi Çözüme Kavuşturulan İş Talep Formu	110
Web Sitesi ile ilgili Yayınlar ve Çözüme Kavuşturulan İş Talep Formu	143
PDKS Kartlı Geçiş Sistemi Çözüme Kavuşturulan İş Talep Formu	10
İnternet Sorunları Çözüme Kavuşturulan İş Talep Formu	65
Grafik Tasarım ve Baskı Birimi Çözüme Kavuşturulan İş Talep Formu	55
Dahili Telefon Çözüme Kavuşturulan İş Talep Formu	34
Başkanlığımız ile ilgili diğer görevler (Laboratuvar Kurulumları) Eğitim Fakültesi 284 Bilgisayar, Fen Edebiyat Fakültesi 96 Bilgisayar, İktisadi ve İdari Bilimler Fakültesi 45, Spor Bilimleri Fakültesi 42 Bilgisayar, Meslek YüksekOkulu 183 Bilgisayar, Sağlık Bilimleri Fakültesi 78 Bilgisayar, Merkezi Araştırma Laboratuvarı 6 Bilgisayar,	734

1.1. Faaliyet Bilgileri

FAALİYET TÜRÜ	SAYISI
Sempozyum ve Kongre	3
Konferans	12
Panel	10
Seminer	10
Açık Oturum	
Söyleşi	11
Tiyatro	1
Konser	3
Sergi	6
Turnuva	1
Teknik Gezi	
Eğitim Semineri	
Çalıştay	1
Program	2
Toplantı	2
Etkinlik (Fakülte, Öğrenci Kulüp Etkinlikleri, Dış Paydaş Etkinlikleri, Tiyatro, Şiir , Müzikal Etkinlikler, Sergi, Toplantılar)	60
Zirve	1
Tören	1
TOPLAM	123

4-Performans Bilgi Sisteminin Değerlendirilmesi

Birimimiz bünyesinde yürütülmekte olan tüm hizmetlerin değerlendirilmesi, veri toplanması, işlenmesi ve kalitesine ilişkin analizler yıl için tüm birimler tarafınca Ebys üzerinden açılan iş talep formları aracılığıyla kategorilendirilmektedir. Bunlar Teknik Servis ile ilgil talepler, Web Sayfası ile ilgili talepler, Kurumsal mail ile ilgili talepler, İnternet Sorunları, Grafik tasarım ve baskı işlemleri, İletişim güncelleme işlemleri, Sistem ve Network işlemleri, Güvenlik Kamerası ve Dahili Telefon İşlemleri, Pdks ve Kart okuyucu talepleri olmak üzere 11 ana başlık halinde kullanıcılarımız tarafından yıl içinde bildirilen sorunlar bu şekliyle kategorize edilmektedir. Yılsonu itibariyle de yıl içinde çözülmüş destek sağlanmış kategoriklerin toplam rakamları üzerinden yıl bazlı karşılaştırma, sistem bazlı karşılaştırma birim performansı ve oluşan sorun havuzu kapsamında iyileştirme yapılması gereken alanlar tespit edilmektedir.

IV- KURUMSAL KABİLİYET ve KAPASİTENİN DEĞERLENDİRİLMESİ

Başkanlığımızın misyon ve vizyonuna temel teşkil eden değer ve ilkeleri şunlardır:
Etik değerler: Toplumun ve insanlığın ortak değerleri olan etik değerlere bağlı kalmak ve bu değerlerin gelişimine katkı sağlamak.
Katılımcılık ve şeffaflık: Başkanlık faaliyetlerini gerçekleştirmede çalışanların ve ilişki kurabileceğimiz özellikteki diğer birimlerin fikir, öneri ve görüşlerini almak, sıkça yapılan toplantılarla faaliyetlerin gerçekleştirilmesi aşamalarından çalışanları ve ilgili birimleri haberdar etmek kurumumuza en gerçekçi ve yararlı hizmeti sunma konusunda ilgili birimlerle görüş alışverişinde bulunma konusunda duyarlı olmak.
Adalet ve eşitlik: Tüm çalışanlara sağlanan hizmette ve haklarını koruma, isteklerini karşılama konusunda adalet ve eşitlik ilkesini vazgeçilmez ilke kabul etmek.
Saygı ve güvenilirlik: Hizmet sunumunda kurum içi ve dışı ilişkide kişilik ve emeğe saygıyı temel almak. Kişisel bilgi gizliliği ve güvenliğini sağlamak.
Kalite: Üretilen iş, desteklenen projeler ve sağlanan hizmetlerde ilişkide bulunduğumuz kurum içi ve dışı tüm kullanıcılara anılan süreçlerde optimum yarar sağlayacak şekilde destek vermek. Öğrenci ve çalışanlarımıza, eğitim ve araştırmacılarımıza ve diğer kullanıcılarımıza faaliyet alanlarında gelişmiş teknoloji katkısı ile en kaliteli hizmeti sunmak.
Dayanışma ve işbirliği: Hizmet ve projelerimizde Başkanlığımızın yürütmesi gereken faaliyetler konusunda ilgili kişi, kurum ve birimlerle dayanışma içinde hareket etmek.
Açıklık ve Yaratıcılık: Tüm yenilik ve gelişmelere açık olmak ve vizyonun gerektirdiği yaratıcılık ve yeniliklerde risk alarak öncü olmak.
Kurum ve Ülke Yararı: Üretilen hizmet, proje ve geliştirilen davranış biçimlerinde kurum ve ülke yararının daima ön planda tutulması. Tasarrufa yönelik çalışma biçimi. Açık kaynak sistemlerin bu amaçla kullanımı. Kullanıcıların amaca yönelik eğitimi ve bilinçlendirilmesi. Yapılanmamızın bu düşünce ışığında gerçekleştirilmesi

A- Üstünlükler

Her geçen gün toplam değeri artan Ağrı İbrahim Çeçen Üniversitesinin bir birimi olmak

Genç ve dinamik bir kadroya sahip olmak

Üniversite üst yönetiminin tam desteği

ULAKBİM bağlantı hız ve kapasitemiz

Üniversitemiz tüm birimlerinin fiber ağa dahil olması

Kablosuz İnternet Altyapımız

Daire Başkanımızın teknik (mühendis) kökenli olması

Hizmet üretiminde ve sunumunda hoşgörülü ve çözüm odaklı yaklaşımımız

Çalışanlarımızın özverili olması

Bilgi Yönetim Sistemlerimiz

Sunucu altyapısının sanallaştırma sistemi üzerinde yer alması

B- Zayıflıklar

Bilgi işlem hizmetlerine ayrılan finansal kaynakların yetersizliği.

Üniversite birimlerinin –Merkez ve diğer- aralarındaki dayanışma ve koordinasyon eksikliğinin yansımaları,

Ücret, servis v. b gibi sosyal ve maddi imkân yetersizliklerinin motivasyona olumsuz etkisi

Üniversite birimlerinde yetkin personel olmayışının bilişim hizmetlerine olumsuz katkısı Hizmet kalitesi, güvenlik v.b. sorunları)

Bilişim ile ilgili diğer üniversite, kurum ve organizasyonlar ile iletişim ve dayanışma eksikliği

Yetişmiş teknik personelin maaş ve sosyal imkânların azlığı nedeniyle başka kurumlara geçme çabaları.

Açık Kaynak kodlu yazılım kullanımının yaygınlaştıramaması

Kullanıcılara sunulan hizmetlerde eksiklik ve aksama

Sunucu sistemlerinin yedeği alınmış olsa da farklı lokasyonlarda yedeklenmemesi (FKM)

Ağ altyapısında yeterli yedekliliği sağlayacak donanım bulunmaması

Dokümantasyon ve raporlama sisteminin tam oturtulamamış olması

Kurum varlıklarının izlenememesi ve yönetilememesi, Kurum varlıklarının raporlanması, sınıflandırılması, ve kullanım süreleri ile ilgili rapor alınamaması, kurum kaynaklarımız üzerinde gerekli hakimiyet ve plan yapılamıyor olması, strtaejiler geliştirilemiyor olması

BGYS Sisteminin Kurulamamış olması

Birim hafızasını teşkil eden kritik görevde çalışanların alternatifinin oluşturulamaması

Kurum yapısı ve Kültürü, Kurum prosedür ve talimatlarının tam anlamıyla karşılık bulmaması

Fiber kablo haritalandırılmasının olmaması, kazı çalışmalarında kablo kopmalarının yaşanması, kazı yapılmadan önce birimler arası koordinasyon eksikliği. Galeri sisteminin projelendirilmemiş olması

Kurum genelinde kullanılmakta olan bilgisayarların kullanım sürelerinin ömrünü tamamlaması, eskiyen teknoloji olarak kalması

C- Değerlendirme

Başkanlığımız eldeki bütçe ve insan kaynaklarının olabildiğince verimli kullanarak son derece yararlı hizmetler üretmiş birçok konuda başarılı olmuştur. Dünyaya paralel olarak tüm uygulamaların sayısal ortamda çalışır hale getirildiği bir dönemde BİDB nın çok önemli rolü olduğu görülmektedir. Bilişim sistemlerinde oluşabilecek herhangi menfi durum kurumumuz için para, zaman ve en kötüsü prestij kaybına sebep olacaktır. Sistemin aynı şekilde çalışması daha da artacak olan bilişim ihtiyaçları ve önceden tahmin edilemeyen tehditler bilişim sistemlerine ve insan gücü yatırımlarının artarak sürmesi gerekmektedir

V- ÖNERİ VE TEDBİRLER

Tüm personelin bilgi güvenliği konusunda bilinçlendirilmesini sağlamak,

Kişisel bilgi güvenliği farkındalık eğitimi yapılmalı,

Yeni projelerin geliştirilmesi kapsamında ihtiyaç duyulan teknik altyapının güçlendirilmesi .

Cisco veya Microsoft Network kurslarının üniversitemizde de düzenlenmesi,

Üniversitemiz networkünün ve uygulamalarının penetrasyon (sızma testi) testlerini yaptırmak,

Donanım Envanterinin Yönetimi

Yazılım Envanterinin Yönetimi

Tehdit ve Zaafiyet Yönetimi

E-posta sunucu yönetimi

Zararlı Yazılımlardan Korunma Son Kullanıcı Lisanslı Yazılım Desteği

Teknik personelin sayısını ve niteliğini arttırmak

Öğrencilerin yaz stajı için birimimizde uygulamalı eğitime alınması (yazılım , network , teknik servis uygulamaları)

Kablolu ve kablosuz internetin bağlantı hızlarını arttırmak, altyapısal iyileştirmeler yapmak,

Bilgi İşlem hizmetlerinde yaşanan aksaklıkların kaynağında yok edilebilmesi için, akademik ve idari birimlerde bilgi işlem ile koordineli çalışacak teknik personelin bulunmasını sağlamak

Teknik personelin kurs, seminer vb. etkinliklerden yeterince yararlanabilmesini sağlamak,

Düzenli olarak uygulanacak Bilgi işlem memnuniyet anketi ve bu kapsamda yapılacak iyileştirmeler ile sunulan hizmetlerin kalitesini arttırmak

Felaket Kurtarma Merkezi kurmak (İkinci bir veri merkezi oluşturarak herhangi bir afet durumunda kurumun iş ve işleyişinin aksamadan devam etmesini sağlamak ve veri kayıplarını en aza indirmek),

İSO 27001 Bilgi Güvenliği Yönetim Sistemi Standardını üniversitemize kazandırmak, Dokumantasyon ve raporlama düzenini oluşturmak

Tüm kurum kullanıcılarını Kimlik Denetim Sistemine dâhil etmek,

Birim Ebys Sorumluları ve Birim Web Sorumluları ile aylık değerlendirmeler ve iyileştirme toplantıları düzenlemek

Bilişim kaynakları envanteri yazılımı ile mevcut kaynaklarımızın kontrolünü ve dağılımını kontrol edebilmek.

IP Telefon hizmetini hayata geçirmek,

Kartlı geçiş sistemlerimizi yenilemek

Destek merkezi oluşturmak , Help desk , Yardım Masası , Sorun Havuzu , Bilgi Bankası

Yönetim Bilgi Sisteminin kurulması-

Network Sistem Donanım altyapısının güçlendirilmesi

TEDBİRLER	TEDBİR AÇIKLAMASI ÖNERİLER
Donanım Envanterinin Yönetimi	Veri saklama, işleme ve iletme yeteneği olan tüm donanımların güncel bir envanteri tutulmalı
Donanım Envanter İçeriğinin Yönetimi	her bir donanımın ağ adresini, donanım adresini, makine adını, seri numarasını, markasını, modelini, destek alınan tedarikçi sözleşme bilgilerini (bakım süresi, kapsamı vb.), donanımın sorumlusunu, sorumlu kişinin birimini içermelidir
Donanım Envanterine Kaydedilmemiş Donanımların Yönetimi	Yeni tedarik edilen ya da ağa yeni bağlanacak donanımların, donanım varlık envanterine kaydı yapılmadan kurum ağına bağlanmamasına yönelik politika ve prosedürler oluşturulmalı ve uygulanmalıdır
Aktif Keşif Araçlarının Kullanılması	Kurum ağına bağlı cihazları tanımlamak ve donanım varlık envanterindeki değişiklikleri takip etmek için aktif keşif araçları kullanılmalıdır

DHCP Kayıt Mekanizması ile Yeni Donanımların Tespiti	Kurumun donanım envanterini güncel tutmak için tüm DHCP sunucularında ya da IP adres yönetim araçlarında kayıt mekanizmasının kullanımı sağlanmalıdır
Kullanım Ömrünü Tamamlayan Cihazların Veri Depolama Üniteleri	Kullanım ömrünü tamamlayan cihazların veri depolama üniteleri (HDD, SSD, USB, disk, harici bellek vb.) güvenli bir şekilde imha edilmelidir
Kurum Ağı Bağlantı Noktalarında Kimlik Denetimi Yapılması	Sadece onaylı donanımların kurum ağına bağlanabilmesi için, 802.1x standardı veya NAC çözümleri kullanılarak kurum ağına bağlanan cihazlara kimlik denetimi yapılmalıdır
Donanım Varlıklarının Kimlik Denetimi için İstemci Sertifikalarının Kullanılması	
Sabit Disk Güvenliği	Kurum tarafından satın alınan kullanıcı bilgisayarlarına ait sabit diskler, veri kurtarmaya imkân sağlamayacak şekilde güvenli silme işlemine tabi tutulduktan sonra sistemlere dâhil edilmelidir.

TEDBİRLER	TEDBİR AÇIKLAMASI
Yazılım Envanterinin Yönetimi	yazılımların adı, sürümü, yayımcısı, destek alınan tedarikçi sözleşme bilgileri (bakım süresi, kapsamı vb.), lisans bilgileri ve edinim tarihi bilgileri, yazılımın yüklendiği donanımlar kayıt altına alınmalı ve izlenebilir olmalıdır
Yazılım Envanter İçeriğinin Yönetilmesi	Kurumun onaylı yazılım envanterine yalnızca üreticisi tarafından desteklenen yazılımlar dâhil edilmelidir Yazılım envanterinde kayıtlı olan yazılımlar için güncelleme desteği devamlılığı sağlanmalıdır. Üreticisi tarafından sunulan destek hizmeti sona ermiş ancak iş gereksinimleri sebebi ile kullanılması gereken yazılımlar, yazılım envanterinde “üretici tarafından desteklenmeyen” olarak etiketlenmelidir.
Yazılımın Üreticisi Tarafından Desteklenmesi	Kurumun onaylı yazılım envanterine yalnızca üreticisi tarafından desteklenen yazılımlar dâhil edilmelidir. Yazılım envanterinde kayıtlı olan yazılımlar için güncelleme desteği devamlılığı sağlanmalıdır. Üreticisi tarafından sunulan destek hizmeti sona ermiş ancak iş gereksinimleri sebebi ile kullanılması gereken yazılımlar, yazılım envanterinde “üretici tarafından desteklenmeyen” olarak etiketlenmelidir.
Yazılım Envanterine Kaydedilmemiş Yazılımların Yönetimi	Kurum tarafından onaylanmayan yazılımların kullanılmasına yönelik politika ve prosedürler oluşturulmalı ve uygulanmalıdır

Yazılım Envanteri Yönetim Araçlarının Kullanımı	Kurum sistemlerindeki tüm yazılımlar için envanter yönetim araçları kullanılmalıdır. Söz konusu envanter yönetim araçları, yazılımların mevcut durumları ile ilgili raporlama yeteneğine sahip olmalıdır.
Yazılım ve Donanım Envanterinin Entegre Edilmesi	Yazılım ve donanım envanteri birbirleri ile entegre edilmelidir. Entegre edilen envanter merkezi olarak yönetilmelidir.
Beyaz Liste Yönetimi	Kurum uygulama beyaz liste yönetimi yazılımı kullanmalıdır. Uygulama tarafından en az aşağıda yer alan kısıtlamalar devreye alınmalıdır. Yalnızca onaylı yazılım kütüphanelerinin (* .dll, * .ocx, * .so vb.) yüklenmesi Yalnızca onaylı ve dijital olarak imzalanmış betik dosyalarının (* .ps1, * .py, makrolar vb.) çalıştırılması

Yazılım Güncelleme Araçlarının Kullanımı	Tüm sistemlerdeki yazılımların, mevcut iş gereksinimlerini karşılayacak ve yazılım üreticisi tarafından sağlanan en kararlı ve güncel güvenlik sürümleri ile çalıştırılmakta olduğu otomatik yazılım güncelleme araçları kullanılarak kontrol edilmelidir.
Zararlı Yazılımların Engellenmesi	Zararlı yazılımların kuruma ait ve/veya kurum tarafından yönetilen kullanıcı uç nokta cihazları ve altyapı bileşenleri üzerinde çalışmasını, kaydedilmesini ve aktarılmasını engellemek için politikalar/prosedürler tanımlanmalı ve işletilmelidir. Personelin beyaz listede bulunan uygulamalar haricinde uygulama kurmasının engellenmesine yönelik politika/prosedür oluşturulmalıdır. Politika/prosedürün uygulanmasını temin etmek üzere gerekli teknolojik altyapılar ve uyarı mekanizmaları aktif edilmelidir
Zafiyet/Yama Yönetimi	Kurumsal uygulamaların, kurum ağının ve sistem bileşenlerinin güvenlik açıklarının zamanında tespit edilmesi için uygulanacak politikalar ve süreçler tanımlanmalıdır. Zafiyet ve yama yönetimine ilişkin değişiklikler, tanımlanmış değişiklik yönetimi süreci üzerinden kontrollü olarak gerçekleştirilmelidir.
Yüksek ve Üzeri Seviyede Zafiyet İçeren Sunucu/Uygulamaların Yalıtılması	Yüksek ve üzeri seviyede zafiyet barındıran sunucu ve uygulamalar, diğer sistemlerden fiziksel ya da mantıksal olarak izole edilmelidir.
Son Kullanıcıların Yetkisiz Program Ekleme/Kaldırma İşlemlerinin Engellenmesi	Son kullanıcıların, güvenlik sıkılaştırmaları kapsamında kurum tarafından uygulanması gerekli görülen konfigürasyonlara müdahale etmemesi ve beyaz listede bulunan programlar haricinde program kurmalarının engellenmesi için son kullanıcı hesaplarının yerel yönetici yetkileri kaldırılmalıd
Güvenlik Açıkları için Risk Analizi Tabanlı Önceliklendirme	Tespit edilen güvenlik açıklarının giderilmesi için hazırlanan aksiyon planına yönelik önceliklendirme risk analizi tabanlı yapılmalıdır
Güvenlik Sıkılaştırmalarının Yapılması	Kurumsal uygulamalar (web, DNS, e-posta, FTP vb. ile diğer uygulamalar) ve kurum ağındaki bileşenler, işletim sisteminin ve paket yazılımların kurulumuyla gelen varsayılan güvenlik ayarlarıyla kullanılmamalıdır. Kullanıma alınmadan önce bilgi güvenliği gereksinimleri dikkate alınarak gerekli güvenlik sıkılaştırmaları yapılmalıdır

İşletim Sistemi Yama Yönetimi Araçlarının Kullanımı	Güvenlik güncellemeleri başta olmak üzere işletim sistemlerine yönelik güncellemelerin ve yamaların üreticisi tarafından bildirilen en kararlı, güncel ve güvenilir sürüm dikkate alınarak yapıldığı, otomatik yazılım güncelleme araçları ile kontrol edilmelidir
Zafiyet Tarama Araçlarının Kullanımı	Kurum ağında yer alan tüm sistemler (test sistemleri de dâhil olmak üzere) güvenlik içeriği otomasyon protokolü (SCAP) uyumlu güvenlik zafiyeti tarama aracı kullanılarak periyodik olarak taranmalıdır. Güvenlik taramaları için oluşturulan hesaplar farklı bir amaç için kullanılmamalı, en az yetki ve bilmesi gereken prensibi doğrultusunda yetkilendirme yapılarak ilgili erişim kayıtları tutulmalıdır. Güvenlik taramaları için oluşturulan hesaplar düzenli olarak kontrol edilmeli ve izlenmelidir. Zafiyet tarama araçları, güvenlik açıklarına yönelik yapılan doğrulama faaliyetleri öncesi ve sonrası durumu içerecek şekilde raporlama yapmalıdır. Üretilen raporların güvenliği sağlanmalı ve raporlara sadece yetkili personel erişim sağlamalıdır
Aktif Portların, Servislerin ve Protokollerin Varlık Envanterinde Tutulması	Aktif bağlantı portları, servisler ve protokoller donanım ve yazılım varlık envanterinde yer alan varlıklar ile eşleştirilmelidir. Kurum sistemlerinin tümünü kapsayacak şekilde port, servis ve protokol taramaları gerçekleştirilmeli, açık ve kullanımına ihtiyaç olmayan portların tespit edilmesi durumunda alarm üreten mekanizmalar devreye alınmalıdır

Tekrar Yayınlama (Relay) İşleminin Engellenmesi	Tekrar yayınlama (relay) işlemine, belirlenen IP adresleri dışında izin verilmemeli ve e-posta hizmet protokollerinden kullanılmayanlar kapatılmalıdır
SMTP Kimlik Doğrulaması Kullanımı	E-posta gönderiminde kullanıcı adı ve parola kullanılarak kimlik doğrulaması yapılmalıdır

Kurum Tarafından Onaylanan İnternet Tarayıcıları ve E-Posta İstemcilerinin Kullanımı	Kurum tarafından onaylanmış, üretici tarafından desteği devam eden kararlı ve güncel sürüme sahip internet tarayıcıları ile e-posta istemcileri kullanılmalıdır
E-posta İçeriğindeki Zararlı Bağlantılara (URL) Erişimin Engellenmesi	E-posta içeriğindeki zararlı bağlantılara erişim engellenmelidir.
İstenmeyen E-posta (Spam) Koruması	Spam e-postaları engellemek üzere DNS tabanlı filtreleme ve kara liste yöntemleri uygulanmalıdır
Servis Dışı Bırakma Saldırıları (DoS) Koruması	E-posta bombardımanı ve bağlantı temelli servis dışı bırakma saldırılarına karşı SMTP sunucusunda bağlantı sayısı sınırlama vb. yöntemler ile koruma sağlanmalıdır.
E-posta İçerik Kontrollerinin Yapılması	Gelen/giden tüm e-posta hesaplarına ait içerikler, istenmeyen e-postalar ve e-posta ile yayılabilecek zararlı yazılımlara karşı güvenliği sağlamak amacıyla SMTP Gateway vb. sistemler kullanılarak kontrol edilmelidir.
Sahte ya da Değiştirilmiş EPostaların Engellenmesi	Sahte ya da bütünlüğü bozulmuş e-postaların geçerli etki alanlarına sızma ihtimalini azaltmak için SPF, DKIM vb. teknoloji ve standartlar kullanılmalıdır
Risk İçeren İzinsiz ve/veya Çalıştırılabilir Dosya Türlerinin Engellenmesi	Kurum politikaları ile belirlenmiş olan risk içeren izinsiz ve/veya çalıştırılabilir dosya türleri içeren e-posta veya eposta ekleri engellenmelidir
Zararlı Yazılımdan Korunma Uygulamalarının Kullanılması	Bk. Tedbir No: 3.1.5.1
Güvenlik Sıkılaştırmalarının Yapılması	E-posta sunucuları, varsayılan ayarlarıyla kullanılmamalı ve kullanıma alınmadan önce tüm sunucuların güvenlik sıkılaştırmaları yapılmalıdır.
E-Posta İletişim Güvenliğinin Sağlanması	İstemci ve e-posta sunucuları arasındaki iletişimde bilinen zafiyet içermeyen güvenilir SSL/TLS sürümleri ile birlikte güvenli e-posta iletişim protokolleri (SMTPs, POP3s, IMAPs, HTTPs vb.) kullanılmalıdır. Bk. Tedbir No: 3.2.9.1
E-Posta Sunucu Mimarisi	E-posta sunucuları internetten gelebilecek her türlü saldırıları önlemek üzere katmanlı güvenlik tasarımı prensiplerine göre yapılandırılmalıdır
Üçüncü Taraflardan Temin Edilen E-Posta Hizmetleri	Üçüncü taraflardan temin edilen e-posta hizmetlerinin güvenliği garanti altına alınmalıdır. Bk. Bölüm 4.3

Onaylı İnternet Tarayıcısı ve EPosta İstemcisi Eklentilerinin Kullanımı	Sadece kurum tarafından onaylı internet tarayıcısı ve eposta istemcisi eklentileri kullanılmalıdır.
E-Posta İstemcilerinde Betik Kodlarının Kullanımını Sınırlama	E-posta istemcilerinde sadece kurum tarafından izin verilen betik kodları çalıştırılmalıdır
E-Posta Alışverişlerinin Şifreli ve İmzalı Yapılması	Kurum politikalarına göre gizlilik dereceli bilgi/veri içeren e-posta alışverişleri şifreli ve imzalı olarak yapılmalıdır. Eposta alışverişleri şifreli ve imzalı olarak yapıldığı durumda kullanılan sertifikalar kuruma özel olarak üretilmelidir
E-Posta Sunucularına Uzaktan Erişim	E-posta sunucularına uzaktan yapılacak erişimlerde çok faktörlü kimlik doğrulama mekanizmaları kullanılmalıdır
E-Posta Eklerinin Kum Havuzlarında Çalıştırılması	Kuruma dışarıdan gelen e-posta ekleri çok katmanlı güvenlik analizinden (içerik analizi, beyaz liste/kara liste, imza tabanlı anti-virüs, anti-malware taramaları vb.) geçirilmelidir. Bu aşamadan sonra hala kategorilendirilmemiş e-posta ekleri kum havuzunda çalıştırılmalıdır. Kum havuzu çözümlerinde dosyalar yurt içinde yerleşik olan sunucularda taranmalıdır

Zararlı Yazılımdan Korunma Uygulamalarının Kullanılması ve Merkezi Olarak Yönetilmesi	İstemci ve sunucu sistemlerinin tamamında zararlı yazılımdan korunma uygulamaları kullanılmalı ve zararlı yazılımdan korunma uygulamalarında en güncel yama dosyalarının bulunması ve imza veri tabanının güncel olması sağlanmalıdır. Zararlı yazılımdan korunma uygulamalarına ait politikalar merkezi olarak yönetilmelidir.
taşınabilir Disklerin Zararlı Yazılım Taramalarından Geçirilmesi	Kurumdaki tüm bilgisayarlar, taşınabilir diskleri otomatik olarak zararlı yazılım taramasından geçirecek şekilde yapılandırılmalıdır
Cihazların Otomatik Kod Çalıştırmasına İzin Vermemesi	Kurumdaki tüm bilgisayarlar, taşınabilir ortamlarda otomatik kod çalıştırılmasına izin vermeyecek şekilde yapılandırılmalıdır
Zararlı Yazılımdan Korunma Uygulamalarının Yapılandırılması ve Güncel Tutulması	Zararlı yazılımlardan korunma uygulaması üretici veya ilgili kurum tarafından önerilen şekilde yapılandırılmalı ve güncel tutulmalıdır
İşletim Sistemlerinin Güvenlik Mekanizmalarının Etkinleştirilmesi	Bk. Tedbir No: 5.1.1.12

Zararlı Yazılımdan Korunma Uygulamalarına Ait Kayıtların Merkezi Olarak Tutulması	Tüm zararlı yazılım tespitleri, merkezi yönetim ve kayıt sunucularına iletilmelidir
DNS Sorgularının Kayıtlarının Tutulması	Zararlı IP adreslerine erişimin denetlenmesi için DNS sorguları kayıt altına alınmalıdır
Komut Satırı Kayıtlarının Tutulması	Kurumda, kullanıcı tarafından PowerShell ve Bash gibi komut satırı kullanılarak yapılan işlemler denetlenmeli ve merkezi olarak kayıt altına alınmalıdır.

Ağ Topolojisi	Kurum ağlarına ait topolojiler güvenli bir şekilde tutulmalı ve güncelliği kontrol edilmelidir
Ağ Cihazlarının Güvenli Konfigürasyonu	Ağ cihazları endüstri standartları, en iyi uygulamalar ve üretici tavsiyelerine uygun olarak yapılandırılmalıdır. Varsayılan parola ve kullanıcı adları değiştirilmelidir. Ağ altyapısındaki cihazlar ağ üzerinden yönetilebilir olmalıdır. Yönetimsel erişimlerde komut satırına, konsol erişimine parola ile giriş sağlanmalıdır. Güvenli protokoller ile yönetimsel işlemler gerçekleştirilmelidir
Ağ Cihazlarında Güvenlik Güncellemelerinin Yapılması	Tüm ağ cihazlarında güvenlikle ilgili güncellemelerin üretici tarafından yayımlanan kararlı ve güncel sürümü kullanılmalıdır
Kara Liste veya Beyaz Liste Kullanımı	Kara liste veya beyaz liste kullanılarak varlıkların ağ erişimleri sınırlandırılmalıdır
İzin Verilmeyen Trafiğin Engellenmesi	Kurum ağ sınırlarından sadece izin verilen kaynaklardan izin verilen hedeflere, izin verilen port ve protokoller ile trafiğin akışı sağlanmalıdır.
Ağların İzole Edilmesi	Kablolu ve kablosuz ağlar, bilgi güvenliği gereksinimleri doğrultusunda katmanlara ayrılmalıdır. Yalnızca yetkili sistemlerin, belirli sorumluluklarını yerine getirmek amacıyla gerekli diğer sistemlerle iletişim kurabilmelerini sağlamak için oluşturulan LAN/VLAN'lar arasında erişim denetimi yapılmalıdır. İstemcilerin yer aldığı ağlar ile sunucu/uygulamaların yer aldığı ağlar ayrılmalıdır. Sunucu ağında istemci yer almamalıdır. Yönetimsel işlemler için ayrı yönetim ağları kullanılmalıdır.

DoS/DDoS Koruması	Kurumun internete açık hizmetleri için olası DoS/DDoS saldırılarına karşı servis dışı kalmasını önlemek, iş sürekliliğini sağlamak amacıyla en az aşağıdaki önlemler alınmalıdır. • Güvenlik ürünleri üzerinde DoS/DDoS saldırılarına özel konfigürasyonların yapılması • DDoS engelleme sistemlerinin sınırları ve yeteneklerinin düzenli aralıklarla test edilmesi ve sürekli iyileştirilmesi/güncellenmesi • DDoS koruma için bir servis sağlayıcıdan hizmet temin edilmiş ise; servis sağlayıcıdan yukarıdaki şartlara göre hizmet verildiğine dair taahhüt alınması, tedarik şartname ve sözleşmelerinde bu hususların belirtilmesi
İnternet Ortamından Kurum İçi Kaynaklara Erişim	İnternet ortamından kurum içi kaynaklara kontrol dışı erişim engellenmelidir. İnternet ortamından kurum içi kaynaklara erişim gerekli ise VPN teknolojileri kullanılmalıdır. Uzaktan erişimlerin kurum politika ve prosedürlerine uygun olarak, kısıtlı süre ve yetkilerle yapılması sağlanmalıdır
Kablosuz Erişim Noktalarının Envanterinin Tutulması	Kurum ağına bağlı yetkili kablosuz erişim noktalarının envanteri tutulmalı ve güncelliği sağlanmalıdır
Misafir Ağı Yönetimi	Kurum ağı ile fiziksel ve/veya mantıksal olarak izole edilmiş bir misafir ağı oluşturulmalıdır. Misafirlerin, misafir ağına bağlanmaları öncesinde kimlik bilgilerini doğrulayan mekanizmalar devreye alınmalı ve misafirler tarafından misafir ağı üzerinden yapılan tüm erişimler kayıt altına alınmalıdır. Misafir cihazlarının yalnızca misafir ağına erişimleri mümkün kılınmalıdır
Yerel Güvenlik Duvarı Ayarlarının Yapılması	Tüm sunucu ve istemcilerde yerel güvenlik duvarı yapılandırılmalıdır. Bu yapılandırma en az yetki prensibi göz önüne alınarak yapılmalıdır. Yapılandırma varsayılan reddetme (default deny) kuralını içermelidir. Tüm açık portlara ilişkin güvenlik duvarı kuralları yazılmalıdır
IP Telefon Kullanımı	IP telefon kullanılması durumunda ilgili sistem, altyapı sağlayıcısı veya kurum tarafından güvenlik duvarları ile korunmalıdır
IP Telefon Sistemlerine Ait İz Kayıtlarının Tutulması	IP telefon sistemlerinin iz kayıtları tutulmalıdır. İlgili kayıtlar düzenli aralıklarla bir sunucuda yedeklenmelidir. Bk. Tedbir No: 3.1.8.1
IP Telefon Kullanımında Parola Politikası	IP telefon sisteminde kullanılacak parolalar güçlü olmalı ve periyodik olarak güncellenmelidir. Bk. Tedbir No: 3.2.1.8
Ağ Erişim Denetimleri	Bk. Tedbir No: 3.1.1.7

Ağ Cihazlarına Ait Yapılandırmaların Dokümante Edilmesi	Kurum ağ cihazlarına ait güvenlik yapılandırmaları; ağ trafiğini düzenleyen kurallara ait tanımlar, kullanılma amacı ve kuralı tanımlayan kişi bilgisi yer alacak şekilde dokümante edilmeli ve güncelliği sağlanmalıdır
Ağ Paketlerinin Kaydedilmesi	Kurum tarafından gerekli görülen durumlarda, belirlenen kaynak(lar) ve hedef(ler) arasındaki tüm ağ trafiğinin izlenebilmesi için (pcap vb. formatlarda tüm ağ paketlerinin alınabilmesi) kayıt mekanizmaları oluşturulmalıdır. İhtiyaç duyulması durumunda (güvenlik ihlali, şüpheli ağ trafiği vb.) bu mekanizmalar kullanılarak kurum tarafından belirlenen zaman aralığında ilgili trafik kaydı incelenebilmelidir.
Ağ Sınır Cihazlarında Kayıt Tutulması	Ağ sınır cihazlarındaki bağlantı trafiği, kullanıcı işlemleri gibi bilgiler kayıt altına alınmalıdır
Ağ Tabanlı Saldırı Tespit/Engelleme Sistemi Kullanımı	Saldırıları tespit etmek ve engellemek için ağ tabanlı saldırı tespit ve engelleme sistemleri kullanılmalıdır
Uygulama Katmanında Filtreleme Yapılması	İnternetten gelen veya internete giden tüm ağ trafiği, yetkisiz bağlantıları engellemek için uygulama katmanında filtreleme ve kimlik doğrulaması yapılarak iletilmelidir
Ağ Tabanlı URL Filtreleri Kullanımı	Kurumdaki sistemlerin, kurum tarafından onaylanmayan ve mevzuat gereği erişimi yasak olan web sitelerine bağlanmasını engelleyen ağ tabanlı URL filtreleri uygulanmalıdır.
URL Kategori Hizmeti Kullanımı	URL sınıflandırma servisleri kullanılmalıdır. Bu servislerin kullandığı listeler güncel tutulmalıdır. Kategorilendirilmemiş siteler varsayılan olarak engellenmelidir
URL'lerin Kayıt Altına Alınması	Potansiyel olarak zararlı etkinlikleri tanımlamak ve saldırıya uğramış sistemlerin belirlenmesine yardımcı olmak için sistemlerden gelen tüm isteklere ait URL'ler kaydedilmelidir.
Kurum Ağına Bağlı Kablosuz Erişim Noktalarının Tespiti	Kurum ağına bağlı yetkisiz kablosuz erişim noktalarının tespit edilmesini ve alarm üretilmesini sağlayan ağ tabanlı keşif araçları kullanılmalıdır
İstemcilerin Kablosuz Ağ Erişimlerinin Sınırlandırılması	İstemciler, iş gereksinimleri doğrultusunda yalnızca yetkilendirilmiş kablosuz ağlara erişim sağlamalıdır
Eşler Arası Kablosuz Ağ Erişiminin Engellenmesi	Eşler arası (Peer to Peer) kablosuz ağ erişimine olanak sağlayan yöntemler (ad hoc yöntemi vb.) engellenmelidir.

Kablosuz Çevre Birimleri Aracılığı ile Yapılan Erişimin Engellenmesi	Cihazların, kablosuz çevre birimleri aracılığı ile yapacakları yetkisiz erişimler (bluetooth, NFC vb.) engellenmelidir
Uygulama Seviyesi Saldırıların Engellenmesi	Kurum ağının uygulama seviyesi saldırılara karşı korunması için gerekli yapılar (WAF, IPS, DDoS vb.) uygun şekilde konumlandırılmalı, test edilmeli ve sürekli iyileştirilmelidir. Bu amaçla bir servis sağlayıcıdan hizmet temin edilmiş ise; servis sağlayıcıdan yukarıdaki şartlara göre hizmet verildiğine dair taahhüt alınmalı, tedarik şartname ve sözleşmelerinde bu hususlar belirtilmelidir
IP Telefon Erişim Kontrol Listeleri	IP telefon sistemlerinde erişim kontrol listeleri kullanılmalı ve kimlik sahteciliği saldırılarına karşı önlem alınmalıdır
Ağ Cihazlarının Yapılandırma Yönetimi	Ağ cihazı mevcut yapılandırmaları, onaylanmış ve olması gereken güvenlik yapılandırma içerikleri ile karşılaştırılmalı ve herhangi bir uyumsuzluk tespit edildiğinde alarm üreten mekanizmalar devreye alınmalıdır
Ağ Cihazlarının Yönetimi	Ağ cihazlarının yönetimi, çok faktörlü kimlik doğrulama mekanizmaları kullanılarak şifreli ağ trafiği üzerinden yapılmalıdır. Ağ yönetimi için gerekli işlemler, bu amaç için tahsis edilen ve internet erişimi olmayan makineler üzerinden yapılmalıdır
Kuruma Uzaktan Bağlanan Cihazların Yönetimi	Kuruma uzaktan bağlanacak cihazların; zararlı yazılımdan korunma, işletim sistemi ve uygulama güncelliği vb. hususlar kapsamında kurum politikalarına uygunluğu güvenli uzaktan bağlantı sağlayan sistemler üzerinden (VPN vb.) kontrol edilmelidir. Kurum politikasına uymayan cihazlara bağlantı izni verilmemelidir
Kripto Ağ Cihazlarının Kullanımı	Kritik ağ ortamları arasındaki iletişim için kripto ağ cihazları kullanılmalıdır

Kablosuz İletişim Güvenliği	Kritik veri kablosuz ağ üzerinde taşınırken çok faktörlü kimlik doğrulaması gerektiren kimlik doğrulama protokollerinin (EAP/TLS vb.) bilinen zafiyet içermeyen güvenilir sürümleri kullanılmalıdır
Kablosuz Çevre Birimleri Kullanımının Engellenmesi	Kritik veri işleyen, internete herhangi bir erişimi bulunmayan kapalı ağlarda kablosuz fare ve klavye gibi çevre birimlerinin kullanılması engellenmelidir
Veri Transferi	Düzenli veri aktarımı ihtiyacı bulunan kritik seviyeli ağlarda veri diyotu, hava boşluğu şeklinde çalışan güvenli aktarım yöntemleri üzerinden tek yönlü veri aktarımı yapılmalıdır

Veri Sınıflandırma Politikasının Oluşturulması	Kurum verilerinin sistematik olarak kategorilere ayrılması ve sınıflandırılması için politikalar oluşturulmalıdır
Servis Sağlayıcıdan Alınan Hizmetlerde Veri Güvenliği Hususları	Bulut servisleri kullanımı durumunda veri erişimi, muhafazası, kullanımı kapsamındaki güvenlik hususları servis şartname ve sözleşmelerinde belirtilmelidir.
Kritik Verinin Envanteri Yönetimi	Kurum bünyesinde veya dışında, kurumun teknoloji sistemleri tarafından depolanan, işlenen veya iletilen tüm kritik verinin envanteri tutulmalıdır
Düzenli Olarak Erişilmeyen Kritik Verinin ve Sistemlerin Kaldırılması	Kurum tarafından düzenli olarak erişilmeyen kritik veri veya sistemler ağdan çıkarılmalıdır. Bu sistemler ihtiyaç duyulmadığı durumlarda ağ bağlantısı kesilmiş olarak tutulmalıdır
Bulut Servislerinin Kullanımı	Bulut depolama ve bulut e-posta servisi kullanımında Bölüm 4.3'te ifade edilen hususlar uygulanmalıdır. Bk. Bölüm 4.3
Taşınabilir Ortam Yönetimi	İş ihtiyaçları gereği taşınabilir ortamların kullanılması gerektiği durumlarda, yalnızca kurum tarafından yetkilendirilmiş ve kurum envanterine kayıt edilmiş taşınabilir ortamların kullanılmasına izin verecek şekilde gerekli önlemler alınmalıdır. Bk. Tedbir Başlık No: 3.3.3
Ağda Kritik Veri Taşınması	Ağda kritik verinin taşınmasında güvenli protokoller kullanılmalı (VPN teknolojileri, SSL/TLS vb.) ve kritik veri şifreli olarak taşınmalıdır

Ağ İçerisinde Veri Sızıntısı Önleme	Ağ içerisinde veri akışını kontrol etmek, izlemek ve izinsiz ağ trafiğini takip etmek amacıyla ağ tabanlı veri sızıntısı önleme sistemi kullanılmalıdır
Durağan Veri Güvenliğinin Sağlanması	Durağan veri ortamlarında yer alan kritik veri, şifrelenerek muhafaza edilmelidir. Depolanan kritik veri kimlik doğrulama mekanizması gerektiren ikincil bir araç kullanarak şifrelenmelidir. Kritik veriyi görüntülemek veya kritik veride değişiklik yapmak için gerçekleştirilen tüm işlemler kayıt altına alınmalıdır
Taşınabilir Ortam Engelleme	Kritik sistemler taşınabilir depolama birimlerini desteklemeyecek şekilde yapılandırılmalıdır. Taşınabilir depolama birimleri takıldığında uyarı üretecek mekanizmalar aktif edilmelidir. Bu uyarılar izlenmelidir

İz ve Denetim Kayıtlarının Tutulması	Tüm sistemlerde ve ağ cihazlarında kayıt mekanizması etkin olmalıdır. Kayıtlar, bilgi güvenliği gereksinimleri ve ilgili mevzuat gereği kabul edilebilir süre boyunca cihaz üzerinde veya harici sistemlerde tutulmalı, yetkisiz erişime ve değişime karşı korunmalıdır. Kayıtlar, muhafazaları için tanımlanan kabul edilebilir sürenin sona ermesi ile birlikte güvenli bir şekilde yok edilmelidir
Denetim Kayıtlarının Yönetimi	Sistem yöneticisi, operatörler ve kullanıcıların faaliyetleri kayıt altına alınmalı, kayıtlar korunmalı ve düzenli olarak gözden geçirilmelidir
Zaman Sunucusu Kullanımı	Kayıtlarda zaman damgalarının tutarlı olması için ağa bağlı tüm sistemlerin (sunucular, iş istasyonları, güvenlik ürünleri, ağ aygıtları vb.) düzenli olarak zaman bilgisinin alındığı; yedekli yapıda ve senkronize zaman sunucusu kullanılmalıdır. Bk. Tedbir No: 5.1.1.11

Detaylı Kayıt Tutulması	Sistem iz kayıtları; olay açıklaması, olay kaynağı, olay zamanı, kullanıcı/sistem bilgisi, kaynak adresleri, hedef adresleri ve işlem detayları bilgilerini içerecek şekilde tutulmalı ve bütünlüğü zaman damgası ile korunmalıdır
Kayıtlar için Yeterli Depolama Alanı Tahsisi	Kayıt tutan sistemlerde yeterli depolama alanı tahsis edilmelidir. Depolama alanı doluluk oranı düzenli olarak kontrol edilmelidir
Merkezi Kayıt Yönetimi	Analiz ve inceleme amacıyla kayıtlar merkezi bir kayıt yönetim sisteminde toplanmalı ve düzenli olarak yetkili personel tarafından gözden geçirilmelidir. Kayıt tutma veya gönderme işlemi sırasında hata oluştuğunda uyarı mekanizmaları aktif edilmeli ve izlenmelidir
Kayıt Analizi Araçları Kullanımı	Siber olayların korelasyon kuralları doğrultusunda tespiti ve detaylı analizi için siber tehdit ve olay yönetim sistemleri veya kayıt analizi araçları kullanılmalıdır
Siber Tehdit ve Olay Yönetim Sistemlerinin Düzenli Yapılandırılması	Aksiyon alınabilecek olayların daha iyi tanımlanabilmesi ve gereksiz olayların elenebilmesi amacıyla siber tehdit ve olay yönetim sistemlerinin yapılandırması düzenli olarak gözden geçirilmelidir. Kayıtlar düzenli olarak izlenmelidir. Bk. Tedbir Başlık No: 3.1.10

Güncel Sürümlerin Kullanılması	Sanallaştırma ürünlerinin üretici tarafından desteği devam eden ve kararlı sürümleri kullanılmalıdır. Bu ürünlerin güvenliği ile ilgili duyurular takip edilmelidir
Kapasite Planlaması	Gelecekteki ihtiyaçlar, yasal yükümlülükler ve olası güvenlik riskleri göz önünde bulundurularak sistem kaynaklarının planlaması yapılmalı ve kaynaklar sürekli izlenmelidir. Kapasite artırımı için kurumsal eşik değerleri tanımlanmalıdır
Sanal Makinelerin Yönetilmesi	Sanallaştırma ortamında kullanılmayan sanal makineler kapatılmalı, ağdan izole edilmeli ve sanal makine görev ömrünü tamamlayınca üzerinde yer alan veriler güvenli silme yöntemleri ile imha edilmelidir.

İşletim Sistemi Sıkılaştırmalarının ve Güvenlik Kontrollerinin Yapılması	Kullanılmakta olan işletim sistemleri, iş gereksinimlerini karşılamak için ihtiyaç duyulan bağlantı noktaları, protokoller ve servisleri sağlayacak şekilde sıkılaştırılmalıdır. Zararlı yazılımdan korunma uygulamaları kullanılmalı, dosya bütünlüğünü izleyecek ve kayıt tutacak mekanizmalar devreye alınmalıdır. Bk. Bölüm 5.1
Tedarik Edilen Sanallaştırma Hizmeti Ortam Güvenliğinin Sağlanması	Sanallaştırma hizmetinin üçüncü taraflar aracılığıyla sunulması durumunda, sanallaştırma ortamının güvenliği garanti altına alınmalıdır. Bk. Tedbir No: 3.5.3.3 Bk. Bölüm 4.3
İmaj Bütünlüğünün Denetlenmesi ve İzlenmesi	Tüm sanal makine imajlarının bütünlüğünü denetleyecek ve izleyecek mekanizmalar devreye alınmalıdır
Sanal Ağ Güvenliği	Ağ ortamları ve sanal makineler, kurum tarafından belirlenen kriterlere göre güvenilir ve güvenilmeyen bağlantılar arasındaki trafik kısıtlanacak şekilde yapılandırılmalıdır. Bu yapılandırmalar düzenli olarak gözden geçirilmeli; izin verilen tüm servisler, protokoller, portlar dokümante edilmeli ve kullanım gerekçesi gösterilmelidir. Bk. Tedbir No: 3.1.6.6
Operasyon ve Test Ortamlarının İzolasyonu	Operasyon ve test ortamları güvenlik duvarları, alan/bölge bazlı kimlik doğrulama vb. yöntemler kullanılarak birbirinden ayrılmalı ve bu ortamların yöneticileri için görevler ayrılığı prensibi uygulanmalıdır
Sanallaştırma Yönetim Ortamına Erişim	Sanallaştırma sistemleri yönetim arayüzlerine erişim, iş ihtiyaçları doğrultusunda tanımlanan yetki ile güvenli bir şekilde yapılmalıdır
Sanallaştırma Ortamı Sertifika Yönetimi	Sanallaştırma ortamında kendinden imzalı sertifikalar yerine kuruma ait ve yetkili otoriteden alınmış sertifikalar kullanılmalıdır
Sanal Makineler Arası Trafiğin Kontrol Edilmesi	Sanal makineler arasındaki trafik güvenlik kontrollerinden geçirilmeli, olası zararlı trafiğin ağdaki diğer sanal ve fiziksel makinelere ulaşmaması için gerekli önlemler alınmalıdır

Depolama Ortamları ile İletişim Güvenliğinin Sağlanması	Sanallaştırma ortamları ile birlikte kullanılacak veya kurum bünyesinde müstakil olarak kullanılacak depolama ortamları ile iletişimin güvenliğinin sağlanmasında aşağıdaki hususlar dikkate alınmalıdır. • Ağ dosya paylaşım servisleri, ayrılmış depolama ağlarında veya yönlendirilemeyen ağlarda hizmet vermelidir. • Ağ dosya paylaşım servislerinde, eğer destekleniyorsa trafik şifreli olmalı, uygun kimlik doğrulama protokolleri kullanılarak erişim denetimi yapılmalı ve kayıtlar tutulmalıdır
Fiziksel Kaynakların İzole Edilmesi	Farklı güvenlik seviyesinde yer alan ağlarda kullanılan sanal sistemlere ait kaynaklar fiziksel olarak izole edilmelidir.

Siber Olaylara Müdahale Planlarının Hazırlanması	Siber olaylara müdahale planları; uygulanması gereken akış, rol ve sorumlulukları içerecek şekilde dokümante edilmelidir. Kurumsal SOME Kurulum ve Yönetim Rehberi'ne uygun olarak çalışmalar yürütülmelidir.
Siber Olay Yönetimi Kapsamında Görev Alacak Personelin Belirlenmesi	Siber olayların yönetimi aşamalarında görev alacak personelin rol ve sorumlulukları tanımlanmalı, olay müdahale için gerekli teknik alt yapı personele sağlanmalı ve belirlenen personel ilgili taraflara bildirilmelidir. Siber olay yönetimi kapsamında görev alacak personel Kurumsal SOME Kurulum ve Yönetim Rehberi kriterlerine uygun olmalıdır
İletişim Bilgileri Dokümanının Hazırlanması	Siber olay bildirimi yapılacak resmi kurumlara ilişkin iletişim bilgileri dokümanı oluşturulmalı ve periyodik olarak gözden geçirilmelidir. İletişim bilgileri dokümanı, iletişim kurulacak konu kapsamında iletişim kurulacak kişileri tanımlamalıdır
Siber Tehdit Bildirimlerinin Yönetilmesi	Kurumlar siber olayların tespiti için gerekli altyapıları kurmalı, USOM ve olası diğer siber tehdit istihbarat kaynaklarından alınan bildirimler doğrultusunda gerekli önlemleri almalıdır

Siber Olayların Raporlarının Standardize Edilmesi ve Yayınlanması	Siber olaylar ile ilgili bildirim süresi ve rapora yansıtılacak bilgiler USOM tarafından belirlenen kriterler göz önünde bulundurularak belirlenmeli ve standart hale getirilmelidir. Yaşanan siber olaya ilişkin iş ve işlemlerin detaylı bir şekilde anlatıldığı siber olay müdahale raporu, kurum standartlarına göre hazırlanmalı, üst yönetim, USOM ve varsa bağlı olduğu Sektörel SOME'ye iletilmelidir
Üçüncü Taraflardan Alınan Siber Olay Yönetim Hizmetleri	Kurumların siber olay yönetimi kapsamındaki hizmetleri üçüncü taraflardan alması durumunda hizmetin güvenliği garanti altına alınmalıdır. Bk. Tedbir No: 3.5.3.3 Bk. Bölüm 4.3
SOME Personeli için Periyodik Siber Olay Tatbikatlarının Yapılması	SOME personelinin, gerçek dünyadaki tehditlere cevap verme konusundaki yeteneklerini arttırmak için rutin tatbikatlar planlanmalı ve uygulanmalıdır. Tatbikatlar iletişim kanallarını, karar mekanizmasını ve olaylara müdahale ekibinin teknik yeteneklerini test etmelidir. Tatbikat sonrasında tatbikat sonuçları ve öğrenilmiş dersler değerlendirilmeli ve kayıt altına alınmalıdır
Siber Olay Yönetimi Puanlama ve Önceliklendirme	Olaylar, kuruma potansiyel etkileri göz önünde bulundurularak puanlanmalı ve olayların giderilmesi için hazırlanan aksiyon planında önceliklendirme için risk temelli bir model kullanılmalıdır

Sızma Testleri ve Güvenlik Denetimlerinin Gerçekleştirilmesi	Kurum sistemlerinin güvenlik açıklarını ve saldırı yüzeyini belirlemek için düzenli aralıklarla harici ve dâhili sızma testleri ve güvenlik denetimleri gerçekleştirilmelidir. Sızma testleri ve güvenlik denetimleri gerçekleştirilmeden önce testi gerçekleştirecek taraftan, test süresince elde edilen hiçbir verinin yetkisiz kişilere verilmemesi, aktarılmaması ve ifşa edilmemesine yönelik taahhüt alınmalıdır. Sızma testi ve güvenlik denetimi kapsamı tanımlanmalı ve dokümante edilmelidir. Sosyal mühendislik testleri de sızma testi kapsamına dâhil edilmelidir.

Sızma Testlerinin Kullanıcı Profillerine Göre Gerçekleştirilmesi	Sağlıklı ve gerçek hayata uygun bir sızma testi için testler sırasında anonim kullanıcılar, misafir kullanıcılar, çalışanlar, kurumdan hizmet alan kullanıcılar ve kuruma destek veren kullanıcılar gibi farklı yetki seviyesindeki kullanıcı profilleri kullanılmalıdır
Sızma Testi Gerçekleştirilemeyen Bileşenlerin Yönetimi	Operasyonel ortamda olup sızma testi yapılması mümkün olmayan veya yüksek risk içeren sistemler için güvenlik denetimleri ve güvenlik sıkılaştırmaları düzenli olarak yapılmalıdır.
Sızma Testi için Oluşturulan Hesapların Yönetimi	Sızma testini gerçekleştirmek için kullanılan herhangi bir kullanıcı veya sistem hesabı, yalnızca meşru amaçlar için kullanıldığından emin olmak için kontrol edilmeli, izlenmeli, kayıt altına alınmalı ve test bittikten sonra pasif hale getirilmelidir
Doğrulama Testlerinin Yaptırılması	Kapatılan güvenlik açıklarına yönelik doğrulama testleri görevlerin ayrılığı ilkesi doğrultusunda yapılmalıdır
Sızma Testi ve Güvenlik Denetimi Bulgularının Seviyelendirilmesi	Sızma testi ve güvenlik denetimi bulguları karşılaştırılabilir bir puanlama yöntemi dikkate alınarak raporlanmalıdır
Test Ortamlarının Hazırlanması	Canlı ortamda olup sızma testi yapılması mümkün olmayan ve/veya yüksek risk içeren sistemler için gerçeğine benzer test ortamları oluşturulmalıdır. Test ortamının oluşturulması mümkün olmayan her bir bileşen için 3.1.11.3 numaralı tedbir maddesi uygulanmalıdır
Sızma Testleri ve Güvenlik Denetimlerinin Periyodu	Sızma testleri ve güvenlik denetimleri yılda en az 1 defa yapılmalıdır
Düzenli Kırmızı Takım Tatbikatlarının Yapılması	Siber saldırılara karşı kurumsal hazırlığı test etmek adına düzenli kırmızı takım tatbikatları yapılmalı veya yaptırılmalıdır. Tatbikat sonuçları kurum içi dokümante edilerek raporlanmalıdır. Rapor sonuçlarına göre kurumda gerekli iyileştirmeler sağlanmalıdır
Kurum Ağına Eklenen Yazılımın ve Donanımın Kontrolü	Kurum ağına eklenecek donanıma veya yazılıma, ağa dâhil edilmeden önce zafiyet taraması ve güvenlik denetimi yapılmalıdır

Erişim Kontrol Politikasının Oluşturulması ve Uygulanması	Erişim kontrol politikaları oluşturulmalı, uygulamaya alınmalı ve güncelliği periyodik olarak kontrol edilmelidir. Kullanıcı (sistem yöneticisi ve sisteme işlem amacıyla erişen kullanıcılar) hesap işlemleri (açma, kapama, değişiklik) ve erişim talepleri tanımlı bir süreç ile takip edilmeli ve kayıt altına alınmalıdır

Kullanıcı Hesaplarının Yönetimi	Her kullanıcı için kendine ait ve kendisini benzersiz olarak tanımlayan bir kullanıcı hesabı tanımlanmalı, tüm kullanıcı hesaplarına ait bir parola ataması yapılmalıdır. Kullanıcı hesaplarına ait parolalar belirlenirken dikkat edilmesi gereken kurallar tanımlanmalı ve uygulanmalıdır
Başarısız Oturum Açma Denemelerinin Yönetimi	Oturum açma mekanizmasına yapılacak saldırıları engellemek amacıyla uygun güvenlik önlemleri (istek sınırlandırma, IP bloklama, CAPTCHA vb.) alınmalıdır. Başarısız oturum açma denemeleri kayıt altına alınmalıdır
Varsayılan Kullanıcıların ve Parolaların Değiştirilmesi	Kurum bilgi sistemindeki herhangi bir varlıkta varsayılan kullanıcı adı ve parolalar kullanılmamalıdır. Test ortamlarında kullanımda olan tüm varsayılan kullanıcılar ve parolalar, canlıya alınmadan önce silinmeli veya değiştirilmelidir
Yönetici Hesaplarının Kullanımı	Sistem yöneticilerinin yüksek haklar gerektiren işlemleri yapmak için ayrı bir hesapları olmalıdır. Yönetici hesaplarıyla yapılan işlemler için denetim kayıtları oluşturulmalıdır.
İşlem Yapılmayan Oturumların Sonlandırılması	İşlem yapılmayan oturumlar belirli bir süre sonra sonlandırılmalıdır
Kimlik Doğrulama	Kurum kaynaklarına erişimlerde kimlik doğrulama mekanizmaları kullanılmalıdır.
Kullanıcı Yetkilerinin Güncellenmesi	Sistem yöneticilerinin ve kullanıcılarının yetkileri düzenli olarak gözden geçirilmeli, görev değişikliklerinde erişim yetkileri güncellenmelidir. Bir personelin veya yüklenicinin sorumluluklarının değişmesinden hemen sonra hesapları devre dışı bırakmak ve sistem erişimini iptal etmek için süreç oluşturulmalı ve uygulanmalıdır. Bu hesaplar devre dışı bırakılmalıdır.

Kurum Dışı Paydaşların Uzaktan Erişimi	Kurum dışı paydaşların kurum kaynaklarına uzaktan erişimine, ilgili kurum personelinin onayı dışında izin verilmemelidir. Uzaktan erişimin gerçekleştiği durumlarda ise aşağıdaki kurallar uygulanmalıdır: • Erişim yetkisi sınırlı ve belirli bir süreyle tanımlanmalıdır. Oturum zaman aşımı süresi belirlenmeli ve süre sonunda kullanıcı kimlik doğrulamaya zorlanmalıdır. • Çok faktörlü kimlik doğrulama metotları aktif edilmelidir. • Erişimin gerçekleştiği hedefler ile erişimin yapıldığı kaynaklar için kısıtlama yapılmalıdır. • Erişimlere ilişkin iz kayıtları tutulmalıdır. Bk. Tedbir No: 3.1.8.1 • Herhangi bir anomali ve ihlal durumuna karşın gerekli izleme ve alarm mekanizmaları aktifleştirilmelidir. • Gerektiği durumlarda video kayıt ve personel gözetimi metotları işletilmelidir. • Erişim yolu şifreli ve güvenli olmalıdır
Kullanılmayan Hesapların Devre Dışı Bırakılması	Belirli bir süre kullanılmayan, bir iş süreci veya kurum personeli ile ilişkilendirilemeyen tüm hesaplar otomatik olarak devre dışı bırakılmalıdır
Yönetici Hesaplarının İşletimi	Etki alanı ve yerel hesaplar dâhil tüm yönetim hesaplarını yönetmek için otomatik araçlar kullanılmalıdır. Kurumdaki sistemler bir yönetici hesabı oluşturulduğunda veya silindiğinde kayıt tutacak ve alarm oluşturacak şekilde yapılandırılmalıdır. Tüm yönetici hesap erişimleri için çok faktörlü kimlik doğrulama ve şifreli kanallar kullanılmalıdır. Kurumdaki sistemler bir yönetici hesabından giriş denemesi yapıldığında kayıt tutmalı ve giriş denemesi yapılması durumunda alarm oluşturacak şekilde yapılandırılmalıdır
Betik Dillerinin Kullanımına Yönelik Erişimin Sınırlandırılması	Betik dosyası oluşturma araçlarına (PowerShell ve Python gibi) erişim, yalnızca iş amaçları doğrultusunda bu özelliklere erişmesi gereken hesaplar ile sınırlandırılmalıdır.
Kimlik Yönetim ve Doğrulama Sistemlerinin Envanterinin Tutulması	Yerel veya uzak servis sağlayıcılarında bulunanlar da dâhil olmak üzere, kurumun tüm kimlik doğrulama sistemlerinin ve bu sistemlerle entegre uygulamaların envanteri tutulmalıdır.
Merkezi Kimlik Doğrulama	Kimlik doğrulama merkezi olarak yapılmalıdır. Merkezi kimlik yönetim ve doğrulama sisteminin kullanılamadığı durumlarda, risk analizi çalışması doğrultusunda telafi edici önlemler alınmalıdır.

Yedekleme Planının Oluşturulması	Kurum bünyesinde iş süreçlerinde kullanılan ve iş süreçlerini destekleyen tüm sistemler göz önünde bulundurularak yedekleme ihtiyacı olan sistemler tespit edilmeli ve dokümante edilmiş bir yedekleme planı üzerinden yedekleme yönetimi yapılmalıdır. Yedekleme planı en az aşağıdaki başlıkları içerecek şekilde oluşturulmalıdır: • Yedeği alınan sistemler • Yedekleme işleminin adı • Yedekleme işlemi başlangıç tarih ve saat bilgisi • Yedekleme tipi • Yedekleme periyodu • Yedekleme süreçlerinde versiyonlama

Çok Faktörlü Kimlik Doğrulama Yapılması	Kurum ağına dışarıdan yapılan erişimler çok faktörlü kimlik doğrulaması ile sağlanmalıdır
Kimlik Doğrulama Bilgilerinin Güvenli Olarak Saklanması	Tüm kimlik doğrulama bilgileri güçlü kriptografik algoritmalar kullanılarak saklanmalı ve şifreli kanallar kullanılarak iletilmelidir
Servis Hesaplarının Yönetimi	Servis hesapları en az yetki prensibi göz önünde bulundurularak oluşturulmalıdır. Kullanıcı veya yetkili hesaplar servis hesabı olarak kullanılmamalıdır. Servis hesaplarının kurum içerisinde bir sahibi olmalı ve periyodik olarak gözden geçirilmelidir
Hesap Giriş Davranışlarında Değişikliklerin Saptanması	Kullanıcı davranışları, kullanıcı rolü ve yetki seviyesi değişiklikleri güvenlik ihlal durumlarına karşı izlenmeli ve alarm mekanizmaları devreye alınmalıdır
Oturum Kayıtlarının Tutulması	Gizlilik dereceli verilerin saklandığı/işlendiği sistemler üzerinde sistem yönetimi amacıyla açılan oturumlar sırasında gerçekleştirilen faaliyetler kayıt altına alınmalı ve alınan kayıtların doğrulaması yapılmalıdır
Sistem Yöneticisi Görevlerinin Güvenliği	Tüm sistem yöneticisi görevleri belirli IP adresleri kullanılarak yapılmalıdır. Yönetim işlemlerini gerçekleştiren sistem yöneticileri, sadece yönetimsel haklar gerektiren işler için ilgili hesapları kullanmalıdır. Yetkilendirmelerin senede en az 1 kez olacak şekilde gözden geçirilmesi, gereksinimi kalmamış yetkilerin geri alınması sağlanmalıdır.
Veri ve Parola Güvenliğinin Sağlanması	Veri ve parolaların güvenliğinin sağlanması gerektiğinde otomatik parola yönetim aracı (password vault) kullanılmalıdır

Yedekleme Planının Periyodik Olarak Gözden Geçirilmesi	Yedekleme planı, yedekleme ihtiyaçları göz önünde bulundurularak yılda en az bir kere gözden geçirilmelidir. Bu gözden geçirme kapsamında iş birimleri ile de görüşülerek yedekleme ihtiyacı ortadan kalkan sistemler tespit edilmeli, yedekleme işleminden çıkarılmalı ve yedekleme işleminde olmayan fakat dâhil edilmesi gereken sistemler tespit edilerek yedekleme işlemine dâhil edilmelidir.
Yedekleme İşlemleri için İz Kayıtlarının Oluşturulması	Yedekleme işlemlerine ilişkin iz kayıtları oluşturulmalı, bu kayıtlar bilgi güvenliği gereklilikleri ve ilgili mevzuat göz önünde bulundurularak tanımlanmış süre kadar tutulmalı ve zaman damgası ile korunmalıdır.
Yedekten Geri Dönüş Testleri	Yedekleme ortamlarının çalıştığından ve geri dönülebilir olduğundan emin olmak adına; kapsamdaki sistemlerin, uygulamaların ve verinin yedekleri düzenli olarak geri dönüş testlerine tabi tutulmalı ve gerçekleştirilen geri dönüş testlerine yönelik kayıtlar oluşturulmalıdır. Bu kayıtlar en az aşağıdaki bilgileri içermelidir: • Testin gerçekleştirildiği gün ve saat bilgisi • Testi yapılan sistemler • Testin gerçekleştirildiğini kanıtlayan ekran görüntüleri • Testin başarılı sonuçlanıp sonuçlanmadığı • Test sırasında karşılaşılan sorunlar ve çıkarılan dersler.
Yedekleme Medyalarının Saklanması, Güvenliği ve İmhası	Yedekleme medyalarının envanteri tutulmalı ve envanter periyodik olarak gözden geçirilmelidir. Yedekleme medyaları, fiziksel olarak güvenli ve yedek alınan bölgeden farklı bir konumda saklanmalıdır. Yedeklenen verinin; ana sistemlerin bulunduğu ortamla benzer riskleri içermeyen başka bir ortamda saklandığı teyit edilmelidir. Yedeklenen veri tesis/yerleşke dışına taşınırken güvenliğinin sağlandığı ve bulunduğu ortamın fiziksel ve mantıksal güvenliğinin sağlanmış olduğu teyit edilmelidir. Yedekler kullanım süresinin sona ermesi sonrasında ulusal/uluslararası standartlara uygun olarak güvenli bir şekilde imha edilmeli ve imha kayıtları tutulmalıdır
İş Sürekliliği Kapsamının Tanımlanması	Kurumun faaliyet alanı ile yasal ya da sözleşmelerden doğan yükümlülükleri de göz önünde bulundurularak iş sürekliliği çalışmaları kapsamında ele alınması gereken hizmetler, birimler ve lokasyonlar tanımlanmalıdır

İş Sürekliliği Planlarının Hazırlanması	Kapsam dâhilinde yer alan hizmetler, birimler ve lokasyonlar göz önünde bulundurularak iş sürekliliği planları hazırlanmalı ve belirli aralıklarla gözden geçirilmelidir.
İş Sürekliliği Kapsamında Rol ve Sorumlulukların Tanımlanması	İş sürekliliği kapsamında olan tüm paydaşların ve süreç içinde yer alacak personelin görev ve sorumlulukları dokümante edilmeli ve ilgili taraflara bildirilmelidir.
İş Sürekliliği Çalışmalarında Üçüncü Taraf Hizmetlerin Dikkate Alınması	İş sürekliliği planları kapsamında; hizmet alınan üçüncü tarafların rol ve sorumlulukları ile birlikte tedarik edilen hizmetlerin süreklilik kriterleri de dikkate alınmalıdır.
İş Sürekliliği Planlarının Test Edilmesi	Süreklilik yönetimi dâhilinde tüm planlar kurum tarafından belirlenen periyotlarda test edilmeli ve test sonuçları kayıt altına alınmalıdır.
İş Sürekliliği Planlarının Güvenli Muhafazası	Süreklilik yönetimi dâhilindeki planların, acil durum müdahale prosedürlerinin ve gerekli diğer dokümanların güncel versiyonlarının kurumun yerleşkesi içinde ve mümkünse kurum binası dışında belirlenecek bir yerde tutulması ve her türlü felaket senaryosu sırasında erişilebilir olması sağlanmalıdır
Felaket Kurtarma Planlarının Hazırlanması	İş sürekliliği planları göz önünde bulundurularak kritik bilgi sistemleri bileşenlerine yönelik felaket kurtarma planları oluşturulmalıdır. Plan içerisinde aşağıdaki konular göz önünde bulundurulmalıdır: • Felaket kurtarma planı yapılan yerleşkenin felaket kurtarma merkezinde manuel olarak devreye alınması için gerekli minimum envanter gereksinimi • Felaket sonrası normale dönüş planı kapsamında uygulanacak adımlar • Felaket sonrası adı geçen servise ait verinin aktarma işlemi tamamlandığında kabul edilebilir kayıp veri miktarı ve niteliği, maksimum kesinti süresi ile yedekten geri dönüş süresi

Felaket Kurtarma Planları Kapsamında Rol ve Sorumlulukların Tanımlanması	Felaket kurtarma planlarının devreye alınması aşamasında yer alacak tüm paydaşların ve süreç içinde yer alacak personelin görev ve sorumlulukları dokümante edilmeli ve ilgili taraflara bildirilmelidir.
Felaket Kurtarma Çalışmalarında Üçüncü Taraf Hizmetlerin Dikkate Alınması	Felaket kurtarma planları kapsamında; hizmet alınan üçüncü tarafların rol ve sorumlulukları ile tedarik edilen hizmetlerin sürekliliği dikkate alınmalıdır.
Felaket Kurtarma Planlarının Test Edilmesi	Felaket kurtarma çalışmaları dâhilindeki tüm planlar yılda en az bir kez test edilmeli ve test sonuçları kayıt altına alınmalıdıR
Felaket Kurtarma Planlarının Güvenli Muhafazası	Felaket kurtarma çalışmaları dâhilindeki planların güncel versiyonları her türlü felaket senaryosu sırasında erişilebilir olmalıdır.
Kritik Sistem Sürekliliğinin Sağlanması	Kurum tarafından kritik olarak belirlenen sistem, servis, uygulama ve altyapının hizmet sürekliliğini sağlamak amacıyla gerekli yedeklilik yapıları oluşturulmalıdır. Hizmetler devreye alınırken yedeklilik testleri yapılmalıdır. Hizmet seviye taahhütleri oluşturulmalı, ölçülmeli ve raporlanmalıdır.
Felaket Kurtarma Merkezi Oluşturulması .	Herhangi bir felaket anında bilgi sistemleri işlevlerinin sürdürülebilmesi için bir felaket kurtarma merkezi kurulmalıdır

Uzaktan Çalışma Politikasının Hazırlanması ve Uygulanması	Kurum tarafından uzaktan çalışma faaliyetlerinde uygulanması gereken şartları ve kısıtlamaları tanımlayan bir politika hazırlanmalı ve uygulanmalıdır. Hazırlanan politika asgari olarak aşağıdaki hususları içermelidir. • Önerilen uzaktan çalışma ortamı • Zararlı yazılımlardan korunma ve güvenlik duvarı gereksinimleri • Yetkisiz erişimin engellenmesi • Kablosuz ağ hizmetlerinin kullanımı • Yedekleme gereksinimleri • Fiziksel güvenlik • Kişilere ait teçhizatlar üzerinde geliştirilen işlere ait fikri mülkiyet hakları ile ilgili anlaşmazlıklar • Uzaktan çalışmanın sona ermesi durumunda; yetki ve erişim haklarının iptali ve kullanılan teçhizatın iadesi
Ekipman Güvenliğinin Sağlanması	Kurum personeli, uzaktan çalışma faaliyetlerinde yalnızca kurum tarafından sağlanan ve/veya yapılandırma ayarları kurumun bilgi güvenliği gereksinimlerine uygun olan cihazları kullanmalıdır.
Dosya Paylaşımı	Uzaktan çalışma faaliyetlerinde, çalışma dosyalarını paylaşmak için kurumsal kaynaklar kullanılmalıdır.
Farkındalık Eğitimlerinin Verilmesi	Uzaktan çalışan kurum personeline özellikle güçlü parola kullanımı, sosyal mühendislik ve kimlik avı/oltalama saldırıları gibi konularda farkındalık eğitimleri verilmelidir
Zararlı Yazılımdan Korunma Uygulamaları	Uzaktan çalışma kapsamında kurum bilgilerinin işleneceği cihazlarda zararlı yazılımdan korunma uygulaması kullanılmalı ve zararlı yazılımdan korunma uygulamalarında en güncel yama dosyalarının bulunması ve imza veri tabanının güncel olması sağlanmalıdır.
Güncel İşletim Sistemi ve Uygulamaların Kullanılması	Uzaktan çalışma kapsamında kurum bilgilerinin işleneceği cihazların işletim sistemlerinin ve kullanılan uygulamaların güncel olması sağlanmalı, güvenlik yamaları yüklü olmalıdır.
Kurum Kaynaklarına Uzaktan Erişim	Uzaktan çalışma kapsamında kurum kaynaklarına erişim VPN teknolojileri ve çok faktörlü kimlik doğrulama ile sağlanmalıdır. Erişimler kurum politikalarına göre en az yetki prensibine göre sınırlandırılmalıdır.

Video Konferans Uygulamalarının Kullanımı	Video konferans uygulamaları kurum içerisinde barındırılmalıdır. Kurum içerisinde barındırılmayan üçüncü taraf bir uygulama kullanılacak ise uygulama açık kaynak kodlu olmalıdır.
Güçlü Parola Kullanımı	Uzaktan çalışma kapsamında kurumun politikalarına uygun güçlü parolaların kullanılması sağlanmalıdır
Güncel Video Konferans Uygulamalarının Kullanılması .	Video konferans uygulamasının güncel olması ve uygulamada en güncel yamaların yüklü olması sağlanmalıdır
Video Konferans Görüşmelerine Yetkisiz Katılım	Video konferans görüşmelerine sadece toplantı bağlantı adresi kullanılarak yapılabilecek yetkisiz erişimler engellenmelidir.
Video Konferans Paylaşım İşlemleri ve Sohbet Özelliği	Video konferans uygulaması üzerinden toplantı sırasında toplantı moderatörü/yardımcı moderatör onayı ile; • İstenilen kullanıcının ekran paylaşımı durdurulabilmeli, • Sohbet (chat) özelliği devre dışı bırakılabilmeli, • Dosya paylaşımı özelliği devre dışı bırakılabilmelidir. Video konferans uygulaması üzerinden yapılacak dosya paylaşımlarında dosya kontrolü yapılmalıdır. Dosya kontrolü yapılamıyorsa video konferans uygulaması üzerinden dosya paylaşımı yapılması engellenmelidir. Video konferans uygulaması üzerinden yapılan görüşmeler (dosya paylaşımı, ses, video, chat) uçtan uca şifreli olmalıdır.
Video Konferans Katılımcı Yönetimi	Video konferans uygulaması üzerinden toplantıya erişimin toplantı moderatöründen önce sağlanması engellenmelidir.
Video Konferans Toplantı Odası İsimlendirmeleri	Video konferans uygulaması üzerinde yapılan toplantılarda, toplantı odası isimlendirmeleri karmaşık olarak oluşturulmalıdır
Kullanıcı Bilgisayarında Güvenlik Duvarının Aktif Olması	Uzaktan çalışan kullanıcı bilgisayarlarında güvenlik duvarı yazılımları aktif durumda olmalıdır.
Bekleme Odası Özelliğinin Bulunması	Video konferans uygulaması bekleme odası özelliği içermelidir. Katılımcılar, konferansı organize eden kişinin manuel onayı ile katılım sağlamalıdır.

Uç Nokta Seviyesinde Veri Sızıntısının Önlenmesi	Uzaktan çalışan kullanıcı bilgisayarlarında olası veri sızıntısını engellemek amaçlı uç nokta seviyesinde veri sızıntısını önlemeye yönelik güvenlik önlemleri alınmalıdır
Erişimin Kurum Bilgisayarları ile Sınırlandırılması	Uzaktan çalışma kapsamında sadece kurum cihazları üzerinden erişim sağlanmalıdır. VPN erişiminde kurum tarafından sağlanan cihazlar için oluşturulan sertifikaların kullanılması sağlanmalıdır

X.1. Fırsatlar

İlgili akademik ve idari bölümler ile dayanışma ve işbirliği imkanı

Teknoloji ve iletişim altyapılarına sahip olma ve geliştirme imkânı

.

İlgili alanımızın her kesimden özellikle de yönetimden kabul görmesinin, yatırım ve istihdama etkisi

Yeniliklere ve gelişmelere açık bir yönetim anlayışına sahip olunması

Bilişim teknolojilerinin hızla gelişmesine bağlı olarak, ülkemizde de ilgili yapısal değişikliklerin hızla yaygınlaşması ile bilişim hizmetlerinin ön plana çıkarak, kurumlar için lüks görülen birçok gereksinimin zorunluluk haline gelmesi.

Avrupa Birliğinin hedef ve programları, Yatırım ve araştırmalara devlet desteği
Sürekli gelişen teknolojinin hizmet sunumunda kaliteyi arttırması.

Bilgi işlem ve ilgili teknolojilerin geleceğe şekil veren öncü konular olması

İÇ KONTROL GÜVENCE BEYANI

Harcama yetkilisi olarak yetkim dâhilinde; Bu raporda yer alan bilgilerin güvenilir, tam ve doğru olduğunu beyan ederim.

Bu raporda açıklanan faaliyetler için idare bütçesinden harcama birimimize tahsis edilmiş kaynakların etkili, ekonomik ve verimli bir şekilde kullanıldığını, görev ve yetki alanım çerçevesinde iç kontrol sisteminin idari ve mali kararlar ile bunlara ilişkin işlemlerin yasallık ve düzenliliği hususunda yeterli güvenceyi sağladığını ve harcama birimimizde süreç kontrolünün etkin olarak uygulandığını bildiririm.

Bu güvence, harcama yetkilisi olarak sahip olduğum bilgi ve değerlendirmeler, iç kontroller, iç denetçi raporları ile Sayıştay raporları gibi bilgim dâhilindeki hususlara dayanmaktadır.

Burada raporlanmayan, idarenin menfaatlerine zarar veren herhangi bir husus hakkında bilgim olmadığını beyan ederim. (Yer-Tarih)

İmza

Ömer OKUCU

Daire Başkan V.