2024 YILI

BİLGİ TEKNOLOJİLERİ DAİRE BAŞKANLIĞI

BİRİM İÇ DEĞERLENDİRME RAPORU (BİDR)

ŞABLONU

İÇİNDEKİLER

ÖZET

BİDR raporu, Bilgi Teknolojileri Daire Başkanlığı'nın altyapısının ve süreçlerinin bir analizini sunmaktadır.

Raporun amacı, mevcut Bilgi Teknolojileri sistemlerini ve süreçlerini değerlendirmek, iyileştirme önerileri sunmak ve altyapısının güvenliğini artırmak için yapılan iyileştirme alanları hakkında bilgi vermektedir . Bu raporu hazırlamak birim iç değerlendirmemizi belirlenen Bilgi Teknolojileri hedeflerine uygun bir strateji geliştirmemize yardımcı olmaktadır.

BİDR raporu, Ankara Medipol Üniversitesi Bilgi Teknolojileri Daire Başkanlığı tarafından 2024 yılınına kadar yapılan faaliyetleri ve iyileştirme çalışmalarını kapsar.

BİDR'NİN HAZIRLANMASINDA KATKISI OLANLAR

İlkay ERDOĞAN- Bilgi Teknolojileri Daire Başkanı

Şermin BEKTAŞ- Kurumsal uygulamalar ve yazılım destek uzman yard.

Berat ARIKAN- Sistem Uzman Yardımcısı

Halis AYDOĞAN- Kontrat Kaynak Uzman Yardımcısı

BİRİM HAKKINDA BİLGİLER

İletişim Bilgileri

Bilgi Teknolojileri Daire Başkanı

İlkay ERDOĞAN

Tel: 0312 508 8730

E-posta : ilkay.erdogan@ankaramedipol.edu.tr

Tarihsel Gelişimi

- Bilgi Teknolojileri Daire Başkanlığı 2023 yılında ISO 27001 Standardı ile alakalı hedefler belirlendi. 2024 yılında belirlenen hedefler doğrultusunda ISO 27001 Bilgi Güvenliği Sertifika süreci tamamlandı.
- Bilgi Teknolojileri Daire Başkanlığı tarafından kalite yönetim süreçleri iyileştirme çalışmaları devam etmektedir.
- ISO 27001 Bilgi Güvenliği sertifikası, üniversitemizin bilgi güvenliği süreçlerinin uluslararası kabul görmüş standartlara uygunluğunu göstermektedir. Bu prestijli sertifika, Ankara Medipol Üniversitesi'nin bilgi varlıklarını koruma, veri gizliliğini sağlama ve siber tehditlere karşı dirençli olma taahhüdünün bir yansımasıdır.

Misyonu, Vizyonu, Değerleri ve Hedefleri

Misyon

“Bilgi Teknolojileri Daire Başkanlığı olarak, kurumumuzun iş stratejilerini desteklemek amacıyla güvenilir, yenilikçi ve etkili bilgi teknolojileri hizmetleri sağlamayı taahhüt ediyoruz. Teknoloji standartlarını benimseyerek, sürekli iyileştirme anlayışıyla hareket ediyor ve çalışanlarımızın ve öğrencilerimizin bilgi teknolojileri alanındaki ihtiyaçlarına çözümler sunuyoruz. Güçlü bir ekip ruhu ile, bilgi teknolojileri aracılığıyla kurumun hedeflerine ulaşmasına katkıda bulunuyoruz.”

Vizyon

“Bilgi Teknolojileri Daire Başkanlığı olarak, teknolojik liderlikte öncü olmayı, sürekli olarak teknoloji çözümleri sunmayı ve organizasyon genelinde dijital bilişim sağlayacak noktaya ulaşmayı hedefliyoruz. Öğrenci memnuniyetini odak noktamız yaparak, yenilikçi projeler ve stratejiler geliştirerek kurumunuzun sürdürülebilir bir teknoloji altyapısı oluşturmak için çabalıyoruz. Ekip çalışmasına dayalı, sağlık ve eğitim bilişimi alanında kurumumuzun vizyonunu gerçekleştirmeyi taahhüt ediyoruz.”

Değer

1. Verimlilik
Bilgi teknolojileri, iş süreçlerini hızlandırarak zaman ve maliyet tasarrufu sağlamaktadır. Otomasyon ve dijitalleşme sayesinde manuel işlemler azalmakta, operasyonel verimlilik artmaktadır.
2. Erişilebilirlik
Bilgiye her yerden ve her zaman erişim imkânı sunarak kullanıcıların kesintisiz çalışma ve bilgiye ulaşım süreçlerini desteklemektedir.
3. Güvenlik
Verilerin korunmasını sağlamak amacıyla güçlü şifreleme, erişim kontrolü ve siber güvenlik önlemleri uygulanmaktadır. Yetkisiz erişimlerin önlenmesi ve veri bütünlüğünün sağlanması hedeflenmektedir.
4. İnovasyon
Yeni fikirlerin geliştirilmesini ve uygulanmasını destekleyen bilgi teknolojileri, organizasyonların dijital dönüşüm süreçlerini hızlandırmaktadır.
5. Bağlantısallık
Kişiler, cihazlar ve sistemler arasında kesintisiz iletişim sağlanarak bilgi akışı hızlandırılmakta ve operasyonel süreçler daha etkin yönetilmektedir.
6. Otomasyon
Tekrarlayan işlerin minimize edilmesi, insan hatasının azaltılması ve iş gücünün daha stratejik alanlara yönlendirilmesi sağlanmaktadır.

7. Esneklik
Farklı sektör ve ihtiyaçlara göre uyarlanabilir çözümler sunarak organizasyonların değişen koşullara hızlı bir şekilde adapte olmasını mümkün kılmaktadır.
8. Maliyet Tasarrufu
Bilgi teknolojileri, dijitalleşme ile operasyonel giderleri düşürerek işletmelere uzun vadede maliyet avantajı sağlamaktadır.
9. Hızlı Karar Alma
10. İş Sürekliliği
Felaket kurtarma, veri yedekleme ve yüksek erişilebilirlik çözümleri ile iş süreçlerinin kesintisiz devamlılığı sağlanmaktadır.
11. Ölçeklenebilirlik
Bilgi teknolojileri altyapıları, küçük işletmelerden büyük kuruluşlara kadar büyümeye uygun şekilde yapılandırılabilmektedir.
12. Kullanıcı Deneyimi
Dijital hizmetlerin etkinleştirilmesiyle müşteri ve çalışan memnuniyeti artırılmakta, daha iyi hizmet süreçleri oluşturulmaktadır.
13. Uzaktan Çalışma İmkânı
Hibrit ve uzaktan çalışma modellerini destekleyerek çalışanların esnek çalışma ortamlarına uyum sağlamalarına olanak tanımaktadır.
14. Çevresel Sürdürülebilirlik
Kâğıt tüketiminin azaltılması, enerji verimli sistemlerin kullanılması ve dijitalleşmenin artırılması ile çevresel etkilerin minimize edilmesi hedeflenmektedir.
15. Uyumluluk ve Regülasyonlar
Bilgi güvenliği ve sektör standartlarına uyum sağlanarak yasal düzenlemelere uygunluk temin edilmektedir.
16. Eğitim ve Öğrenme Kolaylığı
Online eğitim platformları ve uzaktan eğitim çözümleri ile bilgiye erişim kolaylaştırılmakta, çalışanların sürekli gelişimi desteklenmektedir.
Bu kalite değerleri, bilgi teknolojilerinin organizasyonlara sunduğu stratejik avantajları ve sürdürülebilir iş süreçleri oluşturmadaki rolünü ortaya koymaktadır.

Hedef

Bilgi Teknolojileri Dairesi olarak, kurumumuzun dijital altyapısını güvenli, verimli ve sürdürülebilir hale getirme hedefi doğrultusunda çalışmalarımızı sürdürmekteyiz. Bu kapsamda, bilgi güvenliği yönetim sistemimizi güçlendirmek amacıyla ISO 27001 sertifikasını alarak uluslararası standartlara uyum sağladık.
Bilgi güvenliği ve veri koruma süreçlerimizi sürekli iyileştirerek, siber tehditlere karşı önleyici tedbirler almak, iş sürekliliğini sağlamak ve kullanıcı memnuniyetini artırmak temel önceliklerimiz arasındadır. Kurum içi süreçlerde dijitalleşmeyi yaygınlaştırarak hizmet kalitesini artırmayı, otomasyon sistemleri ile operasyonel verimliliği yükseltmeyi hedefliyoruz.
Ayrıca, IT bütçesini etkin yönetmek, açık kaynak ve bulut çözümlerinden yararlanarak maliyetleri optimize etmek, entegrasyon süreçlerini hızlandırarak veri akışını güvenli hale getirmek öncelikli hedeflerimiz arasındadır. İş sürekliliğini sağlamak için felaket kurtarma senaryolarını düzenli olarak test ediyor, yedekleme politikalarımızı güncelliyoruz.
ISO 27001 sertifikası ile tescillenen bilgi güvenliği politikalarımız doğrultusunda, tüm sistemlerimizde güvenliği en üst düzeyde tutmaya devam edeceğiz. Yeşil IT projeleriyle enerji verimliliğini artırarak çevresel sürdürülebilirliği desteklemekte ve dijital dönüşüm

süreçlerimizi hızlandırmaktayız. Bu hedefler doğrultusunda, güvenli ve yenilikçi bir IT altyapısı oluşturarak kurumumuzun teknolojik gelişimine katkı sağlamaya devam edeceğiz.

LİDERLİK, YÖNETİŞİM VE KALİTE

A.1. Liderlik ve Kalite

A.1.4. İç kalite güvencesi mekanizmaları

Eğitim ve Toplantı Takibinin Yapılması; BT Kalite Temsilcisi, iç kalite güvencesi sisteminin oluşturulması ve geliştirilmesinde etkin rol almıştır. Bilgi güvenliği yöneticisi tarafından "Bilgi güvenliği farkındalık eğitimi" ile ilgili BT ekibimize eğitimler vererek akreditasyon çalışmalarına önem gösterilmesi gerektiğinin farkındalığını kazandırmaya çalışmaktadır. Eğitim ve toplantı gibi faaliyetler kayıt altına alınması hedeflenmiştir **[1_OD2].** 2024 yılı eğitim süreçlerinde personellere eğitim ile ilgili soru sorularak eğitimin anlaşılabilirliği konusununda değerlendirilmesi hedeflenmektedir **[2_OD3].**

Bilgi Teknolojileri Daire Başkanlığı'na ait web sitesine "Vizyon ve Misyon, Bilgi Güvenliği, BT Hizmet Yönetimi (ITSM), Anket Yönetimi (Limesurvey), Öğrenci Danışmanlığı (MEBİS), Livechat, Elektronik Belge Yönetim Sistemi (EBYS) ile içerikler hazırlanmıştır. [OD3]

GLPI'nin ITSM (Information Technology Service Management) özellikleri, üniversitemizin BT taleplerini etkili bir şekilde yönetmemize olanak tanımaktadır. Öğrencilerden ve personel tarafında gelen MEBIS ve diğer hizmetlerle ilgili problemleri kolayca takip etmek ve çözüme kavuşturmak için kullanılan bu sistem, BT ekibimize daha hızlı ve düzenli bir yardım masası hizmeti sunmamıza imkân sağlamaktadır **[3_OD4].**

GLPI sayesinde taleplerin anında kaydedilmesi, önceliklendirilmesi ve izlenmesi hem öğrencilerin hem de personelin sorunlarına hızlı çözümler bulmamıza olanak tanımaktadır. Bu sayede ITSM, kurum içindeki teknolojik hizmetleri etkili bir biçimde yöneterek kurumsal performansı artırmaktadır [OD3]**[4_OD4].**

Olgunluk Düzeyi (4) Paydaş katılım mekanizmalarının işleyişi izlenmekte ve bağlı iyileştirmeler gerçekleştirilmektedir.

[1] (2) A.1.4.egitim_ve_toplanti_takibi

[2] (3) A.1.4.bilgi_guvenligi

[3] (4) A.1.4.itsm_kullanim_kilavuzu

[4] (4) A.1.4.itsm_takip_raporu

A.1.5. Kamuoyunu bilgilendirme ve hesap verebilirlik

Web Sitesi Bilgilendirme Ankara Medipol Üniversitesi web sitesinde vizyonumuz, misyonumuz ve değerlerimize ilişkin bilgilendirme yapılmaktadır.[OD4] Web sayfasında yer alan duyurular, ilk olarak 2019 yılında yayınlanmıştır. Web sitesinde yer alan duyurular, 06.05.2019 tarihinden itibaren yayınlanmaya başlanmış olup, toplamda 1019 adet duyuru bulunmaktadır. Bunlardan 72 tanesi arşivlenerek saklanmakta, 932 tanesi ise yayınlanmaya

devam etmektedir.Mailing Bilgilendirme, bir kurum veya bireyin belirli bir mesajı, duyuruyu veya bilgilendirmeyi hedef kitleye ulaştırmak için e-posta yoluyla göndermesini ifade etmektedir. Bu e-postalar, genellikle toplu bir şekilde belirli bir mailing listesine gönderilmektedir. Mailing listeleri, belirli bir konuda ilgilenen veya belirli bir kurum veya organizasyonla ilişkili olan kişilerin e-posta adreslerini içermektedir. Kurumdaki personellerin önemli bilgileri veya duyuruları zamanında bilgilendirmek için mailing sistemi kullanılmaktadır. Mail içerikleri etkinlikler, güncellemeler, yeni politikalar, iş fırsatları veya önemli değişiklikler gibi çeşitli konuları kapsamaktadır. Mailing, eğitim materyalleri, eğitim davetiyeleri veya bilgilendirici içerikler gibi eğitim amaçları için kullanılabilmektedir. Kurumlar, çalışanlar arasındaki iletişimi güçlendirmek ve iç haberleşmeyi kolaylaştırmak için mailing kullanmaktadır. İş takip hatırlatmaları, toplantı davetiyeleri, personel politikaları güncellemeleri gibi iç iletişimler için mailing sıklıkla kullanılmaktadır **[1_OD2].**

Olgunluk Düzeyi (4) Kurumun kamuoyunu bilgilendirme ve hesap verebilirlik mekanizmaları izlenmekte ve paydaş görüşleri doğrultusunda iyileştirilmektedir.

[1](2) A.1.5.mailing_bilgilendirme

A.2. Misyon ve Stratejik Amaçlar

A.2.2. Stratejik amaç ve hedefler

Stratejik amaç ve hedeflerimiz kurumun yapısına uygun olacak şekilde değerlendirilerek Ankara Medipol Üniversitesi oluşturulmuştur.

Stratejik Amaç; Kurumsal imajı geliştirerek, kurumsal kimlik ve markalaşmayı güçlendirerek üniversiteyi rekabetçi bir kurumsal ve fiziksel yapıya kavuşturmak, üniversite sıralamalarında istikrarla yükselmek ve ülkemiz araştırma üniversiteleri arasına girmek.
Stratejik Hedefler; Hedef Üniversite bilgi işlem alt yapısı, bilgi işlem sistemi ve web sisteminin geliştirilip güçlendirilmesini sağlamak.

A.3. Yönetim Sistemleri

A.3.1. Bilgi yönetim sistemi

Bilgi yönetimi, kurumun tüm verilerinin toplanması, işlenmesi, depolanması ve dağıtılması sürecini kapsar. Bu süreçte kurum kaynakları, dış ve iç tehditlere karşı korunmalı ve güvenli bir şekilde yönetilmelidir. Bilgi güvenliği, verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumak için kritik bir öneme sahiptir. Bu bağlamda, sunucu güvenliği için yazılımsal ve donanımsal koruma önlemleri alınmıştır.

Kurumun ihtiyaçlarına uygun bir güvenlik yazılımı olarak Trend Micro Deep Security seçilmiştir. Bu yazılımın kurulumu sırasında modüller aktif hale getirilmiş ve güvenlik stratejisi doğrultusunda belirlenen politika ve hedeflere ulaşılacak şekilde yapılandırılmıştır. Web İtibarı Modülü, kritik verilerin korunması amacıyla zararlı ve sahte sitelere erişimi engeller**[1_OD3]**. Uygulama Kontrolü Modülü ise yetkisiz yazılım yüklemelerini, sistem

yöneticisi dışındaki değişiklikleri ve kurum politikalarına uymayan uygulama kurulumlarını engelleyerek güvenliği artırır**[2_OD3]**. Bütünlük İzleme Modülü, Windows ve Linux tabanlı sunucularda dosya bütünlüğünü denetler, yalnızca yetkilendirilmiş değişikliklere izin verir ve yönetim dışındaki değişiklikler hakkında uyarılar gönderir **[3_OD3]**. Ayrıca, İzinsiz Giriş Önleme Modülü, sunucu güvenliğini sağlayarak hizmet kesintilerine yol açabilecek saldırıları engeller**[4_OD3]**. Bu modüller, kurumların operasyonel güvenliğini artırırken, olası tehditlere karşı etkin koruma sağlar. Yapılan yatırımlar ve etkin modüller sayesinde sunucu güvenliği üst düzeyde korunmakta ve güvenlik tehditlerine anında müdahale sağlanmaktadır. Sistem güncellemeleri ve yazılım düzenli olarak kontrol edilip uygulanacak, güvenlik denetimleri ve sızma testleriyle eksiklikler tespit edilip iyileştirme çalışmaları sürdürülecektir. Risk yönetimi kapsamında ise güvenlik açıkları anında tespit edilip değerlendirilerek, düzenli güvenlik raporları hazırlanacaktır.

Trend Micro Apex One (Uç Nokta Güvenliği)Kötü amaçlı yazılımdan koruma modülü, sunucu sistemlerimizi ve son kullanıcı cihazlarımızı kötü amaçlı yazılım, casus yazılım ve Truva atları yazılımlara karşı korumaktadır. Tüm clientlarımızda kurulu olan bu sistem, son kullanıcı güvenliğini ve yukarıda bahsi geçen tehdit unsurlarına karşı, oluşabilecek hizmet kesintisizliğini sağlamaktadır **[5_OD4].**

Trend Micro Deep Discovery (Ağ Güvenliği) Trend Micro Deep Discovery, kötü amaçlı yazılımları tespit eder ve istihbaratı diğer güvenlik katmanlarıyla paylaşır. Ön filtre teknolojisi gecikmeleri önler. Ek genişletilmiş algılama ve yanıt (XDR) yetenekleri, kötü amaçlı yazılımları tespit eder ve durdurur **[6_OD4][7_OD4].**

Güvenlik duvarı (FİREWALL) FortiGate güvenlik duvarı cihazı, sunuculara gelen ve giden trafiği izleyerek kontrol eder. Sunucularımıza yalnızca belirlediğimiz kaynaklardan erişim yapılmasına izin verir ve diğer tüm erişim taleplerini engeller. **VIP (Virtual IP)**, dışarıdan gelen trafiğin iç ağa yönlendirilmesini sağlayan bir yapılandırmadır. Cloudflare'dan gelen trafik, FortiGate cihazındaki VIP aracılığıyla iç sunucularımıza yönlendirilir.Geçen yılki BİDR raporunda belirtilen detayların yanı sıra, 2024 yılı itibariyle sunuculara tek tek SSL sertifikası yüklemek yerine, SSL offload sistemi kullanarak sertifikaları doğrudan FortiGate cihazı üzerinden yönetmeye başladık **[8_OD3].**

Güvenlik Bilgisi ve Olay Yönetimi (SIEM) güvenlik altyapısını izlemek, tehditleri tespit etmek ve bu tehditlere karşı zamanında müdahale edebilmek için kritik öneme sahip bir araçtır. SIEM, çeşitli güvenlik cihazları ve sistemlerden gelen olay verilerini toplayarak, bu verileri analiz eder ve güvenlik ihlalleri gibi potansiyel tehditlere karşı kurumun hızla aksiyon almasını sağlar. Kurumumuzda kullanılan Günlük İnceleme Modülü, bu amaç doğrultusunda önemli bir bileşendir **[9_OD3].** Günlük inceleme modülü, sunucularımızda meydana gelen tüm olayları kaydeden günlük dosyalarını düzenli olarak okuyarak analiz eder. Bu modül, özellikle güvenlik açısından kritik olan verileri sürekli izler ve potansiyel tehditlere karşı uyarılar üretir. Günlük kayıtlarında meydana gelen olaylar, kurumumuzun bilgi güvenliği seviyesini yükseltmek amacıyla titizlikle izlenir. Modül, izlediği günlük dosyalarında belirli bir olay veya anomali tespit ettiğinde, önleyici aksiyonları tetiklemek amacıyla uyarılar gönderir. Bu uyarılar, güvenlik ekibinin hızlı bir şekilde müdahale etmesini sağlar. Örnek olarak, bir sunucuya yapılan yetkisiz giriş denemelerinin sayısının belirli bir eşiği aşması durumunda, sistem otomatik olarak bir uyarı oluşturur.

Uyarı Türleri; Yetkisiz Giriş Denemeleri: Birden fazla başarısız giriş denemesi, potansiyel bir saldırı girişimini gösterebilir. Bu durumda, güvenlik ekibine derhal bir uyarı gönderilir.

Kritik Yapılandırma Değişiklikleri: Sistem yöneticisi dışında yapılan değişiklikler, sunucu güvenliğini tehdit edebilir. Bu tür değişiklikler tespit edilip uyarı oluşturulur.

Hata Mesajları: Sunucularda meydana gelen sistem hataları veya yapılandırma problemleri, genellikle güvenlik zafiyetlerine yol açabilir. Bu tür durumlar da izlenerek gerekli müdahale yapılır.

Bilginin elde edilmesi, kaydedilmesi, güncellenmesi ve paylaşılmasına ilişkin tanımlı süreçler Varlık Envanteri Sayımı **[10_OD4]** kurumda bulunan tüm dijital varlıkların (sunucular, ağ cihazları, yazılımlar, donanımlar vb.) düzenli olarak sayılmasını ve takip edilmesini sağlayan kritik bir güvenlik prosedürüdür. Bu süreç, bilgi güvenliği yönetimi açısından önemli bir adımdır çünkü, mevcut varlıkların tam listesine sahip olmak, güvenlik açıklarını tespit etmek ve siber saldırılara karşı hazırlıklı olmak için gereklidir. Varlık envanteri sayımı, kurumda yer alan tüm cihazlar ve yazılımlar üzerine yapılan taramalarla gerçekleştirilir. Bu sayede, her bir varlığın durumu, özellikleri ve güvenlik durumu hakkında bilgi edinilir. Envanter listesi, sürekli olarak güncellenir ve herhangi bir kayıp, değişiklik ya da yeni eklenen varlıklar raporlanır.

Bilgi güvenliği ve güvenirliğini sağlamaya yönelik süreçler ve uygulamalar kapsamında, kurumumuz belirli dönemlerde kurum içi ve kurum dışı, sahip olduğu tüm sistemlerin ve bilgilerin kötü amaçlı kişi/kişilerin erişiminden kaynaklı kaybolması veya zarar görmesinden korumak amacıyla zafiyet sızma testleri yaptırmaktayız. Sızma Testi Raporu **[11_OD3]** Test sırasında, kurumun sistemleri üzerinde gerçekçi saldırı senaryoları simüle edilerek, zafiyetler tespit edilmeye çalışılır. Testin sonunda, sızma testi raporu hazırlanır. Bu rapor, testin kapsamını, tespit edilen açıkları ve bu açıkları gidermek için alınması gereken aksiyonları içerir.

Birim, ihtiyaçları doğrultusunda geliştirdiği özgün yaklaşım ve uygulamalarla kurum içindeki çeşitli süreçlere yönelik etkili çözümler sunmaktadır. Kurum içi yazışmalar için EBYS **[OD4]**, eğitim-öğretim faaliyetleri için MEBİS otomasyonu **[OD4]** ve sürekli Eğitim Merkezi Yönetim sistemi **[OD4]**, dijitalleşme kapsamında sınavlar için E-sınav Plan (Moodle Aktarım) **[12_OD3]** ve öğrencilere yönelik Anket Yönetimi (LimeSurvey) [OD4] gibi uygulamalar kullanılmaktadır. Ayrıca, LiveChat [OD3] ve Yurt Bilgi Sistemi **[13_OD2]** gibi çözümlerle öğrenci hizmetleri daha verimli hale getirilmektedir. Kurum içindeki takip sistemleri için ise Digital Signage-RubuPlus **[14_OD4]**, RoomScope Oda Yerleşim ve Takip Yazılımı **[15_OD3],**CCTV Kamera NVR Takip Sistemi **[16_OD3]**, Personel Devam Kontrol Sistemi (PDKS) **[17_OD2],** Yemekhane Kartlı Geçiş Sistemi**[18_OD3]** ve Plaka Okuma Sistemi (PTS) **[19_OD2]** gibi yazılımlar geliştirilmiştir. Bu uygulamalar, kurumun verimliliğini artırarak süreçlerin dijital ortamda etkin bir şekilde yönetilmesini sağlamaktadır **[20_OD3].**

Kurumiçi dersliklerde karşılaşılabilecek sorunlara hızlı çözüm sunabilmek amacıyla, her dersliğe karekod ile entegre edilmiş bir WhatsApp destek hattı oluşturulmuştur. Akademisyenlerimiz ve öğrencilerimiz, karşılaştıkları herhangi bir sorun ile ilgili olarak bu destek hattına başvurmakta, saha destek ekibimiz ise anlık olarak yardımcı olmaktadır **[21_OD4].**

Olgunluk Düzeyi (3) Kurum genelinde temel süreçleri (eğitim ve öğretim, araştırma ve geliştirme, toplumsal katkı, kalite güvencesi) destekleyen entegre bilgi yönetim sistemi işletilmektedir.

[1] (3) A.3.1web_itibarı

[2] (3) A.3.1 uygulama_kontrolu

[3] (3) A.3.1 butunluk_izleme

[4] (3) A.3.1izinsiz_girişi_önleme

[5] (4) A.3.1trend micro_apex one(uç nokta guvenligi)

[6] (4) A.3.1trend micro_deep_discovery

[7] (4) A.3.1trend micro_deep_discovery

[8] (3) A.3.1 guvenlik_duvarı_(firewall)

[9] (3) A.3.1guvenlik_bilgisi_ve_olay_yonetimi_(sıem)

[10] (4) A.3.1 varlık_envanteri_sayımı

[11] (3) A.3.1 sızma_testi_raporu

[12] (3) A.3.1 e-sinav_plan_(moodle_aktarım)

[13] (2) A.3.1 yurt_bilgi_sistemi

[14] (4) A.3.1 digital signage_rubuplus

[15] (3) A3.1 roomscope_oda_planı

[16] (3) A.3.1 cctv_kamera_nvr_takip_sistemi

[17] (2) A.3.1 personel_devam_kontrol_sistemi_(pdks)

[18] (3) A.3.1 yemekhane_kartlı_gecis_sistemi

[19] (2) A.3.1 plaka_okuma_sistemi (pts)

[20] (3) A.3.1 yazilimlar

[21] (4) A.3.1 whatsapp_destek_hatti

A.3.4. Süreç yönetimi

BT Hizmet Yönetimi (ITSM) (Information Technology Service Management), Ankara Medipol Üniversitesinde çalışan akademik ve idari personel ile öğrencilerin sorunlarının kaydedilmesi, takibi ve çözümünün yönetilmesi için kullanılan sistemdir.[OD4]

BioPro (Teknik Bakım) sistemi Bilgi Teknolojileri Daire Başkanlığı' mıza ait ürünlerin depo giriş ve çıkış süreçleri takip edilmektedir. Depodan çıkan sarf malzemeler, barkodlama sistemiyle üniversitemizde teslim edilecek ve kurulacak ürünlerimizin lokasyonlara göre izlenebilir hale gelmektedir. Ayrıca, talep üzerine teslim edilen ürünler ilgili kişilere

zimmetlenmekte ve bu bilgiler sistem üzerinde kaydedilmektedir. Zimmet kayıtları, yalnızca elektronik ortamda tutulmakla birlikte, aynı zamanda fiziki olarak dosyalanarak birimimizde arşivlenmektedir.[OD3]

Olgunluk Düzeyi (3) Kurumun genelinde tanımlı süreçler yönetilmektedir.

A.4. Paydaş Katılımı

A.4.1. İç ve dış paydaş katılımı

Bilgi Teknolojileri Daire Başkanlığı iç ve dış paydaşları bulunmaktadır Üniversite paydaşları olan Öğrenci, Akademik ve İdari personelin talep, istek ve şikayetlerini bildirebilecekleri bir yapı mevcuttur. Bu talepler Bilgi Yönetim Sistemi olan BT Hizmet Yönetimi (ITSM) uygulaması**[1_OD4]**, MEBİS arabirimi **[2_OD4]**, Mobil uygulama **[3_OD4]**, birimlere ait destek e-posta adresleri ve çağrı merkezi telefonu üzerinden iletilebilmektedir. Bildirilen istek veya arıza talepleri ilgili birimlere direk olarak aktarılmakta, verilen cevaplar ve sunulan çözümler kayıt altına alınmaktadır. Alınan raporlarla verilen destek hizmetleri takip edilmekte ve iyileştirme yapılabilecek noktaların tespiti için birimlerde incelenmektedir.

Olgunluk Düzeyi (4) Paydaş katılım mekanizmalarının işleyişi izlenmekte ve bağlı iyileştirmeler gerçekleştirilmektedir.

[1](4) A.4.1 mail_talep

[2](4) A.4.1 mebis_talep

[3](4) A.4.1 mobil_talep

EĞİTİM VE ÖĞRETİM

B.3. Öğrenme Kaynakları ve Akademik Destek Hizmetleri

B.3.3.Tesis ve Altyapılar

Bulut Veri Depolama Projesi İnternet üzerinden erişilebilen ve çeşitli veri depolama hizmetlerini sunan bir projedir. Bu proje, kullanıcıların verilerini güvenli bir şekilde saklamalarını, yedeklemelerini ve paylaşmalarını sağlar. Büyük bulut veri depolama sağlayıcıları genellikle sunucu altyapısını yönetir ve kullanıcılara geniş depolama alanı ve diğer ilgili hizmetleri sunar. Bulut Veri Depolama ile dosya paylaşımlarını web arayüzünden yapılabilmesi hedeflenmiştir. "cloud.ankaramedipol.edu.tr" web arayüzü üzerinden dosya paylaşımlarını gerçekleştirmeyi hedefleyen “Bulut Veri Depolama Projesi” için bir güncelleme yayınlandı. Güncelleme, smb1.0 güvenlik protokolü kapatılmış ve daha güvenli olan smb2.0 ve 3.0'ı etkinleştirmiştir. Bu güncelleme süreci Linux arayüzü kullanılarak gerçekleştirilmiştir **[1_OD2].**

Trend Micro Deep Security Sunucu Güvenliği Projesi Sunucu Güvenliği Projesi, sunuculara kullanım amacı dışında erişimlerin kısıtlanması, güvenlik açıklarının kapatılması ve zararlı yazılımların tespit edilerek en hızlı şekilde engellenmesi gibi hedefleri kapsamaktadır. Bilgi güvenliği açısından kritik olan sunucularının güvenliğini sağlamak ve bu sunucuların düzgün çalışmasını ve verimliliğini korumak için önemlidir.Deep Security'de yeni güçlü kurallar

oluşturuldu ve bunların ilk canlı testleri “Pusula SaaS” sunucularında gerçekleştirildi. Bu kurallar Linux ve Windows işletim sistemleri için ayrı ayrı oluşturuldu ve gerçek zamanlı tarama ve manuel tarama planları belirlendi. Sonrasında kurum içinde bulunan tüm sunucular için aynı kurallar sunucuların kullanım amacına göre oluşturuldu **[2_OD4].**

Zabbix Sistemi İzleme Projesi Geçen yılki BİDR raporunda belirtilen şekilde kullanımına devam edilmektedir.Ekstra oluşan hataları görüntüleyebilmek için MEBİS sunucularında IIS hata logları zabbix entegrasyonu ile kontrolü sağlanmaktadır **[3_OD4].**

Trend Micro Apex One Son Kullanıcı Bilgisayarı Güvenliği Projesi “Apex One” son kullanıcı bilgisayarı güvenliği projesi ile kullanım amacı dışında erişimlerin kısıtlanması, güvenlik açıklarının kapatılması ve zararlı yazılımların tespit edilerek en hızlı şekilde engellenmesi gibi hedefleri kapsamaktadır. Apex One ile bilgisayarlara yüklenen antivirüs yazılımları yönetilmektedir. Apex Central ile birden fazla Apex One sunucusu yönetilmektedir. Apex Central üzerinde yazılan tüm kurallar Apex One aracılığıyla bağlı olan tüm bilgisayarlara uygulanır. “Apex One” ve “Apex Central” sunucuları yenilenmiştir. Bu sunucular için yeni sanal ağ (Vlan) oluşturulmuştur. Bu sunucuların databaselerini güvenlik nedeniyle farklı bir yeni sanal ağa (Vlan) konumlandırılmıştır. Bu sayede üniversite içerisinde bulunan bütün kullanıcı bilgisayarlarındaki Apex One ajanları güncellenmiştir. Her haftanın ilk günü kullanıcı bilgisayarlarındaki Apex One ajanları otomatik olarak taranarak eski versiyonları güncellenmektedir **[4_OD4] [5_OD4].**

Kaynak Planlama Uygulaması Veri Tabanı Yenileme Projesi Kalite süreçlerimiz kapsamında belirlenen hedefler doğrultusunda, Kaynak Planlama Uygulaması Veri Tabanı Yenileme Projesi ile önemli adımlar atılmıştır. Proje kapsamında, kaynak planlama uygulamasının veri tabanının sürekli ve kesintisiz erişilebilir olması hedeflenmiştir. Bu doğrultuda, Sürekli Erişilebilirlik; MEBİS uygulamasına ait veri tabanı, “Always On” prensibi çerçevesinde kesintisiz çalışabilir hale getirilmiştir. Yüksek Erişilebilirlik Altyapısı; Tek sunucu yapısından çıkarak, aynı anda iki veya daha fazla sunucunun çalıştığı sistem mimarisi oluşturulmuştur. Böylece, birincil sunucuda yaşanabilecek herhangi bir problem durumunda, tüm veri tabanlarının erişimi otomatik olarak ikincil sunucuya devredilerek veri kaybı engellenmiş ve hizmet sürekliliği sağlanmıştır.Bu düzenlemeler, kalite hedeflerimizle uyumlu olarak veri tabanı erişilebilirliğini artırmış, sistem güvenilirliğini ve iş sürekliliğini temin etmiştir **[6_OD4].**

Geçen yıl, web sitesi veri tabanı sunucusunda yapılan güncellemeler ve değişiklikler sırasında web sitelerinin erişilebilirliğinin kesintisiz olmasını hedeflemiştik. Bu doğrultuda, kurum içi web siteleri için kesintisiz çalışabilirlik ve sürekli erişilebilirlik sağlamak amacıyla veri tabanı kurulumu yapılmıştır. Tek bir sunucu yapısından çıkılarak, aynı anda çalışan iki veya daha fazla sunucunun çalışabilirliği sağlanmıştır. Birincil sunucuda bir problem yaşanması durumunda, tüm veri tabanlarının erişimi ikincil sunucuya otomatik olarak taşınmakta ve veri kaybı önlenerek devamlılık sağlanmaktadır.2024 yılı itibariyle, yapılan geçiş süreci tamamlanmış olup, senkronizasyonun sağlanamayan kısmı üzerinde detaylı çalışmalar yapılmıştır. Mevcut sistemdeki senkronizasyon problemleri giderilmiş ve veri bütünlüğü tam olarak sağlanmıştır. Bu düzenlemelerle birlikte, güncellemeler sırasında daima kesintisiz erişilebilirlik hedefi güvence altına alınmıştır

[7_OD3].

2024 yılı itibariyle, Veeam yedekleme yenileme projesi kapsamında sunucu yedeklemelerinin günlük olarak alınması hedeflenmiş ve sistem yönetimi ekibi tarafından sunucunun aktif hale getirilememesi durumunda en hızlı şekilde sunucuların yedekten kurtarılması sağlanmıştır. Proje ile birlikte, sunucu yedekleri ana sistemden bağımsız olarak ayrı bir veri depolama alanına taşınmış ve böylece sistemde oluşabilecek sorunlar yedekleme sunucusunu etkilemeyecek şekilde yapılandırılmıştır. Veeam yedekleme yenileme projesi doğrultusunda, tüm sunucuların yedekleme süreleri arttırılmış, proxy sunucular oluşturularak yük dağılımı sağlanmıştır. Bu sayede yedekleme performansı artırılmış ve süreçlerin hızı optimize edilmiştir. Ayrıca, yedeklerin ana sistemden bağımsız veri depolama alanlarına taşınarak, sistem sorunlarından etkilenmesi engellenmiştir. Sunucu yedeklemeleri günlük olarak alınmakta ve sistem yönetimi ekibi tarafından sunucu aktif hale getirilememesi durumunda, yedekten hızlı bir şekilde kurtarma işlemi yapılmaktadır **[8_OD3].**

Veeam Yedekleme Bulut Depolama Projesi Veeam S3 Yedekleme sayesinde, kurum içinde kritik olan uygulama verileri ve veri tabanı yedekleri, kurum veri merkezinden bağımsız bir şekilde ayrı bir veri merkezinde tutularak, mevcut yedekleme veri deposu erişilemez olsa dahi kritik verilerin yedeklenmesi hedeflenmiştir. Haftalık olarak yedekleme yapılarak felaket kurtarma senaryosuna dahil edilmiştir **[9_OD3].**

İnternet Hızı Arttırımı; Ankara Medipol Üniversitesi 300 Mbps internet hızı, Superonline firması tarafından sağlanan anlaşma iptal edildi. Yeni yapılan anlaşmaya göre, Türknet firması tarafından sağlanan 1 Gbps ve Türktelekom firması tarafından sağlanan 400 Mbps internet hizmeti ile birlikte kampüste toplamda 1.4 Gbps internet hızı sağlanmaktadır. İnternet çıkışları bu hatlar üzerinden sağlanarak, kullanıcı başına düşen hız kapasitesi artırılmıştır **[10_OD3].**

2024 yılı itibariyle, internet erişim noktalarının (Access Point) sayısının arttırılması ve yeniden konumlandırılması hedeflenmiş olup, bu çalışmalar tamamlanmış ve devam etmektedir. Sınıflar için eğitim-öğretimin interaktif işlemesi amacıyla AP altyapısı ve konumlandırmaları yapılmış ve yapılmaya devam etmektedir. Kız Öğrenci Yurdu WiFi Güçlendirme Projesi kapsamında, 15 katta bulunan toplam 398 odanın etkili bir şekilde WiFi kullanabilmesi için projede belirlenen noktalara AP cihazları (Access Point) yerleştirilmiştir. Bu çalışma ile birlikte, kız öğrenci yurdundaki toplam AP cihazı sayısı 80'e çıkarılarak, WiFi hizmeti ve kalitesi artırılmıştır. Erkek Öğrenci Yurdu WiFi Güçlendirme Projesi kapsamında ise, 4 katta bulunan toplam 120 odanın etkili bir şekilde WiFi kullanabilmesi için projede belirlenen noktalara AP cihazları (Access Point) yerleştirilmiştir. Bu çalışma ile erkek öğrenci yurdundaki toplam AP cihazı sayısı 19'a çıkarılarak, WiFi hizmeti ve kalitesi artırılmıştır **[11_OD4] [12_OD4].**

Personel Takip Sistemi (PDKS) Çalışanların işyerine giriş /çıkışlarının yetkilendirilmesini, çalışma, fazla mesai, devamsızlık, izin, istirahat sürelerinin izlenmesini ve hesaplanmasını sağlar. Kurum içerisinde belirli lokasyonlarda kullanılan İnsoft Pro PDKS yazılımı kurumun üniversite ve Suam Yerleşkeleri içerisine dahil edilmesi hedeflenmiştir. Bu proje kapsamında hedefimiz yemekhane ve cafeteryaların merkezi tek bir noktadan kontrolünün sağlanmasıdır.

Verileri yedeklemek için Microsoft SQL veritabanı kullanılmaktadır. Veritabanında bütünüyle ilişkili tablolar ve obje merkezli tasarım yapılmıştır. Tüm modüller tek bir veri tabanı içinde tutulmaktadır. Hepsi birbiri ile entegre çalışmaktadırlar. Böylelikle teknik problemlerin daha az yaşanması ile ilgili önlemler alınmış olacaktır **[13_OD2].**

2024 yılı itibariyle, Domain ortamında bulunan sunucuların iç güvenlik duvarı, DeepSecurity aracılığıyla aktif edilerek güvenlik önlemleri güçlendirilmiştir. Bu güvenlik çalışması ile özellikle Domain Controller sunucularında yapılan güvenlik önlemleri, her bir bilgisayar veya servis grubu özelinde toplu olarak güncellenen policy kurallarıyla sağlanmaktadır.

Yerel güvenlik duvarının kullanım amacı, dışarıdan erişim sağlayan bağlantılar için filtreleme yaparak yalnızca izin verilen kurallar doğrultusunda bağlantıya izin vermektir. Örneğin, web sunucusu erişimine yönelik hazırlanan kurallarla, sadece web portlarına (80-443) bağlantı izni verilmektedir. Ayrıca, sunucuların kullanım amacı doğrultusunda, policy kurallarından bağımsız olarak DeepSecurity üzerinde sunuculara tekil olarak farklı güvenlik duvarı kuralları eklenmiştir **[14_OD2].**

Önceden, yapılan DNS sorguları kurumun dış IP adresine yönlendirilmekteydi. Ancak, 2024 yılı itibariyle, bu sorgular Cloudflare WAF üzerine taşınarak IP gizlemesi yapılmış ve web uygulamalarına yönelik saldırılara karşı güvenlik artırılmıştır. Bu çalışma her yıl üzerine eklemeler yapılarak sürekli güncellenmeye devam etmektedir **[15_OD4].**

mebis.ankaramedipol.edu.tr adresi, öğrenci ve personellerin kayıt, ders, not, izin gibi kurumsal bilgi sistemlerine erişim sağladığı ve bu bilgileri düzenlediği ana web sayfasıdır. Kurumun öğrenci ve çalışanları tarafından en fazla erişilen web sayfası olduğundan, kesintisiz ve sağlıklı erişim altyapısı için alınan önlemlerden biridir. Kanıt içerisinde paylaşılan görselde, mebis.ankaramedipol.edu.tr adresi ziyaret edildiğinde, ilk olarak karşılaşılan Load Balancing servisi Cloudflare'da yapılandırılmıştır. Kurumumuza gelen iki ayrı internet sağlayıcısı üzerinden sağlanan bu yapı ile, yoğunluk veya kesinti durumunda diğer hattın devreye girmesiyle kesintisizlik sağlanmıştır. Belirtilen iki internet hattı için, her birine ait NAT IP (Sunucunun tüm dünyadan erişilebilmesini sağlayan dış IP adresi) tanımlanmış olup, bu yapı sayesinde kesintisiz internet erişimi ve güvenlik önlemleri desteklenmiştir **[16_OD4].**

2024 yılı itibariyle, Firewall değişim projesi başarıyla tamamlanmıştır. Bu kapsamda, firewall cihaz sayısı birden ikiye çıkarılmış ve daha yüksek kapasiteli cihazlar seçilmiştir. Mevcutta kullanılan FortiGate 500E cihazı yerine, iki adet FortiGate 600E cihazı konumlandırılmıştır. Bu değişikliğin amacı, ana firewall cihazının herhangi bir arıza veya hata durumunda ağ iletişim trafiğinin ikinci firewall cihazı üzerinden devam etmesini sağlamak (High Availability - HA) ve böylece kesintisiz güvenlik sağlamaktır. Bu proje ile birlikte, ağ güvenliği daha güçlü hale getirilmiş ve daha sağlam bir altyapı oluşturulmuştur. 2025 yılı için, Firewall cihazlarının lisansları 3 yıllık olarak yenilenecek ve aynı cihazlarla devam edilecektir. Yenilenen lisans ile birlikte, güvenlik kuralları daha kapsamlı hale getirilecek ve ağ trafiği FortiAnalyzer ile kayıt altına alınarak izlenebilirlik artırılacaktır **[17_OD4].**

2024 yılı itibariyle, Merkezi Log Yönetimi (SIEM) çözümü, başlangıçta Seccops Siber Güvenlik Teknolojileri firması tarafından sağlanırken, 2024 yılının son çeyreğinde NSC firmasından danışmanlık alınmaya karar verilmiştir. Ayrıca, daha önce kullanılan CryptoSim yerine Wazuh kullanılmaya başlanmıştır.Wazuh, açık kaynaklı bir uygulama olarak, DNS, uygulama, güvenlik ve web servislerinin log dosyalarını merkezi olarak toplar ve bu logları imzalayarak kayıt altına alır. Toplanan loglar, tespit edilen zafiyetler ve bulguların geçmişe

dönük incelemelerini sağlar ve alınacak önlemler ve gereksinimler konusunda önemli referanslar sunar. Ayrıca, güvenlik duvarı üzerinden geçen veri trafiği de kayıt altına alınmaktadır.Wazuh ile yazılan kurallar sayesinde, iç ağımızda bulunan bilgisayarların dış dünya ile olan trafiği izlenmektedir. Engellenmiş dış adresler ile trafik tespiti yapılabilmektedir. Ayrıca, iç ağda korelasyon olayları tespit edilerek müdahaleler gerçekleştirilmektedir **[18_OD3] [19_OD3] [20_OD3] [21_OD3] [22_OD3] [23_OD3].**

Mail hesapları lisans optimizasyonu Üniversitemiz ile ilişiği kesilen ve Active Directory hesapları kapatılmış olan Akademik ve İdari personelin kullanmış olduğu ücretli Office365 lisans gruplarından kaldırılması otomasyonu planlanmıştır. Bu otomasyon kapsamında ilişiği kesilen personelin lisans yetkileri kaldırılmakta olup lisans ücreti istemeyen Office365 A1 lisansı verilmektedir. Word, Excel ve benzeri Office uygulamalarını kullanmayan geçici görevlendirme ile çalışan akademik personel, ücretli Office365 lisans gruplarından çıkartılarak lisans ücreti gerektirmeyen Office365 A1 lisansı verilecektir.

Office365 MFA (Çok faktörlü kimlik doğrulama) projesi Üniversitemizde bulunan öğrenci, akademisyen ve diğer personellerin Office365 sistemlerine girişlerinde çok faktörlü kimlik doğrulaması zorunlu hale getirilmiştir. Bu yöntemle kullanıcıların hesapları güvenlik altına alınmıştır **[24_OD4].**

Single Sign-on Projesi Öğrenci, akademisyen ve personelin kullanmış oldukları MEBIS sistemine girişlerde Active Directory ve Office365 entegrasyonu yapılarak kullanıcıların tek kullanıcı ve şifre ile üniversite kaynaklarına erişimi sağlanmış ve hesap güvenlikleri artırılmıştır **[25_OD4].**

SD-WAN (Yazılım Tabanlı Geniş Alan Ağı) Projesi Bu proje kapsamında Türk Telekom ve Superonline internet erişim hatları yedeklenerek hatlardan bir tanesine erişimin kesilmesi halinde kurum internet erişimi diğer operatör üzerinden sağlanmaktadır **[26_OD4].**

Olgunluk Düzeyi (4) Tesis ve altyapının kullanımı izlenmekte ve ihtiyaçlar doğrultusunda iyileştirilmektedir.

[1](2) B.3.3bulut_veri_depolama_projesi

[2](4) B.3.3trend_micro_deep_security_sunucu_guvenligi_projesi

[3](4) B.3.3zabbix_sistem_izleme_projesi

[4](4) B 3.3trend_micro_apex_one_son_kullanici_bilgisayarı_guvenligi projesi.

[5](4) B.3.3trend_micro_apex_one_son_kullanıcı_bilgisayarı_guvenligi_projesi

[6](4) B.3.3kaynak_planlama_uygulaması_veri_tabanı_yenileme_projesi

[7](3) B.3.3web_sitesi_veri_tabani_yenileme_projesi

[8](3) B.3.3veeam_yedekleme_yenileme_projesi

[9](3) B.3.3veeam_yedekleme_bulut_depolama_projesi

[10](3) B.3.3(i. internet_hızı_artirimi)

[11](4) B.3.310-1

[12](4) B.3.310-2

[13](2) B.3.3personel_takip_sistemi_(pdks)

[14](2) B.3.3(c. deepsec)

(15)(4) B.3.3internete_acik_olan_sistemlerin_waf_uzerinden_calistirilmasi

[16](4) B.3.3cloudflare_load_balance

[17](4) B.3.3(g. universite_firewall_degisim_projesi)

[18](3) B.3.3siem

[19](3) B.3.3siem

[20](3) B.3.3siem

[21](3) B.3.3siem

[22](3) B.3.3siem

[23](3) B.3.3siem

[24](4) B.3.3(k. office365_mfa_(cok_faktorlu_kimlik_dogrulama_projesi)

[25](4) B.3.3(l.single_sign-on_projesi)

[26](4) B.3.3(m. sdwan_(yazilim_tabanli_genis_alan_agi_projesi)

B.3.4. Dezavantajlı gruplar

MEBIS EqualWeb Eklentisi; EqualWeb eklentisi, öğrenci bilgi sistemimize entegre edilerek engelsiz üniversite uygulamalarında önemli geliştirmeler sağlmaktadır. Bu eklenti sayesinde, öğrencilerimizin çeşitli engel durumlarına uygun olarak öğrenim kaynaklarına erişimleri kolaylaşmış, çevrim içi içeriklere daha rahat ulaşabilmeleri sağlanmaktadır. EqualWeb'in ekran okuma teknolojileri ve renk kontrastı iyileştirmeleri, görme veya işitme engeli olan öğrencilerin eğitim materyallerine daha etkili bir şekilde erişimini mümkün kılarak eğitimde eşitlik ve erişilebilirlik standartlarını yükseltmektedir. Bu sayede, öğrencilerimizin öğrenme deneyimi daha kapsayıcı ve engelsiz bir şekilde optimize hale gelmektedir.[OD3]

Olgunluk Düzeyi (3) Dezavantajlı grupların eğitim olanaklarına erişimine ilişkin uygulamalar yürütülmektedir.