

**BANDIRMA ONYEDİ EYLÜL ÜNİVERSİTESİ**

**KANUN VE STANDARTLARA UYUM SÜREÇLERİ**

**1. YÖNETİCİ ÖZETİ**

Bu rapor, Bandırma Onyedi Eylül Üniversitesi bünyesinde stratejik bir vizyonla gerçekleştirilen; İç ve Dış Sızma Testleri, ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi (BGYS) Kurulumu, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (DDO) Bilgi ve İletişim Güvenliği Rehberi Uyumu, KVKK Teknik ve Hukuki Uyum Çalışmaları ve Bilgi Güvenliği Farkındalık Eğitimleri süreçlerinin bütüncül bir analizini ve paydaş bazlı fayda dökümünü sunmak amacıyla hazırlanmıştır.

Tamamlanan projeler, üniversitemizin dijital altyapısını reaktif bir savunma anlayışından proaktif bir koruma modeline geçirmiş; siber güvenliğini artırmış, ulusal ve uluslararası standartlara tam uyumunu sağlamış ve en mühim kriterlerimizden olan kurumsal ve kişisel verileri güvence altına almıştır. Her bir hizmetin; kurumumuza operasyonel verimlilik, finansal koruma ve itibar yönetimi açılarından, bağlı olduğumuz üst kurumlara hesap verebilirlik ve ulusal stratejiye uyum konularında, hizmet verdiğimiz öğrencilerimize ve diğer paydaşlarımıza veri mahremiyeti ve hizmet sürekliliği bağlamında ve bu sistemleri yürüten değerli personellerimize güvenli çalışma ortamı ve yetkinlik artışı durumlarından sağladığı stratejik faydalar bulunmaktadır. Aşağıda ilgili yararları detayları ile birlikte verilmiştir.

Yapılan çalışmaların tamamı, kurumumuzun dijital çağdaki itibarını ve dijital döneme uyumunu, güvenilirliğini ve sürdürülebilirliğini pekiştiren temel yapı taşları olup, gelecekteki teknolojik yatırımlar ve akademik girişimler için sağlam bir zemin oluşturmaktadır.

# 2. Bilgi Güvenliği ve Uyum Çalışmalarının Sağladığı Faydalar

## 2.1. İç ve Dış Sızma Testi ve Raporlaması

Süreç Tanımı:

Sızma testi (penetrasyon testi), üniversitemizin bilişim altyapısına (sunucular, ağ cihazları, web uygulamaları, öğrenci bilgi sistemi vb.) yönelik potansiyel siber saldırıların, "etik hacker" olarak bilinen yetkili güvenlik uzmanları tarafından kontrollü bir şekilde simüle edilmesidir. İç sızma testi, kurum ağının içinden bir personelin veya yetkisiz bir misafirin verebileceği zararları; dış sızma testi ise internet üzerinden gelebilecek saldırıları öngörmeyi hedeflemektedir. Süreç sonunda tespit edilen tüm zafiyetler, risk seviyelerine göre sınıflandırılarak detaylı çözüm önerileriyle birlikte bir rapor halinde sunulmuştur.

**Üniversite (Kurum) İçin Faydaları:**

**Stratejik Risk Tespiti:** Sadece teorik riskler değil, saldırganlar tarafından fiilen istismar edilebilecek zafiyetler (örn: güncellenmemiş bir sunucu yazılımı, web sitesindeki bir kodlama hatası, zayıf parola politikası) somut olarak ortaya konulmuştur. Bu sayede, bilişim altyapımızın en zayıf halkaları net bir şekilde görülmüştür.

**Yatırım Önceliklendirme:** Raporlanan zafiyetlerin kritiklik seviyeleri (Yüksek, Orta, Düşük), sınırlı olan siber güvenlik bütçesinin ve insan kaynağının en acil ve en riskli alanlara yönlendirilmesini sağlamıştır.

**Finansal ve Operasyonel Koruma:** Olası bir fidye yazılımı (ransomware) saldırısı sonucu sistemlerin kilitlenmesi, öğrenci verilerinin sızdırılması veya web sitesinin hizmet dışı kalması gibi senaryoların önüne geçilerek, hem ciddi maddi kayıplar hem de eğitim-öğretim faaliyetlerinde yaşanabilecek kesintiler engellenmiştir.

**İtibar Yönetimi:** Bir veri sızıntısının ulusal basına yansıması durumunda kurumun uğrayacağı prestij kaybı, öğrenci ve veli nezdinde yaşanacak güven erozyonu proaktif olarak önlenmiştir.

**Üst Kurumlar (YÖK, DDO, Sayıştay vb.) İçin Faydaları:**

**Denetim ve Uyumluluk Kanıtı:** Özellikle DDO Güvenlik Rehberi ve diğer kamu bilişim standartları, düzenli güvenlik testlerini zorunlu kılmaktadır. Yapılan bu testler, denetimlerde sunulabilecek somut bir uyumluluk kanıtı niteliğindedir.

**Hesap Verebilirlik:** Kamu kaynakları ile kurulan dijital altyapının güvenliğini sağlamak adına gerekli özenin gösterildiği ve proaktif tedbirlerin alındığı ispatlanmıştır. Bu, kurumun şeffaflık ve sorumluluk ilkelerine bağlılığını gösterir.

**Öğrenciler ve Diğer Paydaşlar İçin Faydaları:**

**Kişisel Veri Mahremiyeti:** Öğrencilerin T.C. kimlik numaraları, adresleri, notları, transkriptleri gibi hassas verilerinin kötü niyetli kişilerin eline geçmesi engellenmiştir.

**Güvenli ve Kesintisiz Hizmet:** Öğrenci Bilgi Sistemi, uzaktan eğitim platformları, e-posta hizmetleri gibi kritik servislerin siber saldırılarla kesintiye uğramasının önüne geçilmiş, öğrencilerin mağduriyet yaşaması engellenmiştir.

**Çalışanlar İçin Faydaları:**

**Güvenli Çalışma Ortamı:** Akademik ve idari personelin, çalışmalarını yürüttükleri dijital platformların güvenli olduğunu bilmesi, iş verimliliğini ve motivasyonunu artırır. Personelin kişisel verileri ve akademik çalışmalarının (makaleler, araştırma verileri vb.) bütünlüğü ve gizliliği korunmuştur.

**Sistem Güvenilirliği:** Günlük iş akışlarının siber saldırı kaynaklı teknik arızalar veya veri kayıpları nedeniyle aksamasının önüne geçilmiştir.

### Siber güvenlik süreçlerinin devreye alınmasının getireceği faydalar özet olarak ifade edilirse;

1. Kurumsal bilişim altyapısındaki zafiyetlerin belirlenmesi.
2. Güvenlik açıklarının giderilmesiyle prestij ve güvenilirliğin artması.
3. Olası siber saldırılara karşı hazırlıklı olunması.
4. Kurumun bilgi güvenliği olgunluk seviyesinin yükseltilmesi.
5. Mevzuat ve üst politika belgelerine uyum sağlanması.
6. Akademik verilerin (notlar, belgeler vb.) güvenliğinin artırılması.
7. Kişisel bilgilerin kötüye kullanım riskinin azaltılması.
8. Kurumsal verilerin korunması.
9. Siber saldırılara karşı bireysel farkındalığın artması.

## 2.2. ISO27001 BGYS 2022 Uyum Danışmanlığı ve Belgelendirme

Süreç Tanımı: ISO 27001:2022, bir kurumun bilgi varlıklarını korumak için kurması, işletmesi, izlemesi ve sürekli iyileştirmesi gereken bir Bilgi Güvenliği Yönetim Sistemi'nin (BGYS) gerekliliklerini tanımlayan uluslararası bir standarttır. Bu süreçte, üniversitenin tüm bilgi varlıkları envanteri çıkarılmış, risk analizleri yapılmış, güvenlik politikaları ve prosedürleri oluşturulmuş (örn: Parola Politikası, Temiz Masa Politikası, Erişim Kontrol Prosedürü vb.) ve tüm bu sistemin işlerliği bağımsız bir denetim kuruluşu (TURKAK akreditasyonlu) tarafından denetlenerek belgelendirilmiştir.

**Üniversite (Kurum) İçin Faydaları:**

**Kurumsallaşma ve Sürdürülebilirlik:** Bilgi güvenliği, kişilerin veya departmanların anlık çabalarına bağlı olmaktan çıkarak, tanımlanmış rol ve sorumluluklara, politikalara ve prosedürlere dayalı, kurumsal hafızası olan sürdürülebilir bir yapıya kavuşmuştur.

**Risk Odaklı Yaklaşım:** Kurum, tüm bilgi varlıklarına yönelik tehdit ve zafiyetleri sistematik olarak değerlendirerek, kabul edilemez seviyedeki riskler için kontroller (tedbirler) uygulamaya başlamıştır. Bu, "her şeye aynı anda" müdahale etmek yerine, en önemliyi koruma prensibini benimsetir.

**Uluslararası Geçerlilik ve Prestij:** ISO 27001 sertifikası, üniversitemizin uluslararası projelerde (Erasmus+, Horizon Europe vb.) ve yabancı üniversitelerle yapılacak iş birliklerinde veri güvenliği konusunda güvenilir bir ortak olduğunu gösteren bir kalite belgesidir.

**Süreç Verimliliği:** BGYS kurulumu sırasında iş süreçleri güvenlik perspektifiyle yeniden gözden geçirilmiş, bu da gereksiz veri toplama, yetkisiz erişim gibi verimsizliklerin ortadan kaldırılmasına yardımcı olmuştur.

**Üst Kurumlar İçin Faydaları:**

**Standartlaşma ve Karşılaştırılabilirlik:** Üniversitenin bilgi güvenliği olgunluk seviyesinin, uluslararası kabul görmüş bir standart üzerinden ölçülebilir ve diğer kurumlarla karşılaştırılabilir hale gelmesini sağlar.

**Güvence Mekanizması:** Üst kurumlar için, bağlı kuruluşun bilgi güvenliğini tesadüflere bırakmadığını, kanıtlanmış bir yönetim sistemi çerçevesinde ele aldığını bilmek önemli bir güvencedir.

**Öğrenciler ve Diğer Paydaşlar İçin Faydaları:**

**Sistematik Güvence:** Verilerinin anlık değil, sürekli izlenen, denetlenen ve iyileştirilen bir sistem tarafından korunduğuna dair en üst düzeyde güvenceye sahip olurlar. Bu, üniversiteye olan bağlılığı ve güveni artırır.

**Çalışanlar İçin Faydaları:**

**Rol ve Sorumlulukların Netleşmesi:** "Veri Sahibi", "Veri Sorumlusu", "Sistem Yöneticisi" gibi rollerin ve bu rollerin bilgi güvenliği sorumluluklarının netleşmesi, görev karmaşasını ortadan kaldırır.

**Sürekli İyileştirme Kültürü:** "Planla-Uygula-Kontrol Et-Önlem Al" (PUKÖ) döngüsü sayesinde çalışanlar, güvenlik süreçlerinin bir parçası haline gelir ve sürekli iyileştirme kültürünü benimserler.

### ISO27001 BGYS 2022 Uyum Danışmanlığı ve Belgelendirme’nin kurumumuz adına faydaları şu şekilde özetlenebilir:

1. Uluslararası standartlara uyum sağlanması.
2. Kurumsal itibarın ve rekabet gücünün artırılması.
3. Bilgi güvenliği süreçlerinin sürdürülebilir şekilde yönetilmesi.
4. Kurumun güvenlik seviyesinin belgelenmiş ve denetlenebilir olması.
5. Ulusal ve uluslararası güvenlik beklentilerine uyum.
6. Veri güvenliği konusundaki güvenin artması.
7. Şeffaflık ve güvenilirlik algısının güçlenmesi.
8. Standart operasyonel prosedürlerle çalışılması.
9. Görev ve sorumlulukların daha net belirlenmesi.

## 2.3. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi Güvenliği Rehberi Uyum ve İç Denetim

**Süreç Tanımı:**

Bu rehber, kritik altyapı olarak kabul edilen kamu kurumlarının uyması gereken asgari güvenlik tedbirlerini içeren bir yol haritasıdır. Süreç kapsamında üniversitemizin "Varlık Grupları", "Ağ ve Sistem Güvenliği", "Uygulama ve Veri Güvenliği", "Siber Olay Yönetimi", "Fiziksel Güvenlik" gibi birçok alanda mevcut durumu analiz edilmiş, rehberin gerektirdiği tedbirlerle arasındaki farklar (GAP Analizi) ortaya konulmuş ve uyum için bir eylem planı oluşturularak hayata geçirilmiştir. İç denetim mekanizmaları kurularak uyumun sürekliliği güvence altına alınmıştır.

**Üniversite (Kurum) İçin Faydaları:**

**Zorunlu Mevzuata Tam Uyum:** Bu rehbere uyum isteğe bağlı değil, zorunludur. Sürecin tamamlanması, üniversitemizi olası yasal yaptırımlardan ve idari cezalardan tamamen koruma altına almıştır.

**Ulusal Güvenlik Standardı:** Üniversitemizin siber güvenlik olgunluk seviyesi, ülke genelinde tüm kritik kurumlar için belirlenmiş olan asgari standarda yükseltilmiştir. Bu, izole bir güvenlik anlayışından, ulusal ekosistemin bir parçası olma anlayışına geçişi simgeler.

**Entegre Siber Savunma:** Rehber, Ulusal Siber Olaylara Müdahale Merkezi (USOM) ile entegrasyonu ve siber olayların belirli bir formatta bildirimini zorunlu kılar. Bu sayede, üniversitemiz ulusal siber istihbarat ağından faydalanır ve bir saldırı anında ulusal düzeyde destek alabilir hale gelmiştir.

**Üst Kurumlar (Özellikle DDO) İçin Faydaları:**

**Ulusal Siber Güvenlik Stratejisine Katkı:** Üniversitemizin uyumu, DDO'nun "ulusal siber güvenlik seviyesini yükseltme" stratejik hedefine doğrudan hizmet eder ve bu hedefin başarıyla uygulandığının bir göstergesidir.

**Bütüncül Risk Yönetimi:** DDO, ülkenin genel siber risk haritasını çıkarırken, rehbere uyumlu kurumların varlığı, riskin yönetilebilir ve öngörülebilir olduğu alanları temsil eder.

**Öğrenciler ve Diğer Paydaşlar İçin Faydaları:**

**Devlet Eliyle Güvence:** Verilerinin ve kullandıkları dijital hizmetlerin, sadece üniversite tarafından değil, aynı zamanda devletin en üst siber güvenlik otoritesi tarafından belirlenen standartlarla korunduğunu bilmek, en üst düzeyde güvence sağlar.

**Çalışanlar İçin Faydaları:**

**Standart ve Güvenli Altyapı:** Çalışanların günlük olarak kullandığı ağ altyapısı, sunucular ve yazılımlar, belirli bir güvenlik standardına göre yapılandırıldığı için daha stabil ve güvenli çalışır. Bu, teknik sorunlarla daha az vakit kaybetmelerini sağlar.

**Ulusal Sorumluluk Bilinci:** Kamu personeli olarak, yaptıkları işin ve uydukları kuralların ulusal siber güvenliğin bir parçası olduğu bilinci pekişmiştir.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi Güvenliği Rehberi Uyum ve İç Denetim uygulamasının üniversitemize katkıları aşağıda maddeler halinde özetlenmiştir.

1. Ulusal dijital dönüşüm stratejilerine uyum.
2. Süreçlerin sürekli denetlenmesi ve iyileştirilmesi.
3. Kurumsal risklerin önceden tespit edilmesi.
4. Kamu kurumları için rehberde öngörülen standartlara uygunluk.
5. Denetlenebilir ve raporlanabilir yapının sağlanması.
6. Kamu hizmetlerinde güvenli dijital erişim imkanı.
7. Elektronik hizmetlerin güvenli sunulması.
8. Dijitalleşme süreçlerinde rehberden faydalanma.
9. Bilgi güvenliği sorumluluklarının daha net kavranması.

## 2.4. KVKK Teknik ve Hukuki Uyum Çalışmaları

Süreç Tanımı: Bu çalışma, üniversitenin tüm kişisel veri işleme faaliyetlerinin 6698 sayılı Kişisel Verilerin Korunması Kanunu'na (KVKK) uygun hale getirilmesini kapsamaktadır. Süreçte; hangi kişisel verilerin (öğrenci, personel, ziyaretçi, tedarikçi vb.) hangi amaçlarla toplandığı, nerede saklandığı, kimlerle paylaşıldığı ve ne kadar süreyle tutulduğunu gösteren bir "Kişisel Veri İşleme Envanteri" hazırlanmıştır. Bu envanter temel alınarak VERBİS'e (Veri Sorumluları Sicil Bilgi Sistemi) kayıt yapılmış; web sitesi için Aydınlatma Metinleri ve Çerez Politikası, fiziki ve dijital ortamlar için Açık Rıza metinleri, Kişisel Veri Saklama ve İmha Politikası gibi tüm hukuki dokümanlar hazırlanmıştır. Ayrıca, verilerin korunması için şifreleme, yetki matrisi, loglama gibi teknik tedbirler de hayata geçirilmiştir.

**Üniversite (Kurum) İçin Faydaları:**

**Yüksek İdari Para Cezalarından Muafiyet:** KVKK'ya aykırılık durumunda uygulanabilecek ve milyonlarca TL'yi bulabilen ceza riskleri tamamen ortadan kaldırılmıştır. Bu, kurum bütçesi için önemli bir koruma kalkanıdır.

**Hukuki Sorumlulukların Sınırlandırılması:** Veri işleme süreçlerinin hukuka uygun hale getirilmesi, olası bir veri ihlali durumunda veya bir veri sahibinin şikayeti halinde "gerekli tüm tedbirleri alan veri sorumlusu" konumunda olmamızı sağlar.

**Veri Yönetiminde Disiplin ve Şeffaflık:** "Hangi veriyi neden topluyoruz?" sorusunun cevaplanması, gereksiz veri toplamanın önüne geçmiş, veri minimizasyonu ilkesini hayata geçirmiştir. Bu, veri depolama maliyetlerini düşürür ve süreçleri sadeleştirir.

**Üst Kurumlar İçin Faydaları:**

**Yasalara Uygun Faaliyet Güvencesi:** Bağlı kurumun temel bir kanuna tam uyum içinde faaliyet gösterdiğinin bilinmesi, üst yönetim ve denetim mekanizmaları için bir güvencedir.

**Kamu Sektöründe Öncü Rol:** KVKK uyumunu eksiksiz tamamlamış bir üniversite, diğer kamu kurumlarına iyi bir örnek teşkil eder.

**Öğrenciler ve Diğer Paydaşlar İçin Faydaları:**

**Temel Hak ve Özgürlüklerin Korunması:** En temel anayasal haklardan olan "özel hayatın gizliliği" ve "kişisel verilerin korunmasını isteme hakkı" üniversitemiz tarafından güvence altına alınmıştır.

**Tam Şeffaflık ve Kontrol:** Öğrenciler, web sitesindeki aydınlatma metinleri sayesinde verilerinin akıbeti hakkında bilgi sahibi olmuş ve kanuni haklarını (verinin silinmesini isteme, düzeltilmesini isteme vb.) kullanabilecekleri mekanizmalara kavuşmuştur.

**Çalışanlar İçin Faydaları:**

**Çalışan Verilerinin Mahremiyeti:** Personelin özlük bilgilerinden performans değerlendirmelerine kadar tüm kişisel verileri de KVKK güvencesi altına alınmıştır.

**Hukuki Risklerden Korunma:** Özellikle öğrenci işleri, personel işleri gibi birimlerde çalışan personel, kişisel veri işlerken uyması gereken kuralları net bir şekilde öğrenmiş, kendilerini ve kurumu hukuki risklere atacak eylemlerden kaçınma bilinci kazanmıştır.

KVKK Teknik ve Hukuki Uyum Çalışmaları’nın önemi şu şekilde sıralanabilir:

1. Yasal yaptırımlardan korunma.
2. Kurumun sorumluluk bilincinin güçlenmesi.
3. Kurum itibarının korunması.
4. Kişisel verilerin korunması konusunda örnek bir kurum haline gelme.
5. Yasal mevzuata eksiksiz uyum.
6. Mahremiyetin korunması.
7. Kişisel verilerin kötüye kullanılmasının engellenmesi.
8. Veri işleme süreçlerinde şeffaflık.
9. Kendi kişisel verilerinin de güvence altına alınması.

## 2.5. Bilgi Güvenliği Farkındalık Eğitimi

**Süreç Tanımı:**

Bu süreç, "en zayıf halka insan" klişesini "en güçlü savunma hattı insan" anlayışına dönüştürmeyi hedefler. Tüm akademik ve idari personele yönelik olarak düzenlenen bu eğitimlerde; güçlü parola oluşturma ve yönetme, oltalama (phishing) e-postalarını tanıma, sosyal mühendislik saldırılarından korunma, güvenli internet kullanımı, mobil cihaz güvenliği ve fiziksel güvenlik (temiz masa, ekran kilitleme vb.) gibi konular, gerçek hayattan örnekler ve uygulamalı senaryolarla anlatılmıştır. Eğitimlerin etkinliği, habersiz oltalama simülasyonları ve sınavlarla ölçülmüştür.

(Bilgi İşlem Daire Başkanlığı Öğretim Görevlimiz Salih Kiraz tarafından verilen eğitim ve sunum bağlantısı:

<https://pdb.bandirma.edu.tr/Content/Web/Yuklemeler/DosyaYoneticisi/1114/files/Bilgi%20I%CC%87letis%CC%A7im%20ve%20Siber%20Gu%CC%88venlik%20Fark%C4%B1ndal%C4%B1k%20Eg%CC%86itimi.pdf>

Siber Güvenlik Farkındalık Eğitimi:

<https://bidb.bandirma.edu.tr/tr/bidb/d/SIBER-GUVENLIK-VE-BILGI-GUVENLIGI-FARKINDALIK-EGITIMI--74712>)

**Üniversite (Kurum) İçin Faydaları:**

**İnsan Kaynaklı Güvenlik İhlallerinde Ciddi Düşüş:** Teknik sistemleri aşamayan siber saldırganların en çok başvurduğu yöntem olan oltalama saldırılarına karşı personelin bilinçlenmesi, kuruma virüs veya fidye yazılımı bulaşma riskini dramatik olarak azaltmıştır.

**Güvenlik Kültürünün İnşası:** Bilgi güvenliğinin, sadece teknik bir konu olmadığı, tüm çalışanların günlük alışkanlıklarıyla doğrudan ilgili olduğu anlayışı kuruma yerleşmiştir. Bu, güvenlik politikalarına uyumu doğal bir davranış haline getirmektedir. Üniversitemizde Bilgi İşlem Daire Başkanlığı tarafından gerçekleştirilen her işlemde personelimiz siber güvenlik, ağ ve bağlantı güvenliği ve iş güvenliği uyarınca kontrollerini ve çalışmalarını yapmaktadır.

**Yatırımın Geri Dönüşünü (ROI) Artırma:** Milyonlarca liralık güvenlik yazılımları ve cihazları, bilinçsiz bir çalışanın oltalama e-postasındaki bir linke tıklamasıyla etkisiz hale gelebilir. Farkındalık eğitimi, bu teknik yatırımların etkinliğini koruyarak yatırımın geri dönüşünü maksimize eder.

**Üst Kurumlar İçin Faydaları:**

**Bilinçli ve Yetkin Kamu Personeli:** Ülke genelinde dijitalleşen kamu hizmetlerinin güvenliği, bu hizmetleri yürüten personelin farkındalık seviyesiyle doğru orantılıdır. Eğitimli personel, ulusal siber güvenlik yetkinliğine doğrudan katkı sağlar.

**Öğrenciler ve Diğer Paydaşlar İçin Faydaları:**

**Dolaylı ama Etkili Koruma:** Öğrencilerin verilerini işleyen, onlarla e-posta yoluyla iletişim kuran personelin bilinçli olması, dolaylı olarak öğrencilerin verilerinin ve dijital iletişimlerinin de güvende olması anlamına gelir. Yanlışlıkla bir öğrenci listesinin herkese gönderilmesi gibi insan hatalarının önüne geçilir.

**Çalışanlar İçin Faydaları:**

**Kişisel Hayatta Dijital Koruma:** Eğitimde öğrenilen bilgiler (güçlü parola, sahte siteleri anlama, sosyal medya gizliliği vb.), personelin sadece kurumsal hesaplarını değil, kendi kişisel e-posta, sosyal medya ve bankacılık hesaplarını da korumasına yardımcı olur. Bu, çalışanlara verilen değerli bir kişisel gelişim katkısıdır.

(Personelimiz tarafından gerçekleştirilen Bilgi Güvenliği Farkındalık Eğitimi bünyesinde bir modül Sosyal Medya Gizliliğine ayrılmıştır.

Bilgi İşlem Daire Başkanlığı Öğretim Görevlimiz Salih Kiraz tarafından verilen eğitim ve sunum bağlantısı:

<https://pdb.bandirma.edu.tr/Content/Web/Yuklemeler/DosyaYoneticisi/1114/files/Bilgi%20I%CC%87letis%CC%A7im%20ve%20Siber%20Gu%CC%88venlik%20Fark%C4%B1ndal%C4%B1k%20Eg%CC%86itimi.pdf>

Siber Güvenlik Farkındalık Eğitimi:

<https://bidb.bandirma.edu.tr/tr/bidb/d/SIBER-GUVENLIK-VE-BILGI-GUVENLIGI-FARKINDALIK-EGITIMI--74712>)

**Özgüven Artışı ve Stres Azalması:** Şüpheli bir e-posta veya durumla karşılaştığında ne yapacağını bilmek, personelin teknolojiye karşı duyduğu stresi azaltır ve kendine güvenini artırır.

## Bilgi Güvenliği Farkındalık Eğitimi’nin sağladığı avantajlar ve fırsatlar özetle;

1. Çalışanların güvenlik farkındalığının artması.
2. Olay sayılarının azalması.
3. Siber güvenlik kültürünün kurumsallaşması.
4. Kamu güvenliği hedefleri ile uyumlu kültürel dönüşüm.
5. Sürdürülebilir bilgi güvenliği yaklaşımı.
6. Sosyal mühendislik saldırılarına karşı korunma. (Dezenformasyonla mücadele adına Daire Başkanlığımız sitesinden duyurular yayınlanmaktadır.

<https://bidb.bandirma.edu.tr/tr/bidb/d/Universitemiz-Personeline-Yonelik-Kisisel-Verilerin-Korunmasi-Kanunu-Farkindalik-Egitimi-Duzenleniyor-18739> ve <https://bidb.bandirma.edu.tr/tr/bidb/d/Elektronik-Sertifika-Sorgulama-E-Imza-63644>

)

1. Siber güvenlik bilincinin yaygınlaşması.
2. Kendi kişisel ve kurumsal bilgilerini koruma alışkanlığı kazanma.
3. Siber olaylara karşı daha dirençli hale gelme.

**3. GENEL SONUÇ VE STRATEJİK DEĞERLENDİRME**

Yukarıda detaylandırılan beş temel proje, bir bütün olarak ele alındığında, Bandırma Onyedi Eylül Üniversitesi'nin dijital varlıklarını koruma, yasal yükümlülüklere uyum sağlama ve tüm paydaşlarına güvenilir bir dijital ekosistem sunma konusundaki bütüncül ve stratejik yaklaşımını ortaya koymaktadır. Bu çalışmalar;

Teknik düzeyde altyapıyı güçlendirmiş,

Prosedürel düzeyde süreçleri ve politikaları standartlaştırmış,

Hukuki düzeyde yasal uyumu sağlamış,

Kültürel düzeyde ise insan faktörünü bir güvenlik varlığına dönüştürmüştür.

Elde edilen bu olgunluk seviyesinin korunması ve daha ileriye taşınması, bu çalışmaların tek seferlik projeler olarak görülmemesine bağlıdır. Bilgi güvenliği, sürekli bir döngüdür. Bu nedenle, sızma testlerinin periyodik olarak tekrarlanması, BGYS iç denetimlerinin aksatılmadan yapılması ve farkındalık eğitimlerinin yeni personel ile tazeleme gruplarına sürekli olarak verilmesi, kazanımların sürdürülebilirliği için elzemdir.