REVİZYON DURUMU		
No	**Revizyon Tarihi**	**Revizyon Detayı**
1	27.10.2026	İlk sürüm

1. AMAÇ

Bu politika, Orta Doğu Teknik Üniversitesi (ODTÜ), Bilgi Güvenliği Yönetim Sistemi (BGYS) kapsamında kullanıcıların, kendilerine tahsis edilen bilgi varlıklarını ve bilgi işleme olanaklarını kullanırken uymaları gereken kuralları belirlemek amacıyla hazırlanmıştır. Politika, bilgi varlıklarının gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunmasını, Üniversite itibarının ve yasal yükümlülüklerinin gözetilmesini amaçlar.

2. KAPSAM

Bu politika, ODTÜ tarafından sunulan bilgi varlıklarını ve bilgi işleme olanaklarını kullanan tüm personeli, öğrencileri ve üçüncü taraf personeli kapsar.

3. TANIMLAR VE KISALTMALAR

ODTÜ	:	Orta Doğu Teknik Üniversitesi
BGYS	:	Bilgi Güvenliği Yönetim Sistemi
BİDB	:	Bilgi İşlem Daire Başkanlığı
BGB	:	Bilgi Güvenliği Birimi
VPN	:	Virtual Private Network (Özel Sanal Ağ)
Üniversite	:	Orta Doğu Teknik Üniversitesi
Kullanıcı	:	Üniversite bilgi varlıklarına erişim yetkisi tanımlanmış gerçek kişi
Bilgi varlığı	:	Üniversite için değer taşıyan her türlü bilgi ile bu bilgiyi işleyen donanım, yazılım, hizmet ve ortamlar
Taşınabilir bellek aygıtı	:	USB bellek, harici disk, hafıza kartı, optik ortam ve benzeri taşınabilir veri depolama ortamları

4. GENEL KURALLAR

Bu politika kapsamında, Üniversite tarafından tahsis edilen bilgisayarlar ve mobil cihazlar, kurumsal ağ ve internet erişimi, kurumsal e-posta hizmeti, yazıcı, taşınabilir bellek aygıtları ile Üniversite bilgi sistemleri üzerinde işlenen tüm bilgilerin kullanıcı tarafından hangi amaçlarla kullanılacağına yönelik genel kurallar aşağıdaki gibidir:

- Üniversite tarafından tahsis edilen bilgi varlıkları esas olarak kurumsal iş süreçlerinde kullanılmalıdır.
- Kullanıcılar, erişim yetkilerini yalnızca rol ve sorumluluklarının gerektirdiği amaçlarla kullanmalıdır. Yetkisi dışındaki bilgilere erişmeye teşebbüs etmemelidir.
- Kullanıcı adı, parola ve diğer kimlik doğrulama bilgileri kişiye özeldir, hiçbir koşulda üçüncü kişilerle paylaşılmaz, yazılı veya elektronik ortamda korunmasız biçimde saklanmaz.
- Üniversitenin sağladığı bilgi varlıkları kullanılarak; yasa dışı faaliyetlerde bulunulamaz, telif hakları ihlal edilemez, taciz, hakaret veya ayrımcılık içeren iletişim yapılamaz, ticari amaçlı faaliyet yürütülemez ve siyasi propaganda yapılamaz.
- Üniversite tarafından bilgiler, sınıflandırma seviyesine uygun şekilde işlenir; yetkisiz kişilere ifşa edilmez. Görevden ayrılma hâlinde dahi gizlilik yükümlülüğü devam eder.
- Kullanıcılar, Üniversite adına sosyal medya ve kamuya açık ortamlarda yetkilendirilmedikçe açıklama yapamaz; kişisel paylaşımlarında Üniversite'ye ait gizli bilgilere yer veremez.
- Şüpheli bir durum, güvenlik ihlali veya cihaz kaybı hâlinde durum gecikmeksizin BİDB'ye ve ilgili birim yöneticisine bildirilir.
- Personel ve öğrenciler, şüphelendikleri güvenlik açıklıklarını kanıtlamaya veya test etmeye çalışmamalıdır. Açıklıkların test edilmesi sistemin kötüye kullanımı olarak yorumlanabilir, sisteme zarar verebilir, dijital kanıtları bozabilir ve testi yapan kişi bakımından hukuki sorumluluk doğurabilir.
- Üniversite bilgi varlıklarının kullanımına ilişkin kayıtlar (log), bilgi güvenliği olaylarının tespiti, araştırılması ve yasal yükümlülüklerin yerine getirilmesi amacıyla gerek görüldüğünde Bilgi İşlem Daire Başkanlığı tarafından incelenebilir. İnceleme, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve Kişisel Verileri Koruma Kurulu kararları doğrultusunda, amaçla sınırlılık ve ölçülülük ilkelerine uygun olarak, yalnızca yetkilendirilmiş personel tarafından ve kayıt altına alınarak yapılır.
- Bilgi İşlem Daire Başkanlığı, bilgi güvenliği riskinin, olayın veya bu politikaya aykırılığın tespiti hâlinde ya da hizmet sürekliliği ve yasal yükümlülükler gerektirdiğinde, önceden bildirimde

bulunmaksızın kullanıcıların Üniversite sistemlerine, hizmetlerine ve bilgi varlıklarına erişimini geçici veya kalıcı olarak sınırlayabilir, kısıtlayabilir veya sonlandırabilir. Uygulanan kısıtlamalar kayıt altına alınır ve ilgili birim yöneticisine bildirilir.

4.1. İnternet Kullanımı

Üniversite tarafından sunulan ağ üzerinden sağlanan internet erişimi, öncelikle eğitim ve araştırma faaliyetlerinin yürütülmesi ve kurumsal iş süreçlerinin desteklenmesi amacıyla sunulur. İnternet kullanımına ilişkin genel kurallar aşağıdaki gibidir:

- İnternet erişimi, güvenlik duvarı üzerinde çalışan web filtreleme çözümü ile denetlenir. Kötü amaçlı yazılım dağıtan, oltalama içeriği barındıran, zararlı yazılımların komuta ve kontrol sunucusu olarak kullanılan ve ilgili mevzuat uyarınca erişimi engellenmesi gereken sitelere erişim engellenir.
- Tarayıcı tarafından üretilen sertifika ve güvenlik uyarıları göz ardı edilerek ilgili siteye devam edilmez, güvenilir olmayan siteye ait alınan uyarılar Bilgi İşlem Daire Başkanlığı'na bildirilir.
- Personelin ve birimlerin Bilgi İşlem Daire Başkanlığı onayı olmaksızın kurumsal verileri ücretsiz veya bireysel bulut servislerine (Dropbox, WeTransfer, kişisel Google Drive/OneDrive vb.) yüklemesi yasaktır. Kurumsal bilgilerin ve kişisel verilerin, Bilgi İşlem Daire Başkanlığı'nın onayından geçmemiş, kurumsal sözleşmesi bulunmayan üçüncü taraf ticari veya ücretsiz bulut depolama, dosya paylaşım ve üretken yapay zekâ servislerine aktarılması kesinlikle yasaktır.
- Kaynağı bilinmeyen sitelerden yazılım, betik veya eklenti indirilmez ve çalıştırılmaz.
- Eğitim, araştırma veya güvenlik incelemesi gibi meşru gerekçelerle kısıtlanmış web kaynaklarına erişim ihtiyacı doğması hâlinde, talep gerekçesiyle birlikte BİDB'ye bildirilir. Uygun görülen talepler, belirli kullanıcı veya sistemlerle ve tanımlı süre ile sınırlı olacak şekilde karşılanır, verilen izinler kayıt altına alınır.

4.2. E-Posta Kullanımı

- Kurumsal e-posta hesapları, Üniversite adına yürütülen yazışmaların gerçekleştirilmesi amacıyla tahsis edilir ve kurumsal iletişim aracı niteliği taşır.

- Kurumsal işlerle ilgili yazışmalar yalnızca kurumsal e-posta hesapları üzerinden yürütülür. Kişisel e-posta hesapları üzerinden kurumsal bilgi gönderilmez ve kurumsal e-postalar kişisel hesaplara yönlendirilmez.
- E-posta hesabı kişiye özeldir; başka bir kullanıcı adına e-posta gönderilmez. Görev devri gerektiren durumlarda yetkilendirme ilgili birim yöneticisinin onayı ile yapılır.
- Gönderilen iletilerin boyutu ve ek dosya türleri sistem tarafından denetlenir. Tanımlanan sınırların üzerindeki iletiler ile izin verilmeyen türdeki dosya ekleri (çalıştırılabilir dosyalar, riskli formatlar) engellenir.
- Şüpheli iletilerdeki bağlantılara tıklanmaz, ekler açılmaz.
- Boyut sınırı nedeniyle e-posta ile gönderilemeyen dosyalar için Üniversite tarafından sağlanan dosya paylaşım yöntemleri kullanılır; kişisel bulut depolama hizmetleri kullanılmaz.
- Kimlik bilgisi, parola veya kişisel veri talep eden iletilere yanıt verilmez. Üniversite hiçbir koşulda e-posta yoluyla parola talep etmez.
- Şüpheli iletiler silinmeden önce BİDB'ye bildirilir. Bildirim, olası bir saldırının diğer kullanıcılara ulaşmadan engellenmesini sağlar.
- Ödeme, hesap değişikliği veya acil işlem talep eden iletiler, gönderen ile farklı bir iletişim kanalı üzerinden doğrulanmadan işleme alınmaz.
- Gizlilik derecesi "Gizli" olan bilgiler, Üniversite dışına e-posta ile gönderilirken şifreli kanallar kullanılır veya dosya şifrelenerek gönderilir, şifre bilgisi farklı bir iletişim kanalı üzerinden alıcıya iletilir.
- Alıcı adresleri gönderim öncesinde kontrol edilir. Çok sayıda dış alıcıya yapılan gönderimlerde, alıcıların birbirinin adresini görmemesi için gizli kopya (BCC) alanı kullanılır.
- Ticari reklamlar, haber duyuruları, zincir e-postalar, istenmeyen toplu iletiler ve doğruluğu teyit edilmemiş uyarı mesajları kurumsal e-posta ile iletilmez.

4.3. Üniversite Bilgi Sistemlerine Uzaktan Erişim ve VPN Kullanımı Kuralları

Üniversite ağına ve bilgi sistemlerine, Üniversite yerleşkesi dışından (evden çalışma, saha çalışması, tedarikçi uzaktan bakımı vb.) erişim, Bilgi İşlem Daire Başkanlığı tarafından sunulan VPN hizmeti üzerinden yapılır ve aşağıdaki kurallara tabidir.

- Üniversite yerleşkesi dışından erişim yalnızca BİDB tarafından sağlanan ve yönetilen VPN hizmeti ve belirlenen istemci yazılımı kullanılarak yapılır. İstemci yazılımı yalnızca BİDB'nin yönlendirdiği kaynaklardan indirilir. Kullanıcılar tarafından ayrı VPN sunucusu, uzaktan erişim aracı veya tünelleme hizmeti kurulması ve kullanılması yasaktır.
- EBYS, e-imza vb. güvenlik açısından kritik servislere Üniversite dışından yalnızca VPN bağlantısı kurulduktan sonra erişim sağlanabilir. Diğer uzak masaüstü ve ekran paylaşım yazılımlarının kurulması ve kullanılması yasaktır.
- VPN hizmeti akademik, idari, eğitim ve araştırma amaçlı kullanım için sunulur. VPN ile bağlanan kullanıcılar, kampüs ağına yerel olarak bağlanan kullanıcılarla aynı kural ve sorumluluklara tabidir. Uzaktan erişim yetkisi en az ayrıcalık ilkesine göre tanımlanır ve yalnızca ihtiyaç duyulan sistemlerle sınırlandırılır.
- VPN bağlantısı, oturum açıldıktan 24 saat sonra otomatik olarak sonlandırılır. Ayrıca 60 dakika boyunca etkin olmayan oturumlar da otomatik olarak sonlandırılır.
- VPN hizmeti varsayılan olarak bölünmüş tünel yapısında çalışır; tünel üzerinden yalnızca ODTÜ kaynaklarına yönelik trafik iletilir, diğer bağlantılar için kullanıcının kendi internet bağlantısı kullanılır. BİDB, güvenlik gereksinimlerine göre belirli profiller için tüm trafiğin tünelden geçirilmesini zorunlu kılabilir.
- VPN ile bağlanılan cihazın işletim sistemi ve uygulamaları güncel olmalı; cihazda güncel ve etkin bir zararlı yazılımdan korunma yazılımı ile yerel güvenlik duvarı bulunmalıdır. Üniversiteye ait olmayan cihazlar VPN ve ağ politikalarına uygun biçimde yapılandırılmalıdır.
- İnternet kafe, kütüphane bilgisayarı gibi ortak kullanıma açık cihazlardan VPN bağlantısı kurulması yasaktır. VPN bağlantısı açıkken cihaz başkalarının kullanımına bırakılmaz, işlem

tamamlandığında bağlantı sonlandırılır. Uzaktan erişimde kurumsal bilgi kişisel cihazlarda depolanmaz.

- VPN bağlantısı üzerinden proxy, DHCP, DNS, yönlendirme vb. servislerin sunulması veya Üniversite ağına başka ağların/cihazların köprülenmesi; port tarama, paket dinleme, parola kırma, hizmet engelleme gibi saldırı veya zafiyet tarama faaliyetleri (yetkili BİDB çalışmaları hariç); P2P dosya paylaşımı ve telif hakkı korumalı içeriğin paylaşılması; kişisel kazanç veya ticari amaçlı kullanım ile toplu/istenmeyen e-posta gönderimi; zararlı yazılım bulaşmış olduğu bilinen veya şüphelenilen cihazla bağlantı kurulması; erişim kısıtlamalarını, kayıt mekanizmalarını veya güvenlik kontrollerini atlatmaya yönelik girişimlerde bulunulması yasaktır.
- Üçüncü tarafların (yüklenici, tedarikçi, danışman vb.) VPN erişim talepleri, ilgili birim yöneticisi veya proje koordinatörü tarafından iş gerekçesi ve süre belirtilerek BİDB'ye iletilir. Üçüncü taraflara kişiye özel hesap tanımlanır, ortak hesap kullanılmaz; erişim yalnızca talep edilen sunucu/sistem ile sınırlı ve süreli verilir, çalışma tamamlandığında hesap kapatılır. Üçüncü taraf kullanıcının erişim ihtiyacı sona erdiğinde, bunu BİDB'ye bildirmek ilgili birim yöneticisinin/proje koordinatörünün sorumluluğundadır.
- BİDB'nin hizmet aldığı tedarikçi personelin uzaktan çalışması sırasında yapılan işlemler BİDB sunucularında ekran kaydı alınarak kaydedilir. Diğer birimlerde üçüncü taraf personelin VPN sonrası ilgili sunucuda yaptığı iş ve işlemler proje koordinatörünün sorumluluğundadır.
- VPN bağlantılarına ilişkin kayıtlar (kullanıcı kodu, bağlantı zamanı, süre, kaynak IP adresi, atanan iç IP adresi vb.) tutulur ve 5651 sayılı Kanun ile ilgili mevzuatta öngörülen süreler boyunca bütünlüğü korunarak saklanır. BİDB olağan dışı bağlantıları (eş zamanlı farklı konumlardan oturum, kısa sürede çok sayıda başarısız giriş, beklenmeyen ülkelerden bağlantı vb.) izler; şüpheli durumlarda oturumu sonlandırabilir ve hesabı geçici olarak askıya alabilir. Kayıtlar yalnızca bilgi güvenliği, hizmet sürekliliği ve yasal yükümlülükler amacıyla, KVKK hükümlerine uygun olarak işlenir.
- Bu kurallara aykırı kullanımın tespiti halinde BİDB, kullanıcının VPN erişimini uyarı yapmaksızın geçici veya kalıcı olarak kapatabilir. İhlaller, Bilgi Güvenliği İhlal Olayı Yönetimi Esaslarına göre

ele alınır; gerekli görülmesi halinde disiplin soruşturması başlatılır veya yasal işlem yapılır, üçüncü taraflar için sözleşme hükümleri uygulanır. VPN hesabının yetkisiz kullanıldığından veya cihazın ele geçirildiğinden şüphelenen kullanıcılar durumu vakit kaybetmeden BİDB'ye bildirmekten sorumludur.

4.4. Son Kullanıcı Cihazlarının Kullanımı

- Kullanıcılara tahsis edilen cihazlar demirbaş/zimmet kayıtları üzerinden envantere alınır ve sahiplik atamaları yapılır. Zimmetli cihazın korunmasından kullanıcı sorumludur.
- Cihazlar, ilgili teknik grubun bilgisi dışında donanımsal veya yazılımsal olarak değiştirilmez; Üniversite dışına çıkarılması gereken durumlarda ilgili birim yöneticisi bilgilendirilir.
- Cihazlara iş amacı dışında yazılım kurulmaz. Kurulabilecek yazılımlar; mevcut yazılımlara ait güncellemeler ve güvenlik yamaları ile Üniversite tarafından onaylanmış yazılımlarla sınırlıdır.
- Lisanssız yazılım, kaynağı bilinmeyen yazılım ve lisans koruma mekanizmalarını devre dışı bırakan araçlar kullanılmaz.
- Fikri mülkiyet haklarına sahip materyaller ile yazılım ürünlerinin kullanımı üzerindeki yasal, düzenleme ve anlaşmalardan kaynaklanan hakların korunması amacıyla işletim sistemleri, ofis uygulamaları ve diğer yazılım ürünleri lisanslı ya da açık kodlu olarak tedarik edilir.
- Lisanssız veya kopya (korsan) yazılım kurulamaz, kullanılamaz. Lisans anahtarı üretme, kırma (crack) vb. yöntemlerle lisans denetimi atlatılamaz. Lisanslı yazılımlar ve telif hakkı kapsamındaki materyaller, lisans koşullarına aykırı biçimde kopyalanamaz, çoğaltılamaz ve dağıtılamaz.
- İşletim sistemi ve uygulama güncellemeleri geciktirilmez, merkezî olarak dağıtılan güncellemelerin uygulanması engellenmez.
- Üniversite tarafından lisanslanan kötü amaçlı yazılım koruma çözümünün kurulu ve etkin tutulması zorunludur. Kullanıcılar tarafından devre dışı bırakılamaz veya kaldırılamaz.
- Kullanıcılar, cihazlarından ayrılırken oturumlarını kilitler. İş günü sonunda cihazlar kapatılır veya oturum kapatılır.
- Kişisel cihazlar üzerinde kurumsal bilgi depolanmaz ve işlenmez.

- Kişisel mobil cihazlardan kurumsal e-posta hizmetine erişim, cihazda erişim kodu ve oturum kilidi bulunması koşuluyla yapılabilir. Bu erişim kurumsal veri depolama hakkı doğurmaz.

4.5. Taşınabilir Bellek Aygıtlarının Kullanımı

Taşınabilir bellek aygıtları, veri sızıntısı ve zararlı yazılım bulaşması açısından yüksek risk taşıdığından kullanımı aşağıdaki kurallara tabidir.

- Taşınabilir bellek aygıtları yalnızca iş amaçlı ve zorunlu hâllerde kullanılır. Kurumsal verilerin merkezî sistemler ve Üniversite tarafından sağlanan paylaşım yöntemleri üzerinden taşınması esastır.
- Gizlilik derecesi "Hizmete Özel" ve üzeri olan bilgilerin taşınabilir bellek aygıtlarına kopyalanması yasaktır. Zorunlu hâllerde bu işlem şifrelenerek yapılır.
- Kişisel veri içeren dosyalar, ilgili birim yöneticisinin onayı olmaksızın taşınabilir bellek aygıtlarına aktarılmaz.
- Cihaza bağlanan taşınabilir bellek aygıtları, kullanılmadan önce kötü amaçlı yazılım koruma çözümü ile taranır.
- Kaynağı bilinmeyen, sahipsiz bulunan veya üçüncü taraflarca hediye/tanıtım amacıyla verilen bellek aygıtları Üniversite tarafından sağlanan cihazlara bağlanmaz.
- Taşınabilir bellek aygıtları gözetimsiz bırakılmaz, kullanılmadığı zamanlarda görünür olmayan bir alanda (dolap, çekmece vb.) muhafaza edilir.
- Aygıt üzerindeki kurumsal veriler, kullanım amacı sona erdiğinde geri döndürülemez şekilde silinir.
- Kurumsal veri içeren bir aygıtın kaybolması veya çalınması hâlinde durum gecikmeksizin BİDB'ye bildirilir.
- Kullanım ömrü sona eren aygıtlar, içerdiği veriler güvenli şekilde silindikten veya aygıt fiziksel olarak imha edildikten sonra elden çıkarılır.

4.6. Yazıcı veya Fotokopi Makinesi Kullanımı

- Yazıcı ve fotokopi cihazları iş amaçlı kullanılır, kişisel amaçlı toplu çıktı alınmaz.
- Gizlilik derecesi "Hizmete Özel" ve üzeri olan belgeler yazdırıldıktan sonra cihaz üzerinde bekletilmez. Yazdırma işleminin hemen ardından alınır.
- Yazıcı ve fotokopi cihazlarının üzerinde, yakınında veya çevresindeki atık kutularında gizlilik dereceli belge, çıktı veya taslak bırakılmaz.
- Gizlilik dereceli belgelerin imhası, evrak imha makinesi kullanılarak yapılır.
- Tarama işlevi kullanılarak oluşturulan belgeler, cihaz belleğinde veya paylaşımlı dizinlerde gereksiz süreyle bırakılmaz.
- Kullanıcılar çalışma alanlarını terk ederken, gizlilik dereceli belgeleri masa üzerinde açıkta bırakmaz. Bu kategorideki belgeler kilitli dolap veya çekmecelerde muhafaza edilir.

5. GÖZDEN GEÇİRME VE GÜNCELLEME

Bu politika, yılda en az bir kez gözden geçirilir.

6. İLGİLİ DOKÜMANLAR

İlgili dokümanların en güncel versiyonlarına (ayrıca bilgi verilmediği sürece) http://security.cc.metu.edu.tr adresinde “Belgeler” bağlantısından ulaşmak mümkündür.

- ISO/IEC 27001 Standardı
- ISO/IEC 27002 Standardı
- Bilgi Güvenliği İhlal Olayı Yönetimi Esasları