



ÇANKIRI KARATEKİN ÜNİVERSİTESİ ERİŞİM KONTROL POLİTİKASI



Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No
BG.PR.001	15.04.2026-10/2	-	-

1. Amaç

Bu politikanın amacı, üniversitenin sahip olduğu bilgi varlıklarının yetkisiz erişimlerden korunmasını sağlamak, yetkili kullanıcıların bilgilere erişimini düzenlemek ve bilgi güvenliğini artırmaktır.

2. Kapsam

Bu politika, üniversitenin tüm bilgi varlıklarına (veri tabanları, bilgi sistemleri, ağlar, dokümanlar vb.) ve bu varlıklara erişimi olan tüm personel, öğrenci ve üçüncü tarafları kapsar.

3. Tanımlar

- **Yetkilendirme:** Kullanıcıların, bilgi varlıklarına erişim izinlerinin belirlenmesi süreci.
- **Kimlik Doğrulama:** Erişim talebinde bulunan kişinin kimliğinin doğrulanması.
- **Erişim Denetimi:** Bilgi varlıklarına yapılan tüm erişimlerin izlenmesi ve kaydedilmesi.
- **İşlevsel Gereksinimler:** Kullanıcıların işlerini yapabilmeleri için gerekli olan minimum erişim düzeyi.

4. Erişim Kontrol Politikası

Bu politika çerçevesinde, erişim kontrolü aşağıdaki prensiplerle yürütülmektedir:

4.1 Minimum Erişim İlkesi

- Kullanıcılara yalnızca işlerini yapabilmeleri için gerekli olan minimum düzeyde erişim hakkı verilir.
- Her kullanıcı, yalnızca iş gereksinimlerine uygun bilgi varlıklarına erişebilir.

4.2 Kimlik Doğrulama ve Yetkilendirme

- Tüm kullanıcılar, üniversitenin bilgi varlıklarına erişmeden önce kimlik doğrulama işlemlerini tamamlamak zorundadır.
- Kullanıcılar için çok faktörlü kimlik doğrulama (MFA) kullanılmalıdır. Özellikle hassas bilgilere ve sistemlere erişimlerde MFA zorunludur.



ÇANKIRI KARATEKİN ÜNİVERSİTESİ ERİŞİM KONTROL POLİTİKASI



Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No
BG.PR.001	15.04.2026-10/2	-	-

- Kimlik doğrulama bilgileri (kullanıcı adı, şifre vb.) gizli tutulmalı ve paylaşılmamalıdır.

4.3 Rol Tabanlı Erişim Kontrolü

- Kullanıcılara, iş pozisyonlarına veya rollerine göre erişim izinleri tanımlanır.
- Erişim yetkileri, kullanıcının rolü değiştiğinde gözden geçirilir ve güncellenir.

4.4 Yetkisiz Erişimlerin Engellenmesi

- Üniversitenin bilgi varlıklarına yetkisiz erişimler engellenir. Şüpheli erişim talepleri güvenlik birimine bildirilir.
- Bilgilere erişim, kullanıcıların sadece iş gereksinimleri doğrultusunda sınırlandırılır.

4.5 Erişim İzni Verme, Gözden Geçirme ve Kaldırma

- Yeni kullanıcıların bilgi varlıklarına erişim izni, yalnızca ilgili yönetici onayıyla verilir.
- Erişim izinleri, belirli periyotlarla gözden geçirilir; görev değişikliği veya işten ayrılma durumunda ilgili kişinin erişim izinleri derhal kaldırılır.

4.6 Kullanıcı Hesap Yönetimi

- Her kullanıcıya, kimliğini tanımlayan benzersiz bir kullanıcı hesabı atanır.
- Kullanıcı hesapları, iş gerekleri doğrultusunda sadece ilgili varlıklara erişim izni sağlar.
- Kullanılmayan kullanıcı hesapları belirli bir süre sonunda askıya alınır veya kapatılır.

5. Erişim Denetimi ve İzleme

- Bilgi varlıklarına yapılan tüm erişim işlemleri, izlenir ve loglanır. Bu loglar, yasal yükümlülükler çerçevesinde belirli bir süre boyunca saklanır.
- Güvenlik ihlali, yetkisiz erişim veya şüpheli bir faaliyet tespit edilirse, bu durum güvenlik birimine bildirilir ve olay yönetimi süreci başlatılır.

6. Parola Politikası

- Parolalar en az 12 karakter uzunluğunda olmalı, büyük-küçük harf, sayı ve özel karakter içermelidir.
- Kullanıcılar parolalarını düzenli olarak değiştirmelidir (en fazla 180 gün).
- Aynı parolanın tekrar kullanımı yasaktır ve parola paylaşımı kesinlikle yasaktır.

7. Üçüncü Taraf Erişimi

- Üniversitenin bilgi varlıklarına üçüncü taraf erişim gereksinimi varsa, bu erişimler



ÇANKIRI KARATEKİN ÜNİVERSİTESİ
ERİŞİM KONTROL POLİTİKASI



Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No
BG.PR.001	15.04.2026-10/2	-	-

belirli bir sözleşme çerçevesinde ve güvenlik biriminin onayı ile sağlanır.

- Üçüncü taraf erişim izinleri, yalnızca belirlenen amaçlarla sınırlandırılır ve erişim sağlandığı süreç boyunca izlenir.

8. Eğitim ve Farkındalık

- Tüm kullanıcılar, bilgi güvenliği ve erişim kontrol politikaları hakkında eğitilir.
- Eğitimler, kullanıcılara erişim yetkilerinin sorumlulukları, şifre güvenliği ve yetkisiz erişimlerin riskleri hakkında bilgi sağlar.

9. Gözden Geçirme ve Güncelleme

- Bu politika, her yıl en az bir kez veya ihtiyaç halinde bilgi güvenliği birimi tarafından gözden geçirilir.
- Politikanın güncellenmesi durumunda tüm personel bilgilendirilir.

10. Yaptırımlar

Bu politikaya uymayan her türlü eylem, yükseköğretim kurumlarını kapsayan ilgili disiplin mevzuatı çerçevesinde değerlendirilir. İhlaller, ilgili mevzuatta belirtilen çeşitli yaptırımlara tabi olabilir.

11. Yürürlük

Bu politika, Çankırı Karatekin Üniversitesi Senatosu tarafından kabul edildiği tarihte yürürlüğe girer.