T.C.
DOĞU ANADOLU PROJESİ
BÖLGE KALKINMA İDARESİ BAŞKANLIĞI

BİLGİ VE İLETİŞİM GÜVENLİĞİ POLİTİKASI

Doküman No	DAP-BG-POL-01
Sürüm	1.0
Yürürlük Tarihi	26/06/2026
Gizlilik Derecesi	Tasnif Dışı (Kamuya Açık)
Hazırlayan	Yönetim Hizmetleri Koordinatörlüğü — Bilgi İşlem
Onaylayan	Başkanlık Makamı (Olur)
Dayanak Rehber Sürümü	Bilgi ve İletişim Güvenliği Rehberi (BİGR) Sürüm 1.0

1. AMAÇ

Bu Politika; Doğu Anadolu Projesi Bölge Kalkınma İdaresi Başkanlığının (DAP/İdare) sahip olduğu bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik ilkeleri çerçevesinde korunması, bilgi güvenliği yönetim sisteminin kurulması ve sürdürülmesi, personelin ve ilgili üçüncü tarafların uyması gereken bilgi güvenliği kurallarının çerçevesinin belirlenmesi amacıyla hazırlanmıştır. Politika, İdarenin Bilgi ve İletişim Güvenliği Rehberi (BİGR) ile TS ISO/IEC 27001 standardına uyumunu yansıtan üst doküman niteliğindedir.

2. KAPSAM

Bu Politika; İdarenin merkez teşkilatında ve sorumluluk alanındaki 15 ilde yürütülen iş ve işlemler kapsamında kullanılan tüm bilgi varlıklarını, bilişim sistemlerini (donanım, yazılım, ağ, veri), elektronik ve fiziksel ortamdaki bilgiyi, bu varlıklara erişen personeli ve üçüncü tarafları (yüklenici, tedarikçi, danışman ve hizmet sağlayıcılar) kapsar.

Politika; e-posta ve dizin (AD) sunucuları, elektronik belge yönetim sistemi (EBYS), internet siteleri, veri depolama, veri güvenliği ve lisans hizmetleri ile bu hizmetlerin merkezi yapı üzerinden temin edildiği dış kaynak/tedarikçi ilişkilerini de kapsamına alır.

3. DAYANAK

- • 6/7/2019 tarihli ve 30823 sayılı Resmî Gazete'de yayımlanan 2019/12 sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi
- • 19/3/2025 tarihli ve 32846 sayılı Resmî Gazete'de yayımlanan 7545 sayılı Siber Güvenlik Kanunu
- • 6698 sayılı Kişisel Verilerin Korunması Kanunu (özellikle 12 nci madde)
- • Cumhurbaşkanlığı tarafından yayımlanan Bilgi ve İletişim Güvenliği Rehberi (BİGR) ve Bilgi ve İletişim Güvenliği Denetim Rehberi
- • 642 sayılı Kanun Hükmünde Kararname (İdarenin kuruluş ve görev mevzuatı)

- • TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı

Not: Bilgi ve İletişim Güvenliği Rehberi uyum, denetim ve gözetim faaliyetleri, Dijital Dönüşüm Ofisinin kapatılmasının (28/3/2025 tarihli ve 183 sayılı Cumhurbaşkanlığı Kararnamesi) ardından Siber Güvenlik Başkanlığı bünyesinde yürütülmekte olup ilgili mevzuat yürürlüktedir.

4. TANIMLAR VE KISALTMALAR

- **Bilgi varlığı:** İdare için değer taşıyan; elektronik veya fiziksel ortamdaki her türlü veri, doküman, yazılım, donanım, hizmet ve personeli,
- **BGYS:** Bilgi Güvenliği Yönetim Sistemini,
- **BİGR:** Bilgi ve İletişim Güvenliği Rehberini,
- **BİGDES:** Bilgi ve İletişim Güvenliği Uyum ve Denetim İzleme Sistemini,
- **Gizlilik/Bütünlük/Erişilebilirlik:** Bilginin yalnız yetkililerce erişilebilir, doğru-tutarlı ve gerektiğinde erişilebilir olmasını,
- **Kurum Yetkilisi:** BİGR kapsamında İdare ile Siber Güvenlik Başkanlığı arasındaki koordinasyonu sağlamak üzere belirlenen asıl ve yedek personeli,
- **SOME:** Siber Olaylara Müdahale Ekibini,
- **Üst Yönetici:** İdare Başkanını,

ifade eder.

5. POLİTİKA İLKELERİ

İdarenin bilgi güvenliği yönetimi aşağıdaki temel ilkeler üzerine kurulur:

- • Tüm bilgi varlıklarında gizlilik, bütünlük ve erişilebilirlik esas alınır.
- • Bilgi güvenliği risk temelli yönetilir; riskler kabul edilebilir seviyenin altında tutulur.
- • Erişimde 'bilmesi gereken' ve 'en az yetki' ilkeleri uygulanır.
- • Bilgi güvenliği kurumsallık, süreklilik ve sürdürülebilirlik temelinde, sürekli iyileştirme yaklaşımıyla yürütülür.
- • Mevzuata, sözleşme şartlarına ve standartlara uyum güvence altına alınır.
- • Bilgi güvenliği tüm personelin sorumluluğudur; farkındalık kurum kültürünün parçasıdır.
- • Kişisel veriler hukuka uygun, ölçülü ve güvenli şekilde işlenir ve korunur.

6. BİLGİ GÜVENLİĞİ ORGANİZASYONU VE SORUMLULUKLAR

Rol	Sorumluluk
Üst Yönetici (Başkan)	Politikayı onaylar, gerekli kaynağı tahsis eder, bilgi güvenliğini sahiplenir ve gözetir. BİGDES'te Kurum Üst Yöneticisi olarak kayıtlıdır.
Kurum Yetkilisi (Asıl/Yedek)	BİGR kapsamında Siber Güvenlik Başkanlığı ile koordinasyonu sağlar, BİGDES işlemlerini yürütür. Asıl: Üst Yönetici; Yedek: Bilgi İşlem personeli.
Bilgi Güvenliği / Bilgi İşlem	Yönetim Hizmetleri Koordinatörlüğü bünyesinde; tedbirlerin uygulanması, izlenmesi, sıkılaştırma, yedekleme ve teknik kontrollerden sorumludur.

Kurumsal SOME	Siber olayların tespiti, müdahalesi ve Siber Güvenlik Başkanlığına/USOM'a bildiriminden sorumludur (Kurumsal SOME Yöneticisi koordinasyonunda).
Personel	Politika ve alt prosedürlere uyar, parola/temiz masa-ekran kurallarına riayet eder, şüpheli durumları bildirir.
Üçüncü Taraf / Tedarikçi	Sözleşmelerinde tanımlı gizlilik ve güvenlik şartlarına uyar; merkezi altyapı hizmet sağlayıcıları dâhil.

7. VARLIK YÖNETİMİ VE SINIFLANDIRMA

İdarenin bilgi varlıkları, BİGR'de tanımlı varlık grubu ana başlıkları ile uyumlu olarak tanımlanır, envantere alınır ve kritiklik derecesine (1-3) göre sınıflandırılır. Her varlık grubuna kritiklik derecesine uygun sıkılaştırma ve teknoloji tedbirleri uygulanır. Varlık envanteri ve kritiklik dereceleri düzenli olarak gözden geçirilir.

İdarede tanımlı varlık grubu ana başlıkları: Ağ ve Sistem Güvenliği, Uygulama ve Veri Güvenliği, Taşınabilir Cihaz ve Ortam Güvenliği, Nesnelerin İnterneti (IoT) Güvenliği, Fiziksel Mekânların Güvenliği ve Personel Güvenliği.

8. İNSAN KAYNAKLARI GÜVENLİĞİ VE FARKINDALIK

Personele yılda en az bir kez bilgi güvenliği farkındalık eğitimi verilir; temiz masa-temiz ekran, parola, sosyal mühendislik ve veri sınıflandırma sorumlulukları hatırlatılır. Bilgi güvenliği sorumlusu/sorumlularına ilgili eğitim ve uzmanlık kazandırılır. İşe başlama, görev değişikliği ve işten ayrılma süreçlerinde yetki tanımlama/iptali güvenlik kuralları çerçevesinde yürütülür.

9. ERİŞİM YÖNETİMİ VE PAROLA GÜVENLİĞİ

Tüm kullanıcılar benzersiz kullanıcı adı ve parola ile tanımlanır; hesaplar 'bilmesi gereken' ve 'en az yetki' ilkesine göre yetkilendirilir. Güçlü parola kullanımı zorunludur, parolalar düzenli aralıklarla değiştirilir ve paylaşılmaz. Sistemlerin varsayılan (fabrika) parolaları değiştirilir; yerel yönetici (local admin) parolaları yalnız yetkili Bilgi İşlem personelinde tutulur.

10. FİZİKSEL VE ÇEVRESEL GÜVENLİK

Sistem odası ve kritik alanlara erişim kimlik doğrulama ile sınırlandırılır ve kayıt altına alınır. Sistem odalarının sıcaklık, nem ve enerji süreklilik koşulları sağlanır; yangın, su baskını ve benzeri olaylara karşı önleyici tedbirler alınır.

11. AĞ, SİSTEM VE İŞLETİM GÜVENLİĞİ

Kurumsal ağda yalnız etki alanına (domain) dâhil, güncel ve merkezi virüsten koruma yazılımı ile korunan cihazlar bulundurulur. Güvenlik duvarı/UTM ile ağ trafiği denetlenir; kurumsal ağ, misafir ağı ve diğer sistemler birbirinden mantıksal olarak ayrılır (VLAN). İşletim sistemleri ve yazılımlar güncel ve desteklenen sürümlerde tutulur; desteklenmeyen sürümler kaldırılır. Misafir ağında kimlik doğrulamalı erişim ve 5651 sayılı Kanun kapsamında log kaydı sağlanır.

12. UYGULAMA-VERİ GÜVENLİĞİ VE TEKNİK AÇIKLIK YÖNETİMİ

Kritik veri işleyen uygulamalar için veri tabanı sıkılaştırması uygulanır. İç geliştirme veya dış tedarik edilen yazılımlarda güvenli yazılım geliştirme gereksinimleri gözetilir. Sistemlerde periyodik zafiyet taraması ve gerektiğinde sızma testi yapılır; tespit edilen açıklıklar önceliklendirilerek giderilir.

13. KİŞİSEL VERİLERİN KORUNMASI

Kişisel veriler 6698 sayılı Kanunun 12 nci maddesi uyarınca; hukuka uygun, belirli ve meşru amaçlarla, ölçülü olarak işlenir; teknik ve idari tedbirlerle yetkisiz erişime, kayba ve ifşaya karşı korunur. Veri saklama ve imha süreçleri ilgili mevzuata uygun yürütülür.

14. TAŞINABİLİR CİHAZ VE ORTAM GÜVENLİĞİ

Taşınabilir bilgisayar, akıllı cihaz ve harici bellek ortamlarının kullanımı tanımlı kurallara tabidir. Gizlilik dereceli veriler yetkilendirilmemiş cihazlarda bulundurulmaz; imha ve el değiştirme süreçlerinde veri güvenli şekilde silinir.

15. YEDEKLEME VE İŞ SÜREKLİLİĞİ

Kritik veriler düzenli olarak yedeklenir, yedeklerin bütünlüğü ve geri yüklenebilirliği periyodik test edilir. Bilişim hizmetlerinin kesintiye uğraması ihtimaline karşı iş sürekliliği ve felaket kurtarma yaklaşımı benimsenir; merkezi altyapı hizmet sağlayıcısının süreklilik taahhütleri gözetilir.

16. SİBER OLAY YÖNETİMİ

Tespit edilen zafiyet ve siber olaylar gecikmeksizin Kurumsal SOME tarafından değerlendirilir ve 7545 sayılı Kanunun 7 nci maddesi kapsamında Siber Güvenlik Başkanlığına/USOM'a bildirilir. Olay kayıtları tutulur, kök neden analizi yapılır ve tekrar önleyici tedbirler alınır.

17. TEDARİKÇİ VE ÜÇÜNCÜ TARAF GÜVENLİĞİ

Dışarıdan alınan bilişim hizmetlerinde (merkezi altyapı, bakım, danışmanlık, yazılım vb.) hizmetin kapsamı, süresi, kritiklik durumu ve güvenlik gereksinimleri yazılı hale getirilir. Siber güvenlik ürün ve hizmetleri, mevzuat gereği yetkilendirilmiş/belgelendirilmiş tedarikçilerden temin edilir. Üçüncü taraf erişimleri sınırlandırılır ve izlenir.

18. UYUM VE DENETİM

İdare, BİGR'ye uyum çalışmalarını sürdürür ve güvenlik tedbirlerinin uygulanmasına ilişkin uyum denetimini en az yılda bir kez kurum içi (öz) denetim mekanizmasıyla, Bilgi ve İletişim Güvenliği Denetim Rehberine uygun olarak gerçekleştirir. Denetim sonuçları (denetim görüşü ve tedbir etkinlik durumu) BİGDES üzerinden raporlanır. İdare, Siber Güvenlik Başkanlığı/Bakanlık eliyle yapılan yerinde gözetim denetimlerine tabidir ve bu denetimlere gerekli kolaylığı sağlar.

19. YAPTIRIM

Bu Politikaya ve alt politikalara aykırı davranışlar, fiilin niteliğine göre ilgili personel mevzuatı (657 sayılı Kanun ve diğer mevzuat) ile 7545 sayılı Kanun ve 6698 sayılı Kanun hükümleri çerçevesinde değerlendirilir.

20. GÖZDEN GEÇİRME VE GÜNCELLEME

Bu Politika; mevzuat değişiklikleri, BİGR sürüm güncellemeleri, önemli güvenlik olayları veya kurumsal değişiklikler hâlinde ve her hâlükârda yılda en az bir kez gözden geçirilir. Güncellemeler Başkanlık Makamının onayı ile yürürlüğe girer.

21. YÜRÜRLÜK

Bu Politika, Başkanlık Makamının Olur'u ile yürürlüğe girer ve İdare Başkanı tarafından yürütülür.

Bu Politika, Başkanlık Makamının Olur'u ile yürürlüğe girmiştir.