ÇAĞDAŞ CAM SANAYİ VE TİCARET AŞ
BİLGİ GÜVENLİĞİ POLİTİKASI

Doküman Sürümü: Rev.01 | İlk Onay: YK, 15.12.2025 (Karar No: 2025/23) | Revizyon Onayı: YK, 16.11.2026 (Karar No: 2026/29)

1. AMAÇ VE KAPSAM

Bu politikanın amacı, Çağdaş Cam Sanayi ve Ticaret AŞ ("Şirket") bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumak, bilgi güvenliği risklerini yönetmek ve sermaye piyasası mevzuatına (SPK VII-128.10 sayılı Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği) tam uyum sağlamaktır. Politika; Şirket bünyesindeki tüm bilgi sistemlerini, kurumsal verileri, iş süreçlerini, tüm çalışanları ve dış hizmet sağlayıcıları kapsamaktadır. Bu politika, Şirket'in bilgi güvenliğine ilişkin tek ve bağlayıcı üst politika belgesidir; önceki tarihli tüm bilgi güvenliği politikası metinlerinin yerine geçer.

2. BİLGİ GÜVENLİĞİ HEDEFLERİ

- Bilgi varlıklarını iç ve dış tehditlere karşı sürekli korumak ve izinsiz erişimleri önlemek.
- Bilgi güvenliği ihlallerini tespit etmek ve bu olaylara karşı hızlı müdahale mekanizmaları kurmak.
- Yasal ve düzenleyici gerekliliklere (özellikle SPK tebliğlerine) tam uyum sağlamak.
- Tüm personelin bilgi güvenliği farkındalığını yıllık eğitimlerle artırmak.
- Bilgi güvenliği risklerini yönetim kurulu tarafından onaylanmış kabul edilebilir seviyelerde tutmak.

3. ROLLER, SORUMLULUKLAR VE GÖREV TANIMLARI

- **Yönetim Kurulu:** Politikanın onaylanmasından ve bilgi sistemleri kontrollerinin etkinliğinin gözetilmesinden nihai olarak sorumludur.
- **Üst Yönetim:** Politikanın uygulanmasını gözetir, kritik projeleri onaylar ve bilgi güvenliği için yeterli kaynak tahsis eder.
- **Bilgi Güvenliği Sorumlusu (BGS):** Bilgi sistemleri güvenliğine ilişkin kontrollerin takibinden ve üst yönetime raporlanmasından sorumludur. BGS, bilgi sistemleri yönetimine ilişkin operasyonel bir görev üstlenemez ve doğrudan üst yönetime bağlı çalışır.
- **BT Departman Sorumlusu:** Bilgi sistemleri altyapısının (sunucu, ağ, yazılım vb.) işletiminden, bakımından ve teknik sürekliliğinin sağlanmasından sorumludur. BGS tarafından belirlenen güvenlik kriterlerinin teknik olarak uygulanmasını koordine eder.
- **Tüm Personel:** Şirket'in bilgi güvenliği kurallarına uymak ve şüpheli durumları bildirmekle yükümlüdür.

Bu politikada tanımlanan rollere ilişkin ayrıntılı görev ve sorumluluklar, Bilgi Güvenliği Sorumlusu Görev Tanımı ile bilgi sistemleri rollerine ilişkin görev tanımı dokümanlarında kişi bazında belirlenir; görev tanımları bu politikanın tamamlayıcı ekidir ve politika ile birlikte yılda en az bir kez gözden geçirilir.

4. TEMEL GÜVENLİK PRENSİPLERİ

- **Risk Yönetimi:** Bilgi varlıklarına yönelik riskler yılda en az bir kez analiz edilir ve risk seviyelerine göre iyileştirici faaliyetler planlanır.

- **Erişim Yönetimi:** Kullanıcılara yalnızca işleri için gerekli olan "en az yetki" atanır. Kritik sistemlere ve uzaktan erişimlere yönelik işlemlerde Çok Faktörlü Kimlik Doğrulama (MFA) kullanımı zorunludur.
- **Varlık Yönetimi:** Tüm bilgi varlıkları (donanım, yazılım, veri) envanterde kayıt altına alınır ve kritiklik seviyelerine göre sınıflandırılır.
- **Kayıt ve İzlenebilirlik:** Kritik bilgi sistemleri üzerindeki işlemler ve güvenlik olaylarına ilişkin denetim izleri (loglar) en az 5 yıl boyunca saklanır.
- **İş Sürekliliği ve Yedekleme:** Kritik süreçleri destekleyen sistemlerin yedekleme stratejisi yazılı hale getirilir ve geri dönüş testleri yılda en az bir kez yapılır. Birincil sistemlerin devre dışı kalması durumunda en geç 24 saat içinde faaliyetlerin sürdürülmesi esastır.

5. KONTROLLERİN TESİSİ, DEĞERLENDİRİLMESİ VE GÖZETİMİ

Tebliğ kapsamındaki bilgi sistemleri kontrolleri için kontrol sahipleri, kontrol kanıtları ve kontrol sıklıkları BGS koordinasyonunda hazırlanan kontrol listesinde tanımlanır. Kontrollerin işleyişi BGS tarafından düzenli olarak izlenir; sonuçlar dönemsel olarak Üst Yönetim'e, yılda en az bir kez ise uyum durumu değerlendirmesi ile birlikte Yönetim Kurulu'na raporlanır. Tespit edilen eksiklikler için sorumlusu ve termini belirlenmiş aksiyon planları oluşturulur ve takip edilir.

6. DIŞ HİZMET ALIMI VE ÜÇÜNCÜ TARAFLAR

- Kurumsal kaynak planlama, üretim takip ve ofis/iş birliği sistemleri gibi kritik hizmetlerin alımında; hizmet seviyesi (SLA), veri kaybı hedefi (RPO) ve kurtarma süresi (RTO) değerleri sözleşmelerle netleştirilir.
- Dış hizmet sağlayıcıların Şirket'in bilgi güvenliği standartlarına uyması ve gizlilik yükümlülüklerini yerine getirmesi zorunludur.

7. GÖZDEN GEÇİRME

Bu politika ve bilgi güvenliğine ilişkin tüm sorumluluklar, yılda en az bir kez veya Şirket yapısında önemli bir değişiklik olduğunda, BGS koordinasyonunda gözden geçirilir. Gözden geçirme sonuçları rapor ile kayda alınır; politika değişiklikleri Yönetim Kurulu onayıyla yürürlüğe girer ve personele duyurulur. Duyuru ve yayım kayıtları muhafaza edilir.

8. YÜRÜRLÜK

Bu politika, Yönetim Kurulu tarafından onaylandığı tarihte yürürlüğe girer. Bu politikanın yürürlüğe girmesiyle, daha önceki tarihli tüm bilgi güvenliği politikası metinleri (02.01.2026 tarihli P00 dahil) yürürlükten kalkar.