BGYS Politikası

1.İÇDAŞ A.Ş. BGYS POLİTİKASI

İÇDAŞ BGYS politikası ile kurumsal güvenilirliğini ve temsil ettiği markanın imajını korumayı, üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamayı, firmamızın temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak amacıyla, bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi varlıklarının bilgi güvenliğini sağlamayı ve üst yönetimin bilgi güvenliği yaklaşımını tüm çalışanlara ve ilgili taraflara bildirmeyi hedefler.

İÇDAŞ, Üst yönetim tarafından onaylanmış bu politika ile "BGYS Hedefleri" dokümanında belirtilen hedeflere ulaşmak için aşağıdaki ilkeleri benimser:

- Bilgiyi izinsiz erişime karşı korumak, tespit edilen izinsiz erişim olay sayısını azaltmak,
- Bilginin gizliliğini sağlamak, gizli bilginin ifşası gibi olayları minimumda tutmak,
- Bilginin yetkisiz kişilere kasten verilmemesini sağlamak,
- Bilginin bütünlüğünü sağlamak, bütünlük ile ilgili ihlal sayısını azaltmak,
- Bilgiye erişilebilirliği sağlamak ve uptime oranlarını iş ihtiyaçlarına uygun seviyede tutmak,
- Yürürlükteki yasa ve sözleşmelerin gereklerini karşılamak, yasal yaptırım ve sözleşme uyumsuzluğu sorunlarını minimum seviyede tutmak,
- Tüm çalışanlara bilgi güvenliği eğitimi verilmesini ve tüm bilgi güvenliği açıkları ve şüphe duyulan zayıf noktaların sorumlu kişilere raporlanmasını sağlamak, kayıtsız olay sayısını minimuma indirmek,
- Sisteme olan saldırıları bertaraf etmek, başarılı saldırı sayısını sıfırda tutmak,
- Kapsamdaki süreçlerin en az kesinti ile devam etmesini sağlamak, kesinti süresini yılda 1 günün altında tutmak.

BGYS Politikası

İÇDAŞ, "Bilgi Güvenliği Politikası"nın uygulanmasının sağlanması ve kontrolünün yapılmasının, güvenlik ihlallerinde de gerekli yaptırımın icra edilmesinin yönetim tarafından desteklendiğini beyan eder.

İÇDAŞ müşterileri ve tedarikçileri ile iş ilişkilerindeki bütünlüğü sürdürülmesi rekabet avantajı elde edilmesi ve kurumsal imajın korunması, bilgi varlıklarına zamanında, eksiksiz, doğru ve kesintisiz biçimde ulaşması için bilginin gizliliği, bütünlüğü ve gerektiği zamanda hazır ve hizmette olmasını sağlar.

İÇDAŞ BGYS'yi kurumsal bilginin gizliliği, bütünlüğü ve erişilebilirliğinin yönetilebilmesi, kuruluş dışı taraflarca erişilen, işleme tabi tutulan, iletilen ya da yönetilen kurumsal bilgi ve bilgi sistemlerinin güvenliğini sürdürmek amacı ile görev ve sorumlulukları "Bilgi Güvenliği Organizasyonu Politikası"nda belirtilen, BGYS yönetici ve takımı ile destekler.

Risk yönetim çerçevesi, bilgi güvenliği risklerinin tanımlanmasını, değerlendirilmesini, işlenmesini kapsar. Risk değerlendirmesi, uygulanabilirlik bildirgesi, risk işleme planı ve bilgi güvenliği risklerinin nasıl kontrol edildiği "Risk Yönetim Politikası" ile tanımlanır. Bu politikanın yönetiminden ve gerçekleştirilmesinden BGYS Yöneticisi sorumludur.

Risklerin ortadan kaldırılmasından çok istenmeyen olayların gerçekleşebilme olasılıklarının azaltılması, etkilerinin minimize edilmesi yönünde fırsatlar sağlanması, kabul edilebilir risk seviyelerinin tanımlanması ve artık risklerle ilgili karar verilmesi için "Risk Yönetimi Politikası" uygulanır. Bu politika ve süreçler analiz, iyileştirme ve risklerin izlenmesi yönünde bir sistematik yöntem tanımlar.

İÇDAŞ kuruluşu, binalarına ve bilgilerine yetkisiz kişilerin fiziki olarak erişiminin, giriş yapmasının, kuruluş varlıklarının kayba uğramasının, zarar görmesinin, çalınmasının, tehlikeye düşmesinin ve iş süreçlerinin kesintiye uğramasının önlenmesini "Fiziksel ve Çevre Güvenliği Politikası" ile destekler.

BGYS Politikası

İÇDAŞ, "**Bilgi Güvenliği İhlal Olay Yönetimi Politikası"** ile bilgi sistemlerinde meydana gelebilecek güvenlik ihlallerinin tespiti, analizi ve yanıt verilmesi konusundaki rol ve sorumlulukları belirlenmesini ve ihlal olaylarına hızlı ve doğru şekilde yanıt verilmesinin sağlanmasını hedefler.

İÇDAŞ, bilgi sistemlerinden meydana gelebilecek uzun süreli arıza ya da felaket durumlarının kritik iş süreçlerine etkisinin azaltılması ve süreçlerin kısa sürede kaldığı yerden işletilebilmesinin sağlanması için "**İş Sürekliliği Politikası**"nı destekler.

İÇDAŞ, bilgi varlıklarının doğru ve güvenli bir şekilde işletilmesinin sağlanması, sistem hataları nedeni ile oluşabilecek hasarların minimize edilmesi ve varlıkların gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması, aynı zamanda İÇDAŞ sorumluluk alanları içinde güvenli ağ iletişimleri için uyulması gereken kuralların belirlenmesi için "**İşletme ve İletişim Yönetimi Politikası**"nı destekler.

İÇDAŞ, tüm çalışanların güvenlik politikaları, yasalar, regülasyonlar, sözleşmeler ve güvenlik gereksinimlerine karşı ihlalleri ve uyumluluğunu "**Uyumluluk Politikası**" ile destekler.

İÇDAŞ, bilgi varlıklarının kullanıcılar, taşeronlar, danışmanlar ya da üçüncü taraflarca kasıtlı, suistimal ya da yanlış kullanım sonucu zarar görmesi ya da imhasını önlemek için gerekli güvenlik gereksinimlerini "**İnsan Kaynakları Güvenliği Politikası**" ile tanımlar.

İÇDAŞ, "**Varlık Yönetim Politikası**" ile sahip olduğu bilgi varlıklarının gizliliği, bütünlüğü ve erişilebilirliğinin sağlanması, etkili ve verimli bir şekilde yönetilmesi ve kontrollü bir şekilde kullanılmasını amaçlar. Bu varlıklar bilgi, yazılım, donanım, insan, servisler ve süreçler olarak kategorize edilmiştir.

İÇDAŞ, kurumsal bilgi varlığına fiziksel ve mantıksal erişimlerin sadece yetkilendirilmiş kişilerce ve aygıtlar ile yapılabileceği konusunda bir "**Erişim Kontrol Politikası**" uygulamayı amaçlamaktadır.

İÇDAŞ ve bağlı kuruluşlarında çalışanların, İÇDAŞ kurumsal bilgi ve listelenenlerle sınırlı olmamak kaydı ile tüm bilişim sistem ve servisleri, elektronik posta, intranet, ekstranet, internet ve diğer tüm elektronik haberleşme yöntemlerini ve teknolojileri ile personele hizmet sözleşmesi gereği edimini yerine getirmesi için teslim edilmiş olan ve tümüyle işe özgülenmiş olan bilgisayar, cep telefonu, cep bilgisayarı, navigasyon cihazı, faks, fotokopi ve benzeri cihazların kullanımları sırasında bilginin gizliliği, bütünlüğü ve erişilebilirliğinin korunmasının sağlanmasına ilişkin ilke ve kuralları düzenlemek, bu politika dahilinde yükümlülükleri çalışanlarla paylaşmak ve söz konusu kaynakların kullanılması ile ilgili İÇDAŞ kuralları "**Kabul Edilebilir Kullanım Politikası**" ile belirlenir.

İÇDAŞ, "**Bilgi Sistemleri Temin, Geliştirme ve Bakım Politikası**" ile güvenliğin; bilgi sistemlerinin temin, geliştirme ve bakım yaşam döngüsünün bir parçası haline gelmesi amaçlanır.

2. İLİŞKİLİ POLİTİKA ve DOKÜMANLAR

- Risk Yönetimi Politikası
- Bilgi Güvenliği Organizasyon Politikası
- Varlık Yönetimi Politikası
- İnsan kaynakları Güvenliği Politikası
- Fiziksel ve Çevre Güvenliği Politikası
- İşletme ve İletişim Yönetimi Politikası
- Erişim Kontrol Politikası
- Bilgi Sistemleri Temin, Geliştirme ve Bakım Politikası
- Bilgi Güvenliği İhlal Yönetimi Politikası

- İş Sürekliliği Politikası
- Uyumluluk Politikası
- Kabul Edilebilir Kullanım Politikası
- BGYS Kapsam Beyannamesi
- BGYS Hedefleri Dokümanı

3. DOKÜMAN SAHİBİ

BGYS Yönetimi

4. REVİZYON ve GÖZDEN GEÇİRME

İÇDAŞ yönetimi yeterli kaynak sağlanarak bilgi güvenliği girişimleri desteklemek ve alınan güvenlik önlemlerinin etkinliğini periyodik olarak gözden geçirmekten sorumludur. Ayrıntılı BGYS rolleri ve sorumlulukları Bilgi Güvenliği Organizasyon Politikasında verilmiştir.

5. TANIMLAR

Bilgi Güvenliği Yönetim Sistemi (BGYS): Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sistemlerinin bir parçası.

Bilgi Güvenliği: Bilginin gizliliğinin, bütünlüğünün ve elverişliğinin korunması. Ek olarak doğruluk, hesap verilebilirlik, inkâr edememe ve güvenilirlik gibi özelliklerini de kapsar. (ISO/IEC 27001)

Yönetim: Üst yönetim tarafından atanmış BGYS Yöneticileri.

Üst Yönetim: BGYS Yönetiminin raporlama yaptığı Genel Müdür ve İcra kurulu.

BGYS Politikası

Bilgi Varlığı: Kuruluş için değer ifade eden herhangi değerli bilgi veya veri.

Gizlilik: Bilginin yetkisiz kişiler, varlıklar ya da prosesler için elverişli yapılmaması ya da açıklanmaması özelliği.

Bütünlük: Varlıkların doğruluğunu ve tamlığını koruma özelliği.

Elverişlilik: Yetkili bir tüzel kişi tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliği.

Yönetim Kurulu

20.05.2026