assisTT	**BİLGİ GÜVENLİĞİ POLİTİKASI**

AMAÇ VE KAPSAM

Bu politikanın amacı, TS ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi standardına uygun olarak AssisTT Rehberlik ve Müşteri Hizmetleri A.Ş. bünyesinde Bilgi Güvenliği Politikasının oluşturulması, duyurulması ve uygulanmasına ilişkin esasların belirlenmesidir.

Politika, TS ISO/IEC 27001:2022 standardı temel alınarak hazırlanmış olup, AssisTT Rehberlik ve Müşteri Hizmetleri A.Ş.'nin tüm faaliyet alanlarını kapsamaktadır.

SORUMLULUKLAR VE YETKİLER

Bilgi Güvenliği Kurulu ve Bilgi Güvenliği Kurul Başkanı (Yönetim Temsilcisi), bu politikanın uygulanması ve yürütülmesinden sorumludur.

AssisTT Rehberlik ve Müşteri Hizmetleri A.Ş. bünyesindeki tüm çalışanlar ile üçüncü taraflar; görev tanımları ve uzmanlık alanlarına ek olarak, bu politika ve Bilgi Güvenliği Yönetim Sistemi kapsamında hazırlanan diğer ilgili dokümanlara uymakla yükümlüdür.

TANIMLAR

Şirket: AssisTT Rehberlik ve Müşteri Hizmetleri A.Ş.'yi,
Çalışan: Şirket çalışanlarını, Şirkete bağlı işyerlerinde görev yapan alt işveren işçilerini ve bu kapsamda yer alan tüm unvan ve pozisyonlardaki personeli,
Doküman: Şirketin dokümantasyon yapısı kapsamında oluşturulan Kalite Politikası, Kalite Hedefleri, Kalite El Kitabı, Organizasyon Şemaları, Yönetmelikler, Süreçler, Prosedürler, Talimatlar, Formlar, Listeler ve Dış Kaynaklı Dokümanları,
BGYS: TS ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemini
ifade eder.

BİLGİ GÜVENLİĞİ POLİTİKASININ TANIMI

Bilgi Güvenliği Politikası, Şirketimizin bilgilerinin yönetimini, korunmasını, dağıtımını ve önemli işlevlerinin korunmasını düzenleyen kurallar ve uygulamalar bütünüdür. Bilgi güvenliği politikası, bu politika doğrultusunda uygulanacak dokümanların amaçlarını tanımlayan en üst düzey dokümandır.

BİLGİ GÜVENLİĞİ POLİTİKASININ BİLEŞENLERİ

Bilgi Güvenliği Yönetim Sistemi Politikası, şirketin bilgi güvenliği ihtiyacını ve bilgi güvenliği kavramını şirketin bilgi kaynaklarını kullanan her kişiye anlatma amacıyla hazırlanmıştır. Bilgi güvenliği politikası, şirket yönetiminin bilgi güvenliğine dair verdiği desteği gösterir.

assisTT	**BİLGİ GÜVENLİĞİ POLİTİKASI**

1. Bilgi güvenliğinin tanımı, genel kapsamı ve hedefi,
2. Bilgi güvenliğinin kurum için neden önemli olduğu, bilgi güvenliği sağlanmasının amacı ve bilgi güvenliği ilkeleri, bu amaç ve ilkeler için yönetim desteği,
3. Kontrol hedefleri ve kontrollerin seçimi için risk değerlendirmesi ve risk yönetimini de içeren bir çerçevenin ortaya konulması,
4. Bilgi Güvenliği yönetim sisteminin sürekli iyileştirilmesi için bir taahhüt içerir.
5. Güvenlik politikaları, ilkeleri, standartları ve uyum gereksinimlerinin özet bir açıklaması,
5. Bilgi güvenliği ile ilgili tüm görev ve sorumlulukların tanımı,
7. Diğer ayrıntılı politikalar ve belirli bilgi sistemleri için prosedürler veya kullanıcıların uyması gereken kurallar gibi politikayı destekleyen dokümanlara atıflardan oluşur.

BİLGİ GÜVENLİĞİNİN TANIMI, GENEL KAPSAMI VE HEDEFİ

- **BİLGİ GÜVENLİĞİNİN TANIMI**

Bilgi güvenliği politikası şirketin geneline hitap eder. Şirket içinde farklı görevlerde birçok çalışanların Bilgi Güvenliği ve Bilgi Güvenliği Kavramın herkes tarafından anlaşılmasını sağlamak için, politikada bilgi güvenliğinin açık ve anlaşılır bir tanımı yapılarak sistemde yayınlanır. Bu politikada, Bilgi Güvenliği kurumun bilgi varlıklarının aşağıdaki özelliklerinin korunması olarak tanımlanır:

GİZLİLİK: Bilginin sadece yetkili kişiler tarafından erişilebilir olması
BÜTÜNLÜK: Bilginin yetkisiz değiştirmelerden korunması ve değiştirildiğinde farkına varılması
KULLANILABİLİRLİK: Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an kullanılabilir olması

- **BİLGİ GÜVENLİĞİ İHTİYACI VE BİLGİ GÜVENLİĞİ KAPSAMI**

AssisTT Rehberlik ve Müşteri Hizmetleri A.Ş tüm lokasyonlarını ve birimlerini kapar. Çağrı Merkezi ve Müşteri Memnuniyeti Hizmetleri sunumudur.

- **BİLGİ GÜVENLİĞİ HEDEFLERİ**

Bilgi güvenliği hedefleri, bilgi güvenliğinin yönetimi ile ulaşılacak amaç hakkında çalışanları bilgilendirmektir. Bu hedefler şirketin iş gerekleri ve stratejileri ile yakından ilgilidir.

BİLGİ GÜVENLİĞİNİN ŞİRKET İÇİN NEDEN ÖNEMLİ OLDUĞU, BİLGİ GÜVENLİĞİ SAĞLANMASININ AMACI VE BİLGİ GÜVENLİĞİ İLKELERİ, BU AMAÇ VE İLKELER İÇİN YÖNETİM DESTEĞİ

- **ŞİRKET YÖNETİMİ**

- Şirketin güvenilirliğini ve temsil ettiği makamın imajını korumak,
- Üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak,
- Şirketin temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak amacıyla şirket hizmetlerinin gerçekleştirilmesinde kullanılan tüm varlıklarının bilgi güvenliğini sağlamayı hedefler.

assistt	**BİLGİ GÜVENLİĞİ POLİTİKASI**

KONTROL HEDEFLERİ VE KONTROLLERİN SEÇİMİ İÇİN RİSK DEĞERLENDİRMESİ VE RİSK YÖNETİMİNİ DE İÇEREN BİR ÇERÇEVENİN ORTAYA KONULMASI

- **RİSK YÖNETİM ÇERÇEVESİ**

Şirketin, bilgi güvenliği risklerini nasıl yönettiğini Risk Analizi ve Değerlendirme Prosedüründe açıklamaktadır. Bilgi güvenliğini sağlamak için uygulayacağı kontrolleri ve bu kontrolleri hangi risklerle bağlantılı olduğu nasıl uygulandığı açıklanmaktadır.

GÜVENLİK POLİTİKALARI, İLKELERİ, STANDARTLARI VE UYUM GEREKSİNİMLERİNİN ÖZET BİR AÇIKLAMASI

- **YÖNETİMİN BİLGİ GÜVENLİĞİNİ SAĞLAMA SÖZÜ VE POLİTİKA DOKÜMANININ ONAYI**

Yönetim, bilgi güvenliği sağlama taahhüdü, bilgi güvenliği amaçlarına ulaşma konusunda kararlılığını ve bu iş için gereken desteği sağlayacağını ifade ederken, şirket çalışanlarının bilgi güvenliğine önem vermesini de sağlamaktadır. Bu dokümanın sistemde yayınlanması yönetim tarafından onaylandığı anlamını taşır. Şirket yönetimi olarak, Şirket Bilgi Güvenliği Politikasının uygulanmasının sağlanmasının ve kontrolünün yapılmasının, güvenlik ihlallerinde de gerekli yaptırımın icra edilmesinin yönetim tarafından desteklendiğini beyan eder.

- **BİLGİ GÜVENLİĞİ KURULU**

Bu politikada belirtilen yönetimlerden ve gerçekleştirilmesinden Bilgi Güvenliği Kurulu sorumludur. Bilgi güvenliği kurulu üyeleri Bilgi Güvenliği Görev ve Sorumlulukları Prosedürü'nde tanımlıdır.

- **BİLGİ GÜVENLİĞİ İLKELERİ**

Bilgi güvenliği ilkeleri, şirketteki bilgi güvenliği ile ilgili genel kuralları koyar. Bu ilkeler kullanıcılara çeşitli konu ve kavramlarla ilintili beklenen davranışları tanımlar.

- **BİLGİ GÜVENLİĞİ İLE İLGİLİ TÜM GÖREV VE SORUMLULUKLARIN TANIMI**

AssisTT Rehberlik ve Müşteri Hizmetleri A.Ş. bünyesinde bilgi güvenliğinin etkin bir şekilde sağlanabilmesi için tüm çalışanların görev ve sorumlulukları açıkça tanımlanmıştır. Bilgi güvenliği kapsamında yer alan roller, bu rollere atanmış kişilerin görev tanımları ile bu görevlerin yerine getirilmesinden doğan sorumluluklar, Bilgi Güvenliği Görev ve Sorumluluklar Prosedürü içerisinde detaylı şekilde açıklanmıştır.

Bilgi Güvenliği Görev ve Sorumluluklar Prosedürü, bilgi güvenliği yönetim sisteminin sürdürülebilirliğini ve etkinliğini sağlamak amacıyla, Şirket genelinde bilgi güvenliğine ilişkin farkındalık yaratmak, görev dağılımını netleştirmek ve tüm paydaşların bilgi güvenliği yükümlülüklerini yerine getirmesini sağlamak üzere hazırlanmıştır.

Tüm çalışanlar, görev tanımları doğrultusunda bilgi güvenliği süreçlerine aktif olarak katılmak ve ilgili politika, prosedür ve talimatlara uymakla yükümlüdür. Ayrıca, bilgi güvenliği ile ilgili risklerin belirlenmesi, raporlanması ve gerektiğinde aksiyon alınması süreçlerine destek vermek de çalışanların sorumluluğundadır.

assisTT	**BİLGİ GÜVENLİĞİ POLİTİKASI**

POLİTİKANIN İHLALİ VE YAPTIRIMLAR

Bir kullanıcının politikaya uymadığı ve politikayı ihlal ettiği durumlarda o kullanıcıya yaptırımlar Disiplin Esasları Prosedürü'müz kapsamında değerlendirilir.

DİĞER AYRINTILI POLİTİKALAR VE BELİRLİ BİLGİ SİSTEMLERİ İÇİN PROSEDÜRLER VEYA KULLANICILARIN UYMASI GEREKEN KURALLAR GİBİ POLİTİKAYI DESTEKLEYEN DOKÜMANLARA ATIFLAR (DİĞER KURAL, YÖNERGE, STANDART VE SÜREÇLERE ATIFLAR)

Bilgi güvenliği politikası tek başına bir doküman değildir. Bilgi güvenliği amaçlarının gerçekleşmesi için hazırlanan başka ilgili politikalarla, standartlarla, prosedür ve talimatlarla desteklenmiştir. Şirketin doküman sistemi üzerinden yayınlanan iç dokümanlar izlenebilir.

BİLGİ GÜVENLİĞİ POLİTİKASI GÖZDEN GEÇİRME

Şirkette bilgi güvenliğinin sağlanması için, uygulamaya konulan kurallar ve alınan önlemlerin uygulanabilirlik ve etkinlik açılarından kontrol edilmesi ve gerekli gözden geçirme ve güncellemeleri yapılır. Bilgi Güvenliği Politikası da buna dâhildir.
Bu politika, Bilgi Güvenliği Kurulu tarafından yılda en az 1 defa gözden geçirilir. Yönetmeliklerde veya bilgi güvenliği uygulama süreçlerindeki değişiklikler ve yeni eklenen tesisler için politikanın gözden geçirilmesini ve güncelliğinin korunmasını gerektirir. Gözden geçirilen ve güncellenen politika Doküman Yönetimi Prosedürü doğrultusunda onaylanır ve ilgili sistemlerde yayınlanır ve duyurulur.