**ICE BİLİŞİM TEKNOLOJİLERİ A.Ş.**
**BİLGİ GÜVENLİĞİ POLİTİKASI**

ICE Bilişim Teknolojileri A.Ş. Bilgi Güvenliği Politikası'nın amacı; kuruluşun faaliyetleri kapsamında oluşturulan, işlenen, saklanan, iletilen ve yönetilen kurumsal bilgiler ile müşterilere, çalışanlara, tedarikçilere, çözüm ortaklarına ve diğer ilgili taraflara ait bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumaktır.

Bu politika ile bilgi güvenliği risklerinin sistematik olarak yönetilmesi, bilgi varlıklarının yetkisiz erişim, kullanım, değiştirme, ifşa, kayıp ve imhaya karşı korunması, elektronik belge hizmetlerinin güvenilir şekilde sunulması, iş sürekliliğinin desteklenmesi ve müşteri güveninin sürdürülmesi amaçlanır.

ICE Bilişim Teknolojileri A.Ş. üst yönetimi, bilgi güvenliğinin kuruluşun hizmet kalitesi, müşteri memnuniyeti, yasal yükümlülükleri, iş sürekliliği ve kurumsal itibarı açısından önemini kabul eder; Bilgi Güvenliği Yönetim Sisteminin uygulanmasını, sürdürülmesini ve sürekli iyileştirilmesini destekler.

Bu politika; ICE Bilişim Teknolojileri A.Ş.'nin Bilgi Güvenliği Yönetim Sistemi (BGYS) kapsamındaki faaliyetlerini, süreçlerini, bilgi varlıklarını, bilgi teknolojileri altyapısını ve bu varlıklara erişimi bulunan çalışanları, yöneticileri, danışmanları, yetkilendirilmiş dış hizmet sağlayıcılarını ve diğer ilgili tarafları kapsar. Politika kapsamındaki başlıca faaliyetler şunlardır:

- e-Fatura, e-Arşiv Fatura, e-Defter, e-İrsaliye ve e-Saklama hizmetleri,
- Bulut bilişim hizmetleri ve ilgili bilgi teknolojileri altyapısı,
- Telekomünikasyon ürün ve hizmetleri,
- KDV iade ve ilgili danışmanlık faaliyetleri,
- Müşteri, çalışan, tedarikçi ve iş ortaklarına ait bilgilerin işlenmesi,
- Elektronik kayıtların oluşturulması, iletilmesi, saklanması, arşivlenmesi ve gerektiğinde geri alınması,
- Kurumsal sistemlerin, uygulamaların, ağların, kullanıcı hesaplarının ve bilgi varlıklarının yönetimi,
- Dış veri merkezi, bulut bilişim, internet ve telekomünikasyon hizmet sağlayıcılarıyla ilişkili süreçler,
- Bilgi güvenliğini, hizmet sürekliliğini ve müşteri hizmetlerini etkileyebilecek iç ve dış bağımlılıklar.

Uygulama sınırları, BGYS kapsam dokümanında, süreç tanımlarında ve ilgili dokümante edilmiş bilgilerde belirlenir. Dış hizmet sağlayıcılarından alınan hizmetler, kuruluşun sorumluluklarını ve hizmetlerin güvenliğini etkilediği ölçüde risk değerlendirmelerine ve ilgili kontrol faaliyetlerine dâhil edilir.

**TEMEL İLKELERİMİZ**

ICE Bilişim Teknolojileri A.Ş. bilgi güvenliği faaliyetlerini aşağıdaki temel ilkeler doğrultusunda yürütür.

**Gizlilik:** Bilgilere yalnızca yetkili kişi ve sistemlerin, görevleri ve yetkileri kapsamında erişmesini sağlamak.

**Bütünlük:** Bilgilerin doğruluğunu, eksiksizliğini ve yetkisiz veya hatalı değişikliklere karşı korunmasını sağlamak.

**Erişilebilirlik:** Yetkili kullanıcıların ihtiyaç duydukları bilgi ve hizmetlere, belirlenen gereksinimler ve kabul edilen risk seviyeleri doğrultusunda erişebilmesini desteklemek.

**Hesap verebilirlik ve izlenebilirlik:** Bilgi varlıklarına erişimlerin ve kritik işlemlerin, risk ve teknik imkânlarla orantılı şekilde izlenebilmesini ve gerektiğinde incelenebilmesini desteklemek.

**Risk temelli yaklaşım:** Bilgi güvenliği risklerini belirlemek, analiz etmek, değerlendirmek, uygun kontrolleri seçmek ve riskleri kuruluş tarafından kabul edilen ölçütler doğrultusunda yönetmek.

**Asgari yetki ve görevle sınırlı erişim:** Kullanıcılara yalnızca görevlerini yerine getirmek için ihtiyaç duydukları erişim haklarını vermek.

**Sürekli iyileştirme:** Bilgi güvenliği performansını, riskleri, olayları, denetim sonuçlarını ve değişen gereksinimleri dikkate alarak yönetim sistemini geliştirmek.

**BİLGİ GÜVENLİĞİ TAAHHÜTLERİMİZ**

ICE Bilişim Teknolojileri A.Ş. üst yönetimi olarak aşağıdaki konularda taahhütte bulunuruz.

**Yasal ve sözleşmesel şartlara uyum**

Bilgi güvenliği, kişisel verilerin korunması, elektronik belge hizmetleri ve faaliyetlerimizle ilişkili diğer konularda uygulanabilir yasal ve düzenleyici şartların, müşteri sözleşmelerinin, hizmet taahhütlerinin ve diğer bağlayıcı gerekliliklerin belirlenmesini ve izlenmesini destekleriz. İlgili şartların süreçlere yansıtılmasını, sorumlulukların belirlenmesini ve uyumun değerlendirilmesini esas alırız. Yasal yükümlülükler ve sözleşmesel bildirim gereklilikleri, uygulanabilir oldukları ölçüde ilgili prosedür ve süreçlerde ele alınır.

**Bilgi varlıklarının envanteri, sahipliği ve sınıflandırılması**

Kuruluşumuzun sahip olduğu veya sorumluluğunu üstlendiği bilgi varlıklarının belirlenmesini, envanterlerinin oluşturulmasını ve güncel tutulmasını esas alırız. Bilgi varlıkları; iş süreçleri, müşteri gereksinimleri, gizlilik, bütünlük, erişilebilirlik, yasal yükümlülükler ve olası kayıp veya kesintilerin etkileri dikkate alınarak değerlendirilir. Uygun olduğu ölçüde bilgi varlıklarının sahibi, kullanım amacı, bulunduğu ortam, erişim yetkileri ve korunma gereksinimleri tanımlanır. Bilgilerin hassasiyetine ve kullanım amacına uygun sınıflandırma kurallarının oluşturulmasını; saklama, paylaşma, aktarma, erişim ve imha işlemlerinin belirlenen kurallara göre yürütülmesini destekleriz.

**Erişim kontrolü ve kullanıcı sorumlulukları**

Bilgi sistemlerine erişimlerin yetkilendirilmesini, erişim haklarının görev ve sorumluluklarla uyumlu biçimde sınırlandırılmasını ve ihtiyaçlar değiştikçe gözden geçirilmesini esas alırız. Kullanıcı hesaplarının, parolaların, ayrıcalıklı hesapların, uzaktan erişimlerin ve hizmet hesaplarının güvenli yönetimini destekleriz. Kullanıcıların kendilerine tahsis edilen hesapları yalnızca yetkileri kapsamında kullanmalarını, erişim bilgilerini başkalarıyla paylaşmamalarını ve bilgi güvenliği ihlali şüphesini gecikmeden bildirmelerini bekleriz. Erişim yetkileri; işe giriş, görev değişikliği, sözleşme değişikliği ve işten ayrılma gibi durumlarda yeniden değerlendirilir. İhtiyaç kalmayan veya yetkisiz hâle gelen erişimlerin uygun şekilde kaldırılması ya da değiştirilmesi sağlanır.

**Görevler ayrılığı ve yetki yönetimi**

Bilgi güvenliği açısından kritik işlemlerde, mümkün ve gerekli olduğu ölçüde, bir işlemin başlatılması, onaylanması, uygulanması ve kontrol edilmesi görevlerinin uygun şekilde ayrıştırılmasını destekleriz. Görevler ayrılığının teknik veya organizasyonel nedenlerle tam olarak sağlanamadığı durumlarda, risk değerlendirmesi sonucunda uygun telafi edici kontrollerin belirlenmesini esas alırız. Ayrıcalıklı erişimler ve kritik sistemlerde yapılan işlemler, risk düzeyi ve teknik imkânlar doğrultusunda sınırlandırılır ve gerektiğinde izlenir.

**Elektronik belge ve müşteri bilgilerinin güvenliği**

e-Fatura, e-Arşiv Fatura, e-Defter, e-İrsaliye ve e-Saklama hizmetleri kapsamında işlenen elektronik belgelerin, işlem kayıtlarının ve müşteri bilgilerinin gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı esas alırız. Bilgilerin doğru müşteri ve işlemle ilişkilendirilmesini, yetkisiz değişikliklerin önlenmesini, güvenli aktarım ve saklama koşullarının değerlendirilmesini ve ilgili kayıtların gerektiğinde izlenebilmesini destekleriz. Elektronik kayıtların oluşturulması, iletilmesi, saklanması, arşivlenmesi, geri alınması ve imhasına ilişkin gereksinimler; hizmetin niteliği, uygulanabilir mevzuat, müşteri sözleşmeleri ve ilgili prosedürler doğrultusunda ele alınır.

**Kişisel verilerin korunması ve gizlilik**

Çalışanlara, müşterilere ve diğer ilgili kişilere ait kişisel verilerin uygulanabilir mevzuat ve sözleşmesel yükümlülükler doğrultusunda işlenmesini ve korunmasını esas alırız. Kişisel verilere erişimin görev ve yetki gereksinimleriyle sınırlandırılmasını; verilerin yetkisiz açıklanması, aktarılması, kaybolması veya uygunsuz şekilde kullanılmasına karşı uygun teknik ve idari önlemlerin belirlenmesini destekleriz. Kişisel verilerin saklanması, aktarılması, erişimi ve imhasına ilişkin gereksinimler ilgili süreçler kapsamında değerlendirilir. Kişisel veri ihlali şüphesi bulunan durumlar, bilgi güvenliği olay yönetimi ve uygulanabilir bildirim yükümlülükleri çerçevesinde ele alınır.

**Siber güvenlik ve zararlı yazılımlardan korunma**

Bilgi sistemlerini kötü amaçlı yazılımlar, kimlik avı, fidye yazılımları, yetkisiz erişim, hizmet dışı bırakma saldırıları, güvenlik açıkları ve diğer siber tehditlere karşı korumak amacıyla risk temelli teknik ve idari kontrollerin belirlenmesini destekleriz. Sistemlerin ve uygulamaların güvenli yapılandırılması, güvenlik güncellemelerinin değerlendirilmesi, zararlı yazılımlardan korunma, ağ güvenliği, güvenlik olaylarının tespiti ve gerekli müdahale faaliyetlerinin yürütülmesini esas alırız. Güvenlik açıkları ve tehditler, hizmetlerin ve bilgi varlıklarının kritiklik düzeyine göre değerlendirilir. Tespit edilen riskler için uygun iyileştirme ve takip faaliyetleri planlanır.

**Şifreleme ve kriptografik anahtarların korunması**

Bilgilerin hassasiyeti, aktarım ortamı, saklama koşulları ve risk düzeyi dikkate alınarak şifreleme yöntemlerine ihtiyaç olup olmadığının değerlendirilmesini esas alırız. Şifreleme kullanılan durumlarda, kriptografik anahtarların ve ilgili erişim bilgilerinin yetkisiz erişime, kayba, değişikliğe ve uygunsuz kullanıma karşı korunmasına yönelik kuralların belirlenmesini destekleriz.

Şifreleme yöntemleri ve anahtar yönetimi; ilgili sistemlerin teknik olanakları, hizmet sağlayıcıların sorumlulukları, sözleşmesel gereksinimler ve uygulanabilir standartlar dikkate alınarak yönetilir.

**Mobil cihazlar ve taşınabilir ortamların güvenliği**

Kurumsal bilgilere mobil cihazlar veya taşınabilir veri ortamları üzerinden erişilmesi ya da bu ortamlarda bilgi saklanması durumunda, ilgili risklerin değerlendirilmesini ve uygun koruma tedbirlerinin belirlenmesini esas alırız. Kurumsal bilgilerin yetkisiz cihazlara, kişisel e-posta hesaplarına veya onaylanmamış bulut hizmetlerine aktarılmasının önlenmesini destekleriz. Taşınabilir ortamların kullanımı, bilgi aktarımı, kayıp veya çalıntı durumlarının bildirilmesi ve güvenli imhasına ilişkin kurallar ilgili prosedürlerde tanımlanır.

**Yazılım geliştirme, test ve üretim ortamlarının güvenliği**

Kuruluş bünyesinde yazılım geliştirme, uygulama değişikliği, entegrasyon veya bakım faaliyetleri yürütülmesi durumunda, bilgi güvenliği gereksinimlerinin ilgili yaşam döngüsü aşamalarında dikkate alınmasını esas alırız. Uygulanabilir olduğu ölçüde geliştirme, test ve üretim ortamlarının ayrıştırılmasını; gerçek müşteri verilerinin test ortamlarında kullanımının risk değerlendirmesine tabi tutulmasını; değişikliklerin uygun şekilde yetkilendirilmesini, test edilmesini ve kontrollü olarak devreye alınmasını destekleriz.

Yazılım geliştirme veya bakım hizmetlerinin dışarıdan alınması hâlinde, ilgili güvenlik gereksinimleri ve sorumluluklar tedarikçi yönetimi kapsamında değerlendirilir.

**Fiziksel ve çevresel güvenlik**

Bilgi varlıklarının bulunduğu çalışma alanları, sistem odaları, ekipmanlar ve ilgili fiziksel ortamların güvenliğini etkileyebilecek risklerin değerlendirilmesini destekleriz. Yetkisiz fiziksel erişim, ekipman kaybı veya hasarı, yangın, su baskını, aşırı sıcaklık, elektrik kesintisi ve benzeri olayların bilgi varlıkları ve hizmetler üzerindeki etkileri dikkate alınır. Dış veri merkezi ve bulut hizmet sağlayıcılarının fiziksel güvenlik kontrolleri, hizmet sözleşmeleri ve sağlayıcıların sorumlulukları çerçevesinde değerlendirilir. Kuruluşun doğrudan kontrolünde olmayan fiziksel güvenlik tedbirleri bakımından, uygun güvence ve bilgi edinme mekanizmalarının değerlendirilmesini esas alırız.

**Dış hizmet sağlayıcıları, bulut ve veri merkezi güvenliği**

Kuruluşumuzun hizmet sunumunda yararlandığı dış veri merkezi, bulut bilişim, internet, telekomünikasyon hizmet sağlayıcıları ve diğer tedarikçilerin bilgi güvenliği ve hizmet sürekliliği üzerindeki etkilerini dikkate alırız. Tedarikçi seçimi ve hizmet ilişkisinin yönetiminde, hizmetin niteliği ve risk düzeyiyle orantılı güvenlik gereksinimlerinin, erişim yetkilerinin, sorumlulukların, hizmet sürekliliği beklentilerinin ve sözleşmesel yükümlülüklerin belirlenmesini destekleriz. Dış hizmet sağlayıcılarından kaynaklanabilecek kesinti, veri kaybı, yetkisiz erişim, güvenlik açığı ve hizmet güvenliği riskleri değerlendirilir. Hizmet sağlayıcıların performansı, ilgili sözleşmeler, hizmet gereksinimleri ve uygulanabilir kontrol mekanizmaları doğrultusunda izlenir ve gerektiğinde yeniden değerlendirilir.

Kuruluşumuzun kritik hizmetlerinde dış veri merkezi veya bulut altyapısına bağımlılığı bulunduğu dikkate alınarak, hizmet sağlayıcı kaynaklı kesintilerin ve erişilebilirlik sorunlarının iş sürekliliği üzerindeki etkilerinin değerlendirilmesini esas alırız.

**Bilgi güvenliği olaylarının yönetimi**

Bilgi güvenliği olaylarının ve olay şüphelerinin zamanında bildirilmesini, değerlendirilmesini, kayıt altına alınmasını ve uygun şekilde ele alınmasını destekleriz. Olayların müşteri verileri, elektronik belge hizmetleri, kurumsal sistemler ve diğer kritik faaliyetler üzerindeki etkileri değerlendirilir. Gerekli durumlarda ilgili teknik ekipler, yönetim, dış hizmet sağlayıcıları, müşteriler ve diğer yetkili taraflarla koordinasyon sağlanır.

Olayların sınıflandırılması, önceliklendirilmesi, müdahalesi, kayıtlarının korunması ve sonuçlarının değerlendirilmesi ilgili prosedürler kapsamında yürütülür. Yasal veya sözleşmesel bildirim gerektiren durumlarda, uygulanabilir yükümlülükler dikkate alınır.
Olaylardan elde edilen sonuçların tekrarın önlenmesi, risklerin azaltılması ve yönetim sisteminin iyileştirilmesi amacıyla kullanılmasını esas alırız.

**İş sürekliliği ve BT hizmetlerinin devamlılığı**

Bilgi güvenliği ile iş sürekliliği ve BT hizmet yönetimi arasındaki ilişkiyi dikkate alırız. Kritik bilgi varlıklarının ve hizmetlerin kesintiye uğramasına yol açabilecek risklerin belirlenmesini; uygun hazırlık, müdahale, kurtarma ve iyileştirme düzenlemelerinin planlanmasını destekleriz. Bilgi güvenliği olayları, sistem arızaları, dış hizmet sağlayıcı kesintileri, elektrik ve iletişim kesintileri, veri kaybı ve benzeri durumların hizmetlerimiz üzerindeki etkileri değerlendirilir. Kurtarma öncelikleri, sorumluluklar ve uygulanabilir süreklilik gereksinimleri ilgili iş sürekliliği ve BT hizmet yönetimi süreçleri kapsamında ele alınır. Yedekleme, geri yükleme ve kurtarma düzenlemeleri; hizmet gereksinimleri, risk değerlendirmeleri, teknik olanaklar ve dış hizmet sağlayıcılarla yapılan düzenlemeler dikkate alınarak belirlenir. Uygun olduğu durumlarda kurtarma faaliyetlerinin etkinliği test edilir veya doğrulanır.

**İklim değişikliği ve çevresel riskler**

İklim değişikliğinin kuruluşumuzun faaliyetleri ve bilgi güvenliği üzerinde ilgili olabilecek etkilerini kuruluş bağlamı ve risk değerlendirmeleri kapsamında dikkate alırız. Aşırı sıcaklık, sel, fırtına, yangın, elektrik kesintisi ve benzeri çevresel olayların veri merkezi, bulut bilişim, telekomünikasyon altyapısı, bilgi sistemleri ve hizmetlerin erişilebilirliği üzerindeki olası etkilerini değerlendiririz.
İklim kaynaklı risklerin önemli bulunması durumunda, bunlara yönelik uygun önlemlerin ve hizmet sürekliliği düzenlemelerinin belirlenmesini destekleriz. Dış hizmet sağlayıcılarının bu risklerden etkilenme olasılığı da gerekli görülen durumlarda değerlendirmeye dâhil edilir.

**İnsan kaynağı, farkındalık ve yetkinlik**

Çalışanların ve bilgi varlıklarına erişimi bulunan diğer ilgili kişilerin bilgi güvenliği sorumluluklarını anlamalarını, gerekli farkındalık ve yetkinlikleri kazanmalarını ve güvenli çalışma kurallarına uymalarını destekleriz. Bilgi güvenliği gereksinimlerinin işe giriş, görev değişikliği ve işten ayrılma süreçlerinde dikkate alınmasını esas alırız. Eğitim ve farkındalık ihtiyaçları, görevlerin niteliği, erişim düzeyi, riskler ve olaylardan elde edilen sonuçlar doğrultusunda belirlenir. Bilgi güvenliği kurallarının çalışanlar ve ilgili taraflar tarafından anlaşılması ve uygulanması için uygun bilgilendirme, eğitim ve iletişim faaliyetleri planlanır.

**Müşteri memnuniyeti ve şikâyetlerin yönetimi**

Müşterilerden gelen bilgi güvenliği, hizmet kalitesi, erişilebilirlik, veri güvenliği ve hizmet kesintileriyle ilgili bildirim ve şikâyetlerin uygun, tarafsız, gizliliğe saygılı ve izlenebilir şekilde ele alınmasını destekleriz. Şikâyetlerin alınması, değerlendirilmesi, ilgili sorumlulara iletilmesi, çözüm sürecinin izlenmesi ve sonuçların bildirilmesi ilgili süreçler kapsamında yürütülür. Şikâyetlerden elde edilen sonuçların hizmet kalitesinin, müşteri memnuniyetinin ve bilgi güvenliği uygulamalarının iyileştirilmesinde kullanılmasını esas alırız.

**Risklerin ve fırsatların yönetimi**

Bilgi güvenliği risklerini; bilgi varlıkları, süreçler, teknolojik gelişmeler, tehditler, zafiyetler, müşteri gereksinimleri, yasal yükümlülükler ve dış hizmet sağlayıcılarına bağımlılıklar doğrultusunda değerlendiririz. Risklerin analiz edilmesi, değerlendirilmesi ve ele alınmasına yönelik kontrollerin belirlenmesini, uygulanmasını ve etkinliğinin değerlendirilmesini destekleriz. Risk değerlendirmesi ve risk işleme çalışmaları; önemli değişiklikler, olaylar, denetim sonuçları ve yeni tehditler doğrultusunda gerektiğinde güncellenir.
Bilgi güvenliğiyle ilgili fırsatlar; teknolojik gelişmeler, süreç iyileştirmeleri, güvenlik kontrollerinin geliştirilmesi ve hizmet sürekliliğinin güçlendirilmesi açısından değerlendirilir.

**Bilgi güvenliği hedefleri ve performansın değerlendirilmesi**

Bilgi güvenliği hedeflerini bu politika ve kuruluşun stratejik yönüyle uyumlu şekilde belirlemeyi esas alırız. Hedeflerin mümkün olduğu ölçüde ölçülebilir, izlenebilir ve ilgili risklerle bağlantılı olmasını destekleriz. Performans değerlendirmelerinde, uygulanabilir olduğu ölçüde aşağıdaki göstergeler dikkate alınabilir:

- Bilgi güvenliği olaylarının sayısı, türü ve sonuçları,
- Risk değerlendirmeleri ve risk işleme faaliyetlerinin durumu,
- Erişim yetkilerinin gözden geçirilmesi ve uygunsuz erişimlerin giderilmesi,
- Bilgi güvenliği eğitim ve farkındalık faaliyetlerinin gerçekleşme durumu,
- İç denetim bulguları ve düzeltici faaliyetlerin durumu,
- Dış hizmet sağlayıcılarının hizmet ve güvenlik performansı,
- İş sürekliliği, yedekleme ve kurtarma çalışmalarının sonuçları,
- Müşteri şikâyetleri ve hizmet güvenliğini etkileyen bildirimler.

Hedefler ve performans sonuçları uygun aralıklarla değerlendirilir; gerekli görülen durumlarda iyileştirme faaliyetleri planlanır.

**İç denetim, uygunsuzluklar ve sürekli iyileştirme**

Bilgi Güvenliği Yönetim Sisteminin uygunluğunu, yeterliliğini ve etkinliğini değerlendirmek amacıyla planlı aralıklarla iç denetimlerin gerçekleştirilmesini destekleriz. Denetim sonuçları, olay kayıtları, risk değerlendirmeleri, performans göstergeleri, müşteri geri bildirimleri ve dış hizmet sağlayıcılarının performansı iyileştirme ihtiyaçlarının belirlenmesinde dikkate alınır. Tespit edilen uygunsuzlukların nedenlerinin değerlendirilmesini, gerekli düzeltici faaliyetlerin planlanmasını ve sonuçlarının izlenmesini esas alırız.
Bilgi güvenliği yönetim sisteminin sürekli iyileştirilmesi için gerekli faaliyetleri destekleriz.

**Politika ihlalleri ve istisnaların yönetimi**

Bu politikaya veya ilgili bilgi güvenliği kurallarına aykırı durumlar değerlendirilir, gerekli olduğunda kayıt altına alınır ve riskin etkisine uygun şekilde ele alınır. İhlallerin nedenleri ve sonuçları dikkate alınarak erişimlerin sınırlandırılması, düzeltici faaliyetlerin başlatılması veya ilgili taraflarla koordinasyon sağlanması gibi uygun önlemler belirlenebilir. Politika gerekliliklerinden istisna verilmesi gereken durumlarda, istisnanın gerekçesi, kapsamı, süresi, oluşturduğu riskler ve gerekli onaylar değerlendirilir. İstisnalar kontrolsüz ve süresiz

uygulamalara dönüşmeyecek şekilde yönetilir. Çalışanlarla ilgili işlemler, yürürlükteki mevzuat ve kuruluşun ilgili düzenlemeleri çerçevesinde yürütülür.

**DİĞER YÖNETİM SİSTEMLERİYLE İLİŞKİ**

Bilgi güvenliği faaliyetlerimizi, kuruluşumuzda uygulanan diğer yönetim sistemleriyle bütünleşik bir yaklaşımla yürütmeyi esas alırız.

- **ISO 9001 – Kalite Yönetim Sistemi:** Hizmetlerin uygunluğu, müşteri şartları, süreç performansı, müşteri memnuniyeti ve sürekli iyileştirme.
- **ISO/IEC 27001 – Bilgi Güvenliği Yönetim Sistemi:** Bilgi güvenliği risklerinin yönetimi, güvenlik kontrolleri, performansın izlenmesi ve BGYS'nin sürekli iyileştirilmesi.
- **ISO 22301 – İş Sürekliliği Yönetim Sistemi:** Kritik faaliyetlerin sürekliliği, kesintilere hazırlık, kurtarma ve hizmet sağlayıcı bağımlılıkları.
- **ISO/IEC 20000-1 – BT Hizmet Yönetim Sistemi:** BT hizmetlerinin planlanması, sunulması, izlenmesi, olay yönetimi ve hizmet iyileştirme.
- **ISO 10002 – Müşteri Memnuniyeti ve Şikâyetlerin Ele Alınması:** Müşteri şikâyetlerinin sistematik, tarafsız, gizliliğe saygılı ve izlenebilir şekilde ele alınması.

İlgili yönetim sistemlerinin ortak süreçleri, riskleri, hedefleri ve iyileştirme faaliyetleri mümkün olduğu ölçüde koordineli biçimde yönetilir.

**GÖREV VE SORUMLULUKLAR**

**Üst Yönetim**

- Bilgi Güvenliği Politikasını onaylar ve kuruluşun amacı ile stratejik yönüyle uyumunu gözetir.
- Bilgi güvenliği için gerekli kaynak ve sorumlulukların değerlendirilmesini destekler.
- Bilgi güvenliği hedeflerini ve yönetim sistemi performansını uygun aralıklarla gözden geçirir.
- Bilgi güvenliğinin kuruluş genelinde benimsenmesini ve sürekli iyileştirilmesini destekler.

**BGYS Sorumlusu ve ilgili yönetim rolleri**

- BGYS kapsamındaki çalışmaların koordinasyonuna katkı sağlar.
- Bilgi güvenliği risklerinin, kontrollerin ve hedeflerin izlenmesini koordine eder.
- Olaylar, denetimler, performans ve iyileştirme ihtiyaçları hakkında ilgili yönetim rollerine bilgi verir.
- Politikanın ve ilgili dokümante edilmiş bilgilerin gözden geçirilmesine katkı sağlar.

**Bölüm yöneticileri**

- Sorumluluk alanlarındaki bilgi varlıklarının ve güvenlik gereksinimlerinin belirlenmesine katkı sağlar.
- Görev ve yetkilere uygun erişimlerin yönetilmesini destekler.
- Bilgi güvenliği kurallarının ilgili süreçlerde uygulanmasını ve uygunsuzlukların bildirilmesini sağlar.

**Çalışanlar ve diğer yetkili kullanıcılar**

- Bu politikaya ve ilgili prosedürlere uyar.
- Kendilerine verilen erişim yetkilerini yalnızca görevleri kapsamında kullanır.
- Bilgi varlıklarını korur ve güvenlik olaylarını veya şüpheli durumları gecikmeden bildirir.
- Yetkisiz paylaşım, erişim ve kullanım faaliyetlerinden kaçınır.

**Dış hizmet sağlayıcıları**

- Sözleşmelerinde ve ilgili düzenlemelerde tanımlanan bilgi güvenliği sorumluluklarına uyar.
- Kendilerine verilen erişimleri yalnızca yetkilendirildikleri amaçlarla kullanır.
- Bilgi güvenliğini veya hizmet sürekliliğini etkileyebilecek olayları, ilgili sözleşme ve prosedürlerde belirlenen kurallar doğrultusunda bildirir.

**POLİTİKANIN DUYURULMASI VE GÖZDEN GEÇİRİLMESİ**

Bu politika üst yönetim tarafından onaylanır, dokümante edilmiş bilgi olarak korunur ve ilgili çalışanlara duyurulur. Diğer ilgili taraflarla paylaşılması; kuruluşun ihtiyaçları, sözleşmesel yükümlülükleri ve uygulanabilir şartlar doğrultusunda değerlendirilir.

Politika **en az yılda bir kez** gözden geçirilir. Ayrıca aşağıdaki durumlarda gerekli görüldüğünde gözden geçirme yapılır:

- Kuruluşun faaliyetlerinde veya BGYS kapsamındaki süreçlerinde önemli değişiklikler meydana gelmesi,
- Bilgi teknolojileri altyapısında, bulut hizmetlerinde veya dış veri merkezi bağımlılıklarında önemli değişiklikler olması,
- Yeni tehditlerin, güvenlik açıklarının veya önemli bilgi güvenliği olaylarının ortaya çıkması,
- Yasal, düzenleyici veya sözleşmesel gerekliliklerin değişmesi,
- İç denetim, yönetimin gözden geçirmesi veya performans değerlendirmeleri sonucunda güncelleme ihtiyacı belirlenmesi,
- İlgili tarafların gereksinimlerinde veya kuruluşun risklerinde önemli değişiklikler oluşması.

Gerekli güncellemeler doküman kontrol kurallarına uygun olarak gerçekleştirilir ve ilgili taraflara duyurulur.

YÖNETİM KURULU BAŞKANI Günay CİCİOĞLU 30/04/2026 (R03)