BİLGİ GÜVENLİĞİ POLİTİKASI

Kapsam; Söz konusu politika şirketin tüm çalışanlarını, stajyerlerini, geçici personelini, danışmanlarını, dış kaynak personelini, hizmet sağlayıcılarını, ziyaretçilerini ve şirket bilgi sistemlerine erişen tüm iç/dış kullanıcıları kapsamaktadır.

Politika; şirket bünyesinde bulunan veya şirket adına kullanılan tüm bilgi teknolojileri varlıklarını (sunucular, masaüstü ve dizüstü bilgisayarlar, yazıcılar, akıllı telefonlar, tabletler ve diğer mobil cihazlar, ağ cihazları, kablolu/kablosuz ağ altyapısı, veri depolama sistemleri, yedekleme sistemleri, bulut hizmetleri, uygulama ve yazılım envanteri, mesajlaşma ve e-posta sistemleri ile internet erişim altyapısı ve ilgili tüm BT hizmetlerini) kapsar.

Ayrıca, şirket tarafından üretilen, işlenen, saklanan, iletilen veya yönetilen tüm bilgi varlıklarını (kişisel veriler dahil kurumsal bilgi ve dokümantasyon), bu bilgilerin bulunduğu tüm fiziksel lokasyonları (ofisler, veri merkezleri, arşiv alanları vb.), şirket iç kaynaklarına yerel veya uzaktan erişim sağlayan tüm kullanıcı ve cihazları, veri yedekleme süreçlerini ve ilgili donanımları, insan kaynakları süreçleri kapsamında yer alan çalışan ve stajyerleri, bilgi güvenliği ihlallerine ilişkin tüm süreçleri, bu süreçlerle ilişkili mevzuat düzenlemelerini, sözleşmeleri ve özellikle 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamındaki yükümlülükleri de kapsamaktadır.

Bilgi Güvenliğinin Yönetilmesi

- **Bilgi Güvenliği İlkeleri**

✓ Şirket bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişen tüm personel:
✓ Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde Şirkete ait bilginin gizliliğini sağlamalı,
✓ Kritiklik düzeylerine göre işlediği bilgiyi yedeklemeli,
✓ Şirket içi bilgi kaynakları (duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletmemelidir.
✓ Şirket bilişim kaynakları mevzuata aykırı faaliyetler amacıyla kullanılmamalıdır.

- **Politikanın İhlali ve Yaptırımları**

✓ Bilgi güvenliği politikası, prosedür ve talimatlarına uyulmaması halinde, Şirket personelin imzaladığı Gizlilik Sözleşmesi cezai şart maddesi uygulanacaktır.

BT Varlıkları Yönetim Politikası

✓ Bilgi teknolojileri envanteri sadece ilgili iş aktivitelerinde atama ve/veya yetkilendirme şeklinde kullanılmalıdır.
✓ Zimmet sahibi kullanıcılar (zimmet formu imzaladığı cihazlar için) BT envanterinin korunmasından ve doğru şekilde kullanılmasından sorumludur.
✓ Masaüstü ve dizüstü bilgisayarlar kullanılmadıkları durumda fiziksel güvenlik altına alınmalıdır. Söz konusu cihazların üstünde gizli bilgiler saklandığı durumda otomatik araçlar kullanılarak bilgiler geri döndürülemeyecek şekilde silinmelidir.
✓ Kullanıcılar kendilerine zimmetlenen varlıkları temiz kullanmak ve kazalardan korumak veya uygunsuz şekilde kullanmamakla yükümlüdür.
✓ BT envanterinde sadece yetkilendirilen BT teknik personeli yapılandırma değişikliği yapmakla yetkilidir. İfade edilen haricindeki kullanıcıların yazılım ve donanım değişikliği gerçekleştirmesi yasaktır.
✓ Dizüstü, akıllı telefon ve tablet benzeri cihazlar çalınmaya karşı korunması sorumluluğu zimmeti yapılan personelin yükümlülüğündedir.
✓ Dizüstü, akıllı telefon ve tablet benzeri taşınabilir cihazlardaki veriler çalınmaya karşı şifreleme ve veri imha yöntemleriyle korunmalıdır.

Kullanıcı ve Erişim Kontrol Yönetim Politikası

✓ Gizli bilgi taşıyan sistemler iki faktörlü (şifre+SMS) erişim kontrolü ile korunmalıdır.
✓ Kaynaklara erişim kişi bazlı yetkilendirme, grup bazlı yetkilendirme gerçekleştirilir.
✓ Erişim hakları yetkili kişi tarafından merkezi olarak tanımlanır ve yönetilir.
✓ Görevleri veya işleri değişen veya kurumdan ayrılan kullanıcıların erişim hakları aynı iş günü içerisinde kullanıma kapatılır.

E-Posta Yönetim Politikası

- ✓ Şirket tarafından kullanıcılara atanan e-posta adresleri ve mesaj alanları sadece iş amaçlı kullanılmalıdır. Kişisel e-posta adreslerinin kullanımı yasaktır.
- ✓ Şirket kaynakları kullanılarak yetkisiz reklam, iş harici mesajlaşma, spam, politik kampanya ve iş süreçlerine aykırı her türlü kullanım yasaktır.
- ✓ Şirket e-posta sistemleri, saldırgan, ırkçı, müstehcen veya kanun ve yönetmeliklere aykırı amaçlarda kullanılmamalıdır.
- ✓ Şirket e-posta sisteminin kullanımı personel kurumda çalışırken aktif olmalıdır. İlişiğin kesilmesi ve işten ayrılma durumlarında kullanıcı hesapları pasifleştirilmelidir.
- ✓ Kullanıcılar e-posta sistemlerini kendilerine atanmış benzersiz kullanıcılar aracılığıyla giriş yapmalıdır.
- ✓ Kurumsal e-posta adreslerine erişimler güçlü şifrelerle korunmalıdır.
- ✓ Virüs ve zararlı yazılımları tespit eden sistemler kullanıcı PC ve sunucuların en yüksek eposta güvenliğini sağlayacak şekilde konumlandırılmalıdır.
- ✓ E-postaların Şirket dışındaki e-posta adreslerine yönlendirilmesi yasaktır.

İnternet Erişim Yönetim Politikası

- ✓ Tüm kullanıcılar kısıtlı şekilde internete erişebilir. Şirket tarafından aşağıdaki yasaya göre kısıtlanan web siteleri Ağ Geçidi uygulamasıyla kontrol edilmektedir.
- ✓ 5651 numaralı "İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında" konulu yönetmelik kapsamında yasaklanan kategorilerdeki web sitelerine giriş engellenmelidir. Bu çerçevede 26.9.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nda yer alan aşağıdaki kanun maddelerine aykırı siteler yasaklanacaktır:
  * İntihara yönlendirme (madde 84)
  * Çocukların cinsel istismarı (madde 103, birinci fıkra)
  * Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190)
  * Sağlık için tehlikeli madde temini (madde 194)
  * Müstehcenlik (madde 226)
  * Fuhuş (madde 227)
  * Kumar oynanması için yer ve imkân sağlama (madde 228)
  * 25.7.1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun
- ✓ Kullanıcılar, Şirket tarafından sunulmuş olan internet erişim, elektronik ve anlık mesajlaşma hizmetini şirketin belirlediği politikalar uyarınca iş amaçlı olarak kullanmalıdır.
- ✓ Kullanıcılar internet erişimlerinde Şirket kültür ve saygınlığına uygun hareket etmekle yükümlüdür.

Zararlı Yazılımlara Karşı Korunma Yönetim Politikası

- ✓ Şirkette olan tüm bilgisayar, notebook ve tabletlerde lisanslı antivirüs sistem kullanılmalı ve en son sürümüyle güncellenmelidir.
- ✓ Şirketin ağına bağlanan tüm bilgisayar ve cihazlarda gerçek zamanlı koruma sağlayan antivirüs kurulu olması zorunlu olmakla beraber virüs koruma devre dışı bırakılamaz.
- ✓ Şirketin ait sunucu ve bilgisayarlar merkezi olarak yönetilen ve onaylı antivirüs sistemini kullanmalıdır.
- ✓ Antivirüs uygulaması düzenli ve otomatik olarak virüs güncellemelerini gerçekleştirmelidir.
- ✓ Taşınabilir bilgi depolama ortamlarında (CD/DVD, flaş bellek, harici disk, vb.) bağlantı kısıtlanmıştır.
- ✓ Tüm bilgisayarlar ve ortamlar, belirlenmiş zaman aralıklarında otomatik olarak taranmalıdır.
- ✓ Kötü niyetli yazılım ve zararlı/mobil kod içerebilecek dosya türleri ve dosya türlerini barındıran kaynaklar çalıştırılmadan önce mutlaka antivirüs sisteminde taranarak güvenli olduğuna emin olduktan sonra dosya açılmalıdır.

KVKK Uyumunun Sağlanması Politikası

- ✓ Kişisel verilerin Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenmesi sağlanmalıdır.
- ✓ İlgili kişinin haklarını korunmalıdır; Kişisel Verileri hukuka aykırı olarak işlenmesi ve erişilmesin önlemelidir, kişisel verilerin muhafazası sağlanmalıdır.
- ✓ Kişisel Veri Envanteri oluşturulmalıdır.
- ✓ Kişisel verilerin yurtdışına aktarılması, silinmesi, yok edilmesi veya anonim hale getirilmesi kanuna uygun olarak yönetilmelidir.
- ✓ Mevcut sözleşmeler (Çalışan, Katılımcı, Müşteri, Taşeron vb.) kanunla uyumlu hale getirilmelidir.
- ✓ Veri Sahibini aydınlatma ve açık rıza alma yükümlülükleri yerine getirilmelidir.
- ✓ Veri sahiplerinin başvurularını değerlendirmek ve sonuçlandırma mekanizması olmalıdır.
- ✓ Organizasyon yapısını oluşturulmalıdır.
- ✓ Veri Sorumluları Sicili 'ne (VERBİS) kayıt işlemi yapılmalı ve gerektiğinde güncellenmelidir.

- ✓ Kişisel Veri Güvenliğine sağlanmasına yönelik olarak idari ve teknik tedbirlerin alınması sağlanmalıdır.

Uzaktan Erişim Yönetim Politikası

- ✓ Şirketin iç kaynaklarına dışarıdan erişimlerin gerçekleşmesi için kullanıcının gerekli yetkiye sahip olması gerekmektedir. Dışarıdan erişim talebi bilgi işlem sorumlusunun onayıyla verilir.
- ✓ Şirket iç kaynaklarına güvensiz ağdan erişimler iki faktörlü kimlik doğrulaması sağlayan SSL-VPN aracılığıyla gerçekleştirilir.
- ✓ Ağ tasarımı, dışarıdan gelen trafiği, sadece ağın belirli kısımlarıyla sınırlandıracak ve tanımlı giriş noktalarına yönlendirecek şekilde yapılandırılmalıdır.

Ağ Güvenlik Yönetim Politikası

- ✓ Ağ cihazları (router, hub, bridge, switch ve güvenlik duvarı, vb.) ile ilgili tanımlama ve yapılandırma portlarına sadece yetkili personel şifre kontrolüyle erişim sağlamalıdır.
- ✓ İlk kurulum sonrasında ağ cihazlarındaki, üretici tarafından sağlanan varsayılan parolalar ve parametreler değiştirilmelidir.
- ✓ Kablosuz misafir ağlarında giriş şifreli yapılmalıdır ve şifre Bilgi işlem sorumlusu tarafından verilmelidir.
- ✓ Güvenlik duvarı kuralları, suiistimale açık iletişim protokollerini yasaklayacak şekilde düzenlenmelidir.
- ✓ En az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

Fiziksel Güvenlik Yönetim Politikası

- ✓ Çalışma ortamı ve bina güvenliğine yönelik fiziksel ve çevresel güvenlik kuralları aşağıda maddeler halinde sıralanmıştır.
- ✓ Çalışma ortamı veya bina girişinde, görevli kişinin bulunduğu bir resepsiyon alanı veya girişin kontrol edilmesini sağlayan bir uygulama olmalıdır.
- ✓ Çalışma ortamı veya bina genelinde haftanın 7 günü, günün 24 saati aktif olan alt güvenlik sistemi bulunmalıdır.
- ✓ Ziyaretçilerin kişisel bilgileri, geliş ve ayrılış bilgileri kaydedilmelidir.
- ✓ Çalışma ortamlarında güvenlik kameraları kurulu olmalı, gözetim altında tutulmalı ve kayıtlar geriye dönük saklanmalıdır.
- ✓ Kapı erişim ve kamera sistemleri yetkisiz erişimlere karşı parmak izi / kart okuyucu ile korunmalıdır.
- ✓ Bilgi işlem alanları ile belirlenmiş diğer kritik noktalar toz, ısı, duman, nem ve su sızıntısına karşı detektör koruması altında olup, bu noktalar 7 gün 24 saat kesintisiz izlenerek kontrol altında tutulmalıdır.
- ✓ Çalışma ortamı ve bina yürürlükteki deprem yönetmeliklerine göre inşa edilmiş olmalı veya bina güçlendirmeleri yapılmış olmalıdır.
- ✓ Bilgi sistemi cihazlarının bulunduğu alanlara erişim refakatle ve onaylı şekilde gerçekleştirilmelidir.
- ✓ En az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

Sunucu Güvenlik Yönetim Politikası

- ✓ Sunucu güvenlik yönetimine yönelik fiziksel ve çevresel güvenlik kuralları aşağıda maddeler halinde sıralanmıştır.
- ✓ Sunucularda tanımlanan iş ihtiyacına sunucu görevine uygun şekilde yazılımlar kurulmalıdır.
- ✓ Sunucularda kullanılmayan servis ve portlar kapatılmalıdır.
- ✓ Sunucular düzenli olarak yedeklenmelidir.
- ✓ Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.
- ✓ Sunucular fiziksel ve mantıksal olarak ayrıştırılmış ağlarda kullanım amaçlarına uygun şekilde konumlandırılmalıdır.

Veri Yedekleme Yönetim Politikası

- ✓ Şirketin önemli verilerinin bulunduğu ortak veri klasörü ve veri tabanlarının tamamının yedeği uygun ve düzenli olarak alınmalıdır.
- ✓ Yedekleme işlemlerinin sağlanması için bir yedekleme planı oluşturulmalı ve bu plana göre yedekleme işlemi kesintisiz yapılmalıdır.
- ✓ Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.

İnsan Kaynakları Yönetim Politikası

- ✓ Bilgi güvenliğiyle ilgili görev ve sorumluluklar tanımlanan ve yönetim tarafından onaylanan Gizlilik Sözleşmesi çalışanlara tebliğ edilmelidir.
- ✓ Bilgi güvenliğiyle ilgili görev ve sorumluluklar, şirketin bilgi güvenliği politikalarına uygun davranılmasını, varlıkların korunmasını ve diğer dokümante edilmiş (politika, prosedür, taahhütname, vb.) sorumlulukları kapsamalıdır.
- ✓ Çalışanlara işe başlangıçta imzalatılan Gizlilik Sözleşmesi şirketin bilgi güvenliği yaklaşımını içerecek şekilde hazırlanmalı ve gizli bilgiye erişen tüm çalışanlara imzalatılmalıdır.

- ✓ Şirket tarafından çalışanlara sağlanan cep telefonu, araç, bilgisayar ve benzeri Şirket kaynakları sadece iş amaçlı olarak kullanılmalıdır.
- ✓ İş akdi/hizmet sözleşmesi, sözleşme içeriğinde yer alan kayıt ve koşullara aykırı davranılması halinde Gizlilik Sözleşmesinin ilgili maddeleri uygulanmalıdır.
- ✓ Bilgi güvenliği farkındalığını artırmak amacıyla düzenlenen eğitim, oryantasyon programları sürekli tekrarlanmalıdır. İşe yeni başlayan her personele oryantasyon ve bilgi güvenliği eğitimi verilmelidir.
- ✓ İstifa eden çalışan ve/veya Şirket tarafından ihbar önelini kullandırmak suretiyle iş akdi/hizmet sözleşmesi sona erdirilen çalışanın sahip olduğu tüm erişim yetkileri kaldırılmalıdır. PDKS cihazından erişim yetkileri silinmelidir.
- ✓ Uzun süreli sağlık raporu, doğum ve ücretsiz izin kullanan çalışanların uzaktan erişim yetkileri var ise kapatılmalıdır. Ancak sisteme giriş yetkileri kapatılmamalıdır.
- ✓ İşten ayrılan çalışanın, iş amacıyla kullandığı elektronik ve fiziksel varlıklar (cep telefonu/tablet, dizüstü bilgisayar, vb.) zimmet formu ile geri alınır.

Bilgi Güvenliği İhlali Yönetim Politikası

- ✓ Bilgi güvenliği ihlal olayları şirkete bildirilmeli, Şirket kapsamını ilgilendiren olaylarda DÖF Formu oluşturmalı, 6698 sayılı kanun kapsamında yer alan veri ihlali bildirimlerinde ise “Kişisel Veri İhlal Bildirim Form” u doldurulmalı ve ilgili KVKK süreci başlatılmalıdır.
- ✓ Kullanıcıların kasti olarak gerçekleştirdiği Bilgi güvenliği ihlal olaylarında şirketin ve kullanıcı arasında imzalanan Gizlilik Sözleşmesine bağlı olarak sözleşmesinin ilgili maddesi uygulanmalıdır. Ayrıca bu ihlali gerçekleştirerek kurumu doğrudan ve/veya dolaylı olarak zarara uğratan kişi ve/veya kuruluş aleyhine hukuki yollara başvurma hakkını Şirket saklı tutmaktadır.
- ✓ Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilmelidir.