ÖZEL İTALYAN ANA VE İLKOKULU
BİLGİ SİSTEMLERİ GENEL STANDARTLAR VE GÜVENLİK POLİTİKASI
6.11.2019 / Versiyon No: 1

İÇİNDEKİLER

ÖZEL İTALYAN ANA VE İLKOKULU
BİLGİ SİSTEMLERİ GENEL STANDARTLAR VE GÜVENLİK POLİTİKASI
6.11.2019 / Versiyon No: 1

1. Amaç

Güvenlik, "gizlilik", "bütünlük" ve "erişilebilirlik" olarak isimlendirilen üç unsurdan oluşur. Bu güvenlik öğelerinden herhangi biri zarar görürse kurumsal güvenlik zaafiyeti oluşur.

- *Gizlilik* : Bilginin yetkisiz kişilerin eline geçmemesini,
- *Bütünlük* : Bilginin yetkisiz kişiler tarafından değiştirilmemesini,
- *Erişilebilirlik* : Bilginin ilgili ve yetkili kişilerce ulaşılabilir ve kullanılabilirliğini ifade eder.

Bu politikanın amacı;

1.1. Veri Sorumlusu bünyesinde, ticari ve operasyonel her türlü fiziki veya elektronik ortamlardaki bilgi ve verilerin güvenliği ve gizliliğini sağlamak,
1.2. Veri Sorumlusu'na ait olan tüm elektronik bilgi sistem ekipmanlarının fiziksel emniyetini sağlamak,
1.3. Veri Sorumlusu tarafından genel olarak işlerin yürütülmesi amacıyla her türlü yoldan tedarik edilmiş (satın alma, üretme, ortaklık kurma) elektronik bilgi sistemleri ekipmanı ve bunlarla ilgili hizmet kaynaklarının verimli bir şekilde kullanılmasını sağlamak, kişisel çıkar veya kötü amaçlar için değerlendirilmesini önlemek,
1.4. Veri Sorumlusu bünyesinde kullanılan her türlü elektronik bilgi sistemleri ekipmanı ve bunlarla ilgili hizmet kaynaklarının yasal ve lisanslı olmasını sağlamak,
1.5. Veri Sorumlusu'nun kurumsal kimliğini ve yapısını korumak, kurumsal yapısının gelişmesini desteklemek,
1.6. Yasa ve yönetmeliklere uyumlu olarak bilgi güvenliği süreçlerini yürütmektir.

2. Tanımlar

- *Bilgi Sistemleri* : Verilerin/bilgilerin üzerinde tutulduğu, kaydedildiği, işlendiği, iletildiği, saklandığı elektronik, manyetik, yazılı ve diğer ortamlar ile ekipmanları, sistemleri, kişisel bilgisayarları (PC), sunucuları (server), dizüstü bilgisayarları (laptop, notebook); akıllı telefon, tablet, aktif cihaz, disket, kartuş, CD, DVD, BD medyaları, yedekleme birimleri, telli/telsiz iletişim cihazlarını, router, hub, switch ve modemleri; ağ bağlantılarını ve sistemlerini, faks, yazıcı (printer), fotokopi cihazı gibi ve ayrıca sistemlerle bağlantılı ve bunlara ait tüm yazılım, program, uygulama ve benzerlerini ifade eder.
- *Bilgi Sistemleri Direktörlüğü (BSD)* : Veri Sorumlusu'na destek sunan ve bilgi teknolojileri alanında hizmet veren Veri Sorumlusu iç birimini ifade eder.
- *Bilgi Sistemleri Güvenliği (BSG)* : Veri Sorumlusu'na destek sunan, Bilgi Sistemleri Direktörlüğü'ne bağlı çalışan bilgi sistemleri güvenliğinden sorumlu olan alt birimi ifade eder.
- *Gizli/Değerli Bilgi* : Veri Sorumlusu'nun mülkiyetinde olan ve ticari, maddi, manevi değer taşıyan veya her türlü potansiyel ticari değer taşıyacak veya rekabet unsuru olabilecek bilgileri; Veri Sorumlusu'na özgü yöntemlere, çalışma biçimine, iş hacmine, hazırlanmış veya hazırlanmakta olan projelere ait bilgileri, ticari sırları, her türlü bilgi sistemlerine ait lisansları, altyapı, bilgi / veri toplama, saklama, iletim, erişim yöntemleri de dahil olmak üzere teknik bilgi, bilgi sistemlerindeki güvenlik açıklarını, özel gizli veya güvenlik sistemlerine ait her türlü teknik veya gizli bilgiyi, yazılımları, programları ve kaynak kodlarını, şifreleri, özel yetki parametrelerini, elektronik posta (e-

Commented [AA1]: Arkas Grubu dışındaki iştirakler burada ve politika metni boyunca geçtiği her yerde bu 2 tanım yerine kendi bünyelerinde bu görevleri ifa eden birim veya departmanın ismini ve görev tanımını yazmalıdır.

posta) adreslerini, şirket telefon numaralarını, finansal bilgileri, yeni iş veya hizmet fikirlerini, satış stratejilerini, çözümleri, müşteri liste ve portföylerini, endüstriyel tasarımları, marka / ürün adlarını, kayıt, evrak, resim, çizim, şema, sınai mülkiyet ve telif hakkı kapsamındaki bilgileri, logo, amblem, slogan, elektronik veya diğer ortamlarda üretilen ve kullanılan her çeşit ürün, ekipman vb. bilgileri ifade eder.

- *Hizmet Masası* : Veri Sorumlusu çalışanlarına, bilgi sistemleri kullanımıyla ilgili destek sunan, soru ve sorunların çözümü için ilk başvuruyu kabul eden BSD birimini ifade eder.

Commented [AA2]: Arkas BSD şemsiyesi dışında kalan iştiraklerde bu hizmeti kim sağlıyorsa onun adı ve görev tanımı buraya eklenmelidir. Politika metninde geçen "Hizmet Masası" ifadeleri de buna göre gerekliyse revize edilmelidir.

- *Kanun :* 6698 sayılı Kişisel Verilerin Korunması Kanunu'nu ifade eder. Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları belirleyen ve 24/3/2016 tarihinde kabul edilerek, 7/4/2016 tarihinde yürürlüğe giren kanundur.
- *Kişisel Veri* : Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder. Kişilerin adı, soyadı, doğum tarihi ve doğum yeri, kişinin fiziki, ailevi, ekonomik ve sair özelliklerine ilişkin bilgiler, isim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası gibi veriler kişisel veridir.
- *Özel Nitelikli Kişisel Veri* : Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileridir.
- *Sistem Cihazları* : Sadece yetkili çalışanın müdahale ve yetkili erişiminde/kullanımda bulunabileceği, sistem odaları veya sistem odalarının olmadığı yerlerde belirlenmiş bir alanda/bölgede bulunması gereken, şirketlerin tüm bilgi sistemlerinin, veri iletişim kanallarının kesintisiz çalışmasını sağlayan, altyapısını destekleyen, kritik öneme sahip; tüm türlü bilgi sistemlerini, elektrik ve enerji üretim ve destek cihazları, UPS, jeneratör vb. tüm bu sistemlere ait ekipman, donanım, yazılım, program ve uygulamaları ifade eder.
- *Sistem Erişim Bağlantıları/Oturumları* : Bilgi sistemleri aracılığıyla, etki alanı, ağ alanları ve sistemleri, sunucu sistemlerine belli parametreler, kullanıcı adı/şifresi veya benzeri her türlü yetkili erişim ekipmanlarını kullanarak bağlantı sağlanması, oturum açılması, erişim yapılması vb. (domain/network login/logon, AS400 sign on vb.) eylemleri/durumları ifade eder.
- *Üçüncü Şahıslar* : Veri Sorumlusu dışındaki tüm resmi veya resmi olmayan kurum, şirket, kuruluş, örgüt, kişi veya kişiler.
- *Veri/Bilgi* : Kişisel bilgisayar , sunucu , dizüstü bilgisayar, akıllı telefon, tablet, el bilgisayarları, aktif cihazlar, disket, kartuş, CD, DVD, BD medyalar, yedekleme birimleri, telli/telsiz iletişim cihazları, router, hub, switch, modem, ağ bağlantıları ve sistemleri vb. her türlü elektronik/manyetik ortamlar, sistemler ve ekipmanlar ve bunlara ait yazılım, program, uygulamalar vb. üzerinde işlenen, tutulan, kaydedilen, iletilen, saklanan tüm veri ve bilgiler ile; faks, yazıcı, fotokopi, el yazısı vb. ile üretilmiş dosya, yazı, çıktı, doküman, evrak vb. yerlerde tutulan, kaydedilen, iletilen, saklanan tüm veri ve bilgileri ifade eder.
- *Veri İletişim Kanalları* : Her türlü genel amaçlı veri/bilgi veya gizli/değerli bilgiye erişilmesi veya tüm bu verilerin/bilgilerin bulunduğu ortamdan başka ortamlara çeşitli yollardan (telli/telsiz iletişim,

Internet, telefon, GSM, e-posta, ağ üzerinden kopyalama, yedekleme cihazları üzerine taşıma, CD, DVD, BD vb. medyalar ile, faks, modem, fotokopi, yazıcı vb.) iletimi, kopyalanması, taşınmasına olanak veren bilgi sistemlerini ifade eder.

- *Veri Sorumlusu* : ÖZEL İTALYAN ANA VE İLKOKULU ve ortaklık pay oranlarına bağlı kalınmaksızın var olan ve ileride kurulacak bağlı şirketler, iştirakleri ve bunların ortaklık kurduğu ve kuracağı tüm şirketleri ifade eder. Aynı zamanda, kişisel verilerin işleme amaçlarını ve yöntemlerini belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.
- *Veri Sorumlusu İrtibat Kişisi* : Türkiye'de yerleşik olan gerçek ve tüzel kişiler için veri sorumlusu tarafından, Türkiye'de yerleşik olmayan gerçek ve tüzel kişiler için de veri sorumlusu temsilcisi tarafından, Kanun ve bu Kanun'a dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kurum ile iletişimi sağlamak amacıyla sicile kayıt esnasında bildirilen gerçek kişiyi ifade eder.

3. Kapsam

Bu politika, Veri Sorumlusu bünyesinde çalışan (bordrolu, sözleşmeli, stajyer, diğer özel anlaşmalara bağlı vb.), her türlü yetki, unvan, amaçla görev yapan tüm çalışanları kapsamaktadır. Tüm Veri Sorumlusu çalışanları bu politikada belirtilen standart ve kuralları okumak, bilmek ve uymakla yükümlüdür.

4. Yetki ve Sorumluluklar

4.1. *Veri Sorumlusu Yöneticilerinin Sorumlulukları*

4.1.1. Belirlenmiş olan politika ve standartların önemini kendi birimindeki çalışanlara aktarmak, kurumsal ve yasal gereksinimler kapsamında düzenli olarak gözden geçirmek ile sorumludur.

4.1.2. Politika ve standartları, kendi birimindeki çalışanların anlamasına ve politikalara uyumun sağlanmasında yardımcı olmalıdır.

4.1.3. Kendi birimindeki çalışanlarda güvenlik bilincinin oluşması ve yerleşmesine yardımcı olmalıdır.

4.2. *Veri Sorumlusu Çalışanlarının Sorumlulukları*

4.2.1. Bilgi sistemleri işlemlerini belirlenen kurallar ve standartlar doğrultusunda, gerektiğinde BSD bünyesinde görev yapan Hizmet Masası birimlerinden destek alarak gerçekleştirmek ile yükümlüdür.

4.2.2. İlgili güvenlik standartları ve politikalarına aykırı davranışları gözlemlediklerinde en kısa sürede Hizmet Masası veya BSG birimlerine bildirir.

4.3. *BSG Birimi Sorumlulukları*

Bilgi sistemleri güvenlik politika ve standartlarını belirler. Bu politika ve kuralların uygulatılmasını sağlar ve denetlemesini yapar.

4.4. *BSD İlgili Birimlerinin Sorumlulukları*

İlgili güvenlik standartlarını ve teknik düzenlemelerini bilmek ve uygulamakla yükümlüdür. Belirlenmiş olan politika ve standartlara göre Veri Sorumlusu çalışanlarına destek verir.

5. Kurallar ve Uygulama

5.1. Kurum içinde elektronik veya diğer ortamlardaki veriler/bilgiler Veri Sorumlusu'nun mülkiyetindedir ve tüm yasal hakları Veri Sorumlusu'na aittir.

5.2. Veri Sorumlusu bünyesindeki her türlü bilgi sistemleri, veri iletişim kanalları, verileri/bilgileri vb. yalnızca iş amaçlı kullanılmak zorundadır.

5.3. Veri Sorumlusu çalışanları, her türlü bilgi sistemleri, veri iletişim kanalları, veri ve bilgilerin kullanımları sırasında, fiziksel koruma, erişim denetimi, yedekleme, güvenlik ve gizlilik ilkelerine azami önem göstermek ve uymak zorundadırlar. Özellikle kaybolma ve hırsızlık risklerine açık olan taşınabilir cihazlar gözetimsiz bırakılmamalı ve güvenliği sağlanmalıdır.

5.4. Veri Sorumlusu'na ait gizli/değerli bilginin ve her türlü kişisel verilerin gizliliğinin sağlanması esastır. Tüm bu değerli bilgi ve kişisel verilerin veri iletişim kanalları yoluyla Veri Sorumlusu dışına çıkartılması ve üçüncü şahıslara, her ne şekilde ve her ne amaçlı olursa olsun iletilmesi, kullandırılması yasaktır. Ayrıca kurumsal süreçlerde kullanılan özel nitelikli kişisel veriler ve kişisel veriler elektronik veya fiziksel kopya olsun çalışanın evinde, dizüstü bilgisayarlarda veya diğer kişisel taşınabilir cihazlarda ve işyeri dışındaki diğer sahalarda tutulamaz. Verilerin/bilgilerin kurum dışına çıkartılması gereken özel durumlarda, konuyla ilgili Veri Sorumlusu bünyesinde yayımlanmış olan [lütfen buraya "Bilgi Sistemleri Genel Standartlar ve Güvenlik Politikasının" linkini ekleyiniz.] uygulanacaktır.

5.5. Veri Sorumlusu çalışanları, Veri Sorumlusu mülkiyetinde olmayan bilgi sistemlerini bina, ofis, şirket vb. içine sokamaz, kullanamaz. Gerektiği özel durumlarda yalnızca BSD bilgisi ve onayı ile yetkili çalışan gözetiminde giriş yapılabilir.

5.6. Sistem odalarına ve bu odaların olmadığı yerlerdeki sistem cihazlarına yalnızca Veri Sorumlusu BSD bünyesindeki yetkili çalışan giriş yapabilir. Bu çalışan dışındaki kişilerin sistem odalarına girmesi veya sistem cihazlarına erişmesi gerektiği durumlarda, konuyla ilgili Veri Sorumlusu bünyesinde yayımlanmış olan "Bilgi Sistemleri Genel Standartlar ve Güvenlik Politikası" uygulanacaktır.

5.7. Üçüncü şahısların Veri Sorumlusu bilgi sistemleri ve bu sistemler üzerindeki her türlü bilgiyi veri iletişim kanallarıyla kullanması gerektiği durumlarda, konuyla ilgili Veri Sorumlusu bünyesinde yayımlanmış olan "Bilgi Sistemleri Genel Standartlar ve Güvenlik Politikası" uygulanacaktır.

5.8. Çalışma saatleri sonunda masaüstünde herhangi bir doküman bırakılamaz, gizli/değerli, kişisel ve kurumsal veri içeren belgeler, özel proje dosyaları ofis masalarının parçası olan kilitli çekmecelerde ve dolaplarda tutulmalıdır. Aynı şekilde şifre ve kullanıcı adı yazılı küçük kağıtlar çalışma masası üzerinde veya çevresinde kesinlikle bırakılamaz.

5.9. Veri Sorumlusu çalışanları kullanmakta oldukları bilgi sistemlerine veri iletişim kanallarıyla kendi istekleri ve bilgileri dışında erişilmesine olanak tanımamalıdır. Bilgi sistemlerinde çalışmaları bittiğinde, mutlaka şifre denetimli ekran koruyucularını çalıştırmalı veya sistemden erişim bağlantı / oturumlarını kapatarak (logout/logoff vb.) çıkmalıdırlar.

5.10. BSD bilgisi ve onayı olmadan, bilgi sistemlerine veri iletişim kanallarıyla ne amaçlı olursa olsun, herhangi bir yazılım, donanım veya sistem kopyalanamaz, kurulamaz. Veri Sorumlusu çalışanları, BSD tarafından hazır olarak kendilerine teslim edilmiş hiçbir kişisel bilgisayarda yazılım, donanım veya

sistem ayarlarında değişiklik yapamaz. Değişiklik gerektiği durumlarda her türlü ayar değişikliğini yalnızca, o sistemlerin yetkilisi olan BSD Kullanıcı Destek ekipleri yapacaktır.

5.11. Veri Sorumlusu bünyesindeki bilgi sistemlerinde kullanılan tüm yazılımlar lisanslı ve yasaldır; bu sistemlerin ürün standartlarını BSD belirler. Veri Sorumlusu çalışanları bilgisayar programlarını da kapsayan 5846 sayılı Fikir ve Sanat Eserleri Kanunu'na aykırı hareket edemezler.

5.12. Kişisel bilgisayar veya sunucu sistemlerde virüs koruma (anti-virus) programı kurulu ve sürekli etkin durumda olacaktır. Veri Sorumlusu çalışanları, kullandıkları bilgisayarlarda virüs koruma programının kurulu olmadığını, programın çalışmadığını veya bilgisayara zararlı bulaştığını fark ederlerse, mutlaka en kısa sürede Hizmet Masası birimlerine haber vermelidirler.

5.13. Kullanıcı kimliği ya da şifreler kişiye özeldir ve kimseyle paylaşılmamalıdır. Kullanıcı kimliği ya da şifrenin herhangi yetki dışı kullanım dahil tüm kullanımından ve meydana gelebilecek suiistimal olaylarının yaratabileceği kurum zararlarından çalışanlarımız sorumludur. Kullanıcı kimliğinin ya da şifrenin güvenliğinden kuşku duyulan durumlarda şifreler değiştirilmeli ve derhal Hizmet Masası birimiyle temasa geçilmelidir. Veri Sorumlusu çalışanları, bilgi sistemlerindeki tüm kullanıcı adı, şifre, yetki sistemleri vb. kullanımlarında, BSD'nin Veri Sorumlusu bünyesinde yayımladığı "Şifre Seçimi Ve Kullanımında Uyulması Gereken Güvenlik Standartları" dokümanını okumalı ve söz konusu dokümanda belirtilen tüm kurallara uyacak şekilde şifre seçmeli ve kullanmalıdırlar.

Commented [AA3]: Arkas BSD şemsiyesi dışında kalan iştiraklerin irtibat kişileri, bu cümleyi metinden çıkarmalı veya kendi uygulamalarına uygun şekilde revize etmelidir.

5.14. Gizli/değerli veriler ile kişisel veriler ağ aracılığı ile güvensiz (şifrelenmemiş) olarak paylaşılamaz ve iletilemez. Veri Sorumlusu çalışanları bu amaca yönelik veri ve bilgi şifrelemede kullanılacak uygun yöntem ve politika için Hizmet Masası birimimizden destek alabileceklerdir. Aynı şekilde gizli/değerli veriler ile kişisel verilerin şirket içerisinde başka bir çalışan ile paylaşılmasının gerektiği durumlarda, iç yazışma zarfları "Kişiye Özel" olarak sadece ilgilisine gönderilmelidir.

5.15. Veri Sorumlusu bünyesinde kurum tarafından verilen internet hizmeti dışında, alternatif internet hizmeti kullanılamaz. Veri Sorumlusu çalışanları, yetkili Internet erişimi veya Internet üzerinden şirket içi ve dışı her türlü diğer erişim gereksinimlerinde konuyla ilgili Veri Sorumlusu genelinde yayımlanmış olan BSG politika ve standartlarına göre istekte bulunacaklardır.

5.16. İnternet, yalnızca şirket mevzuatı, işleri ile ilgili araştırma/geliştirme, bilgi toplama, ihtiyaçlar ve amaçlar kapsamında, ilgili yasal, resmi, kurumsal web sitelerine erişim yapmak için kullanılmalıdır. Kurum cihazları güvenlik açısından gerekli görüldüğünde BSG uzmanları tarafından merkezi olarak kontrol edilebilecektir.

5.17. Veri Sorumlusu çalışanları, şirket e-posta sistemlerini, adreslerini ve e-posta kutularını yalnızca iş amaçlı kullanabilir. Şirket e-posta adreslerini kullanılarak, çalışanlarımıza veya üçüncü şahıslara, kişiliği zedeleyici, müstehcen içerikli, hakaret, tehdit, küfür, siyasi mesaj, slogan, propaganda vb. içeren e-posta iletilemez; şirket e-posta sistem ve adresleri kurumsal şirket politikalarını, kurallarını veya ülke yasalarını ihlal edecek kanundışı işlemlerde kullanılamaz.

5.18. Veri Sorumlusu çalışanları, tanımadıkları adreslerden gelen, ek dosyası, konusu veya içeriği kuşkulu veya belirsiz olan e-postaları kesinlikle açmamalı, herhangi başka bir adrese iletmemeli, en kısa sürede Hizmet Masası birimlerine haber vermelidir. Benzer şekilde, Veri Sorumlusu çalışanları, herhangi bir kaynaktan (e-posta, medya, Internet veya başka yolla) bir virüs ihbar, haber ve uyarısı alırsa, bu bilgiyi herhangi bir üçüncü şahsa veya iş arkadaşına kesinlikle aktarmayıp Hizmet Masasına iletmelidir.

5.19. İş amaçlı her türlü liste servisi (sosyal medya, mailing list, newsgroup) ya da benzeri ortak elektronik posta sistemleri ve dağıtım gruplarına üyeliklerde, Hizmet Masası birimleri aracılığıyla BSD'den onay alınması gerekmektedir.

5.20. Veri Sorumlusu çalışanlarının yapmış olduğu bütün Internet erişimleri ve e-posta kullanımları, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun gereği Veri Sorumlusu içindeki bilgi güvenliği kontrol sistemlerinde kayıtlanıp takip altında bulundurulmaktadır.

5.21. Veri Sorumlusu'na ait veriyi korumak amacıyla, kurumsal kaynaklara şirket dışından veri iletişim kanallarıyla bağlanarak çalışan için ek güvenlik önlemleri alınması gerekecektir. Bu durumlarda çalışanın kullandığı bilgi sistemlerine (kişisel bilgisayar, akıllı telefon, tablet vb.) BSD uzmanları tarafından uygulanacak kontroller (iyileştirme, düzenleme, şifreleme ve zararlı kod önleme) kurumsal kaynaklara erişim süresince çalışır durumda tutulmalıdır.

5.22. Kullanıcıların Veri Sorumlusu kurumsal sistem kaynaklarına erişim yetkileri iş gereksinimlerine göre düzenlenmektedir. Veri Sorumlusu çalışanları kendilerinde ya da çalışma arkadaşlarında gördükleri yetki aşımı ya da paylaşımı gibi uygunsuzlukları en kısa zamanda Hizmet Masası birimine bildirmekle yükümlüdürler.

5.23. Ortak paylaşım alanları, elektronik posta sistemleri kişisel verilerin arşiv depolamasına uygun değildir. Veri Sorumlusu suç veya kanunsuz olması muhtemel olarak görülen her türlü veri, sistem ve malzemeyi kendi bilgi sistemlerinden çıkarma hakkını ve bununla ilgili resmi işlem başlatma hakkını saklı tutar.

5.24. Veri Sorumlusu bünyesinde bilgi sistemleri ve ekipmanları ile iş kapsamı dışında bulut depolama ve mesajlaşma hizmetlerinin (Dropbox, Gdrive, Onedrive, Whatsapp, Hangouts, Box, vb.) kullanılması yasaktır. Bu tür gereksinimler için iş öncelikleri gözetilerek kurumsal uygulamaların belirlenmesi ve hizmete alınması BSD birimlerinin sorumluluğundadır.

5.25. Şirketimiz, kişisel verilerin işlenmesinde hukuksal düzenlemelerle getirilen ilkeler ile genel güven ve dürüstlük kuralına uygun hareket etmektedir. Bu kapsamda şirketimiz, kişisel verilerin işlenmesinde orantılılık gerekliliklerini dikkate almakta, kişisel verileri amacın gerektirdiği dışında kullanmamaktadır. Bu nedenle çalışanlarımız Veri Sorumlusu idari ve iş birimleri tarafından kendisinden talep edilmeyen kişisel verilerini, özel nitelikli kişisel verilerini kurum kaynaklarında saklamamalı ve kullanmamalıdır. İşle ilgili olmayan ve şahsi/özel kullanım amaçlı tüm kişisel veriler (veri sorumlusu tarafından gereğince aydınlatılan ve açık rıza alınanlar hariç olmak üzere), veri sorumlusu tarafından tahsis edilen e-posta kutularında, anlık mesajlaşma yazılımlarında, ofis belgelerinde, taşınabilir bilgisayarlarda ve ortak paylaşım alanlarında bulundurulmamalıdır. Ayrıca çalışanlar, işledikleri bütün kişisel verilerin güvenli şekilde tutulmasını temin etmekle yükümlüdürler. Kişisel Veriler, kazaen veya başka bir şekilde de olsa herhangi yetkisiz bir üçüncü kişiyle sözlü, yazılı veya başka şekilde paylaşılamaz, ifşa edilemez. Kişisel verileri yetkisiz olarak paylaşılması gibi maddede belirtilen prensiplere aykırı durumların derhal Veri Sorumlusu İrtibat Kişisi'ne bildirilmesi gerekmektedir.

5.26. Her çalışan, kurumla ilişiğinin kesilmesi durumunda; Veri Sorumlusu'na ait her türlü gizli/değerli bilgi, veri/bilgi ve bunların tutulduğu veya kayıtlı, yazılı olduğu tüm bilgi sistemlerini işten ayrıldığı yazılı tarihi takiben en fazla 1 iş günü içinde Veri Sorumlusu'na geri teslim etmek zorundadır. İşten çıkartılan veya

kendi isteğiyle işten ayrılan her çalışan, Veri Sorumlusu ile ilişiği kesildiği tarihten itibaren süresiz olarak işbu Politika'nın 5.1. ve 5.4. maddelerine uymakla yükümlüdür.