DOĞAN ŞİRKETLER GRUBU HOLDİNG A.Ş.

BİLGİ GÜVENLİĞİ VE BİLGİ TEKNOLOJİLERİ POLİTİKASI

İÇİNDEKİLER

1. AMAÇ

Bu politikanın amacı, Doğan Şirketler Grubu Holding A.Ş (Doğan Holding) bilgilerinin uygun şekilde korunmasını sağlamak için yönetim talimatları, prosedür şartları ve teknik bir politika oluşturmaktır.

2. KAPSAM

Bu politikanın kapsamında, Doğan Holding ağına erişen üçüncü şahıslar da dâhil olmak üzere tüm kullanıcılar bulunmaktadır. Politika, Doğan Holding'in sahibi olduğu ya da Doğan Holding tarafından yönetilen tüm bilgisayar ve bilgi iletişim sistemlerine uygulanmaktadır. Bu politika, IS027001:2013 Bilgi Güvenliği Yönetim Sistemi Standardı gerekliliklerine dayalı olarak ele alınmış ve hazırlanmıştır.

Bilgi Sistemleri (BS) departmanı, tüm kullanıcıların katılımı ve desteğini istemektedir. Tüm kullanıcılara ,Doğan Holding varlıklarını uygun şekilde korumalarını sağlamak için yeterli eğitim ve yardımcı referans materyalleri temin edilecektir.

Bu politika, dâhili olarak kullanılan tüm bilgisayar sistemleri, yerel alan ağları ve Holding iştirakleri kapsamında hizmet verilen bilgisayarlar veya ağlar ile ara yüze sahip olan harici (çalışanlar/tedarikçiler) bilgisayar veya ağlar için uygulanmaktadır.

Bu politika, Doğan Holding bünyesinde bulunan herkesin bilmesinin ve sürekli olarak uymasının beklendiği temel kontrol tedbirlerini tanımlamaktadır.

3. TANIM ve KISALTMALAR

Bu bölümde politikada geçen özel terim ve deyimler, kavramlar, kısaltmalar vb. kısaca açıklanır.

3.1. Doğan Holding: Doğan Şirketler Grubu Holding A.Ş.

3.2. Doğan Grubu: Doğan Şirketler Grubu Holding A.Ş. ve bağlı ortaklık, iştirak ve iş ortaklıklarıdır.

3.3. Üst Yönetim: Doğan Holding İcra Kurulu, İcra Kurulu Başkanı, C Level Yöneticileri (İştirakler için bu seviye bulunmaması halinde Genel Müdürü) belirten tanımdır.

3.4. Doküman: Doğan Holding politika, yönetmelik, prosedür ve iş süreçlerinin yazılı ve ilgili çalışanların erişimine açık bir şekilde oluşturulmuş prosedür ve benzeri diğer her türlü yazılı metindir.

3.5. Dokümanın Adı: Dokümanın ilişkili olduğu konuyu ifade eder.

3.6. Çalışan: Doğan Grubu Personelini ifade eder,

3.7. Hizmet Sağlayıcısı: Doğan Holding'in hizmet aldığı ve/veya verdiği şirket (tedarikçi, taşeron, müşteri vb.) personelini ifade eder.

4. ROL ve SORUMLULUKLAR

Bilgi Sistemleri (BS) departmanı, tüm kullanıcıların katılımını ve desteğini istemektedir. Tüm kullanıcılara, Doğan Holding varlıklarını uygun şekilde korumalarını sağlamak için yeterli eğitim ve yardımcı referans materyalleri temin edilecektir.

4.1 Yönetim Kurulu

Yönetim Kurulu, Politika'ya, kural ve düzenlemelere uyulmaması durumunda bildirim, inceleme ve yaptırım mekanizmalarının belirlenmesi ve işletilmesinin üst gözetiminden sorumludur.

4.2. İcra Kurulu

Bilgi Güvenliği ve Bilgi Teknolojileri Politikası İcra Kurulu tarafından onaylanmıştır. Politikanın oluşturulmasının, uygulanmasının ve gerektiğinde güncellenmesinin sağlanması konusunda yetkili onay mekanizmasıdır.

4.3. Bilgi Sistemleri Direktörlüğü

İşbu politikanın hazırlanması, geliştirilmesi, yürütülmesi ve güncellenmesinden, Bilgi Sistemleri Direktörlüğü sorumludur. Bilgi Sistemleri Direktörlüğü, bu politika gerektiğinde güncelliği ve geliştirme ihtiyaçları açısından değerlendirir.

Hazırlanan dokümanın kurum portalında yayınlanması Doğan Holding Bilgi Sistemleri Bölüm Yöneticisi'nin sorumluluğundadır.

4.4 Kurumsal İletişim Başkan Yardımcılığı

Hazırlanan dokümanın kurum içi dağıtımının yapılması Doğan Holding Kurumsal İletişim Bölüm Yöneticisi'nin sorumluluğundadır.

4.5 Yatırımcı İlişkileri Direktörlüğü

Yatırımcı İlişkileri Direktörlüğü bu politika çerçevesinde, Doğan Grubu'nun kurumsal yatırımcılar, portföy yöneticileri, analistler, mevcut ve potansiyel hissedarlar arasındaki ilişkilerini düzenlemekten ve kamuyu bilgilendirme uygulamalarını, şeffaf bir şekilde tüm ilgililere eş zamanlı olarak yapmaktan sorumludur. Hazırlanan dokümanın internet sitesinde yayınlanması Doğan Holding Yatırımcı İlişkileri Bölüm Yöneticisi'nin sorumluluğundadır.

5. BİLGİ SORUMLULUKLARI

5.1. Bilgi / Risk Sahipleri

- Tüm elektronik bilgilerin belirli bir bilgi sahibi olması gerekmektedir. Bilgi/risk sahipleri yasal olarak bilginin sahibi değildirler. Bilgi/risk sahipleri veya bunların atadığı kişiler aşağıdaki kararları almak ve faaliyetleri yürütmek ile yükümlüdürler:
  - Elektronik bilgiye erişimin onaylanması,
  - Ek giriş onay kontrollerinin uygulanması ve işletilmesi,
  - Bilgilerini kullanan tüm yeni ve geliştirilmiş uygulama sistemlerinin, bu sistemler, işletim durumuna geçmeden önce onaylanması
  - Bilgi/risk sahipleri, sahip oldukları bilgi ve bilginin tutulduğu ortama ilişkin risklerin sahibi ve onay sorumlusu olarak kabul edilmektedirler.

5.2. Bilgi Sorumluları

- Bilgi sorumluları, uygulama sistemleri ve elektronik bilgilerinin geliştirilmesi ve bakımını destekleyen BS personelidir. Sorumlular, bilgi sistemleri hizmetlerinin bu politika ve genel olarak kabul edilmiş BS standartları ile uyumlu olarak temin edilmesinden sorumludurlar. Fiziksel ve mantıksal erişim kontrol sistemleri kullanarak, Sorumlular, kontrolleri altındaki bilgileri yetkisiz dağıtım, erişim, değiştirme, silme veya kullanıma karşı korumak ile yükümlüdürler. Sorumlular, yedekleme ve geri kazanma sistemleri gibi genel kontrolleri temin etme ve idare etmekten sorumludurlar.

5.3. Kullanıcılar

- Kullanıcılar, elektronik bilgilere erişimi olan herhangi bir birey olarak tanımlanmaktadırlar. Kullanıcıların, Bilgi Sahipleri tarafından tanımlanan, Bilgi Sorumluları tarafından yürütülen veya BS departmanı tarafından oluşturulan tüm güvenlik şartlarına ve Bilgi Güvenliği Politikasında belirtilen hükümlere uymaları gerekmektedir. Kullanıcıların, Bilgi Güvenliği Politikası ve bu politikayı destekleyen tüm politika, prosedür ve standart dokümanlarını bilmeleri ve bunlara uymaları gerekmektedir.

6. BİLGİNİN SINIFLANDIRILMASI

- Doğan Holding bünyesinde, bilgileri dört grupta sınıflandıran bir bilgi politikası oluşturmuştur. Dâhili veya harici olarak üretilen tüm bilgiler, “Çok Gizli, Gizli, Hizmete Özel ve Kamuya Açık” kategorileri altında bilgi sahipleri tarafından

sınıflandırılmaktadır. Tüm kullanıcılar, bu kategorilerin tanımlarını ve bu kategoriler içine giren bilgileri korumak için alınması gereken tedbirleri bilmek ile yükümlüdürler.

6.1. Çok Gizli

- İzinsiz olarak açıklandığı takdirde Doğan Holding'in güvenliğini, çıkarlarını ve diğer kuruluşlarla ilişkilerini olumsuz yönde etkileyebilecek, Doğan Holding'in maddi manevi büyük zararına neden olabilecek nitelikte, olağanüstü önem taşıyan bilgi varlıkları Çok Gizli olarak nitelendirilir.

- Yetkisiz kişinin eline geçmesi, bütünlüğünün bozulması ya da kaybolması durumunda Doğan Holding için kritik öneme sahip olan ve herhangi bir bilgi sızması halinde Doğan Holding üst yönetime rapor edilmesi gereken ve Doğan Holding ve bağlı ortakların karını direkt olarak etkileyecek olan bilgi varlıklarıdır.

- Doğan Holding bünyesindeki birimler ve bağlı diğer kuruluşlar tarafından üretilen veya bu kamu makamları için üretilerek arz edilen bilgiler, Çok Gizli kategorisinde olabilirler. Örneğin; Yönetim Kurulu Kararları, Karar Dosyaları, Doğan Holding İcra Kurulu Toplantı Notları, Doğan Holding Strateji Dokümanları vb.

- Çok Gizli bilgi varlıkları, güvenliği sağlanmış ve sadece yetkili kişilerin erişebileceği şekilde konumlandırılmalı, güvenlik önlemleri alınmalıdır. Fiziki ortamlarda tutulmaları halinde odalarda bulunan kasa veya kilitli dolaplarda saklanmalı; kopyalama, iletme, imha işlemleri için yetkili kişinin onayı alınmalıdır.

- Bu varlıklar, yakılarak ya da birleştirilmeyecek derecede parçalanarak imha edilmelidir. Elektronik ortamda bulunan bu tipte bilgiler için veri şifreleme uygulanmalıdır.

6.2. Gizli

- Gerekli izin alınmadan açıklandığında Doğan Holding'in güvenliği, saygınlık ve çıkarlarını ciddi derecede zedeleyecek, diğer yandan dış/rakip kuruluşlara geniş yararlar sağlayabilecek, Doğan Holding faaliyetlerinin devam ettirebilmesi için kritik öneme sahip olan, sadece ilgili kişilerin erişimine açılabilecek ve yetkisiz erişim sonucunda sorunların yaşanabileceği bilgi türüdür. Örneğin; iş planları, fiyat teklifleri, sözleşmelerle ilgili bilgiler vb.

- Bu tür bilgi varlıkları kasa ya da kilitli ortamda saklanmalı; kopyalama, iletme, imha işlemleri için yetkili kişinin onayı alınmalıdır. Bu varlıklar yakılarak ya da birleştirilmeyecek derecede parçalanarak imha edilmelidir.

- Bu verilere erişim, görevleri ile ilgili olarak az sayıda kişiye tanınmakta olup konu ile ilgisi olmayan personelin erişimine ve Doğan Holding dışından erişime kapalıdır. Bu tip verinin güvenli ortamlarda tutulması gerekir.

6.3. Hizmete Özel

- Doğan Holding için üretilen; prosedürler, iş akışları, listeler, formlar, görev tanımları gibi Holding çalışanlarının erişimine açık olması gereken ve Doğan Holding dışına çıkarılması için Üst Yönetim'den onay alınması gereken bilgi varlıklarıdır. Doğan Holding içinde kullanılmasında, kopyalanmasında sakınca yoktur.

- Ancak içeriği itibarı ile sadece Doğan Holding bünyesindeki bir grup yetki verilmiş kişilerin erişebileceği dokümanlar olması halinde bunların gizlilik derecesi için; "Çok Gizli" veya "Gizli" seçeneklerinden uygun olanı seçilmelidir.

- Dış bilgi taleplerinde, bilgi talep edenin yetkili makam olması ya da hukuken bu bilgiyi almaya hak kazanmış olması gerekmektedir.

6.4. Kamuya Açık

- Güvenlik açısından önemli olmayan, herkese açık olan ya da bir web sitesinde yayınlanan bilgi türüdür.

6.5. Varsayılan Kategori

- Bilgi sahibi tarafından etiketlenmemiş tüm elektronik bilgiler varsayılan kategori olan "Gizli" kategorisine girecektir.

7. ERİŞİM POLİTİKASI

7.1. Bilinmesi Gerekenler

- Kullanıcılara bilgi erişimi, bilinmesi-gereken/erişmesi-gereken bazında sağlanacaktır. Bilgi, yalnızca meşru iş gerekliliği olan kullanıcılara açıklanmalıdır.

- Bilinmesi-gereken kavramının uygulanması için erişim talebi ve onayı sürecini geliştirmiş olup söz konusu süreç "Kullanıcı Hesapları Yönetimi Prosedürü" ve bu prosedüre bağlı prosedür dokümanları içerisinde detaylandırılmıştır.

7.2. Kullanıcı/Kimlik Doğrulama

- Kimlik doğrulama işlemi, sistemin, kullanıcı kimliğini kişiye özel olarak onaylamasıdır. Bu işlem Doğan Holding bünyesinde kullanıcı adı ve şifre aracılığı ile gerçekleştirilmektedir.

- Tüm bilgi varlıklarına erişimde mutlaka kullanıcı doğrulama işlemleri erişim ve yetkilendirmeden önce tamamlanmalıdır. Geçersiz, kayıtsız veya denetlenemeyen kullanıcı doğrulamalarına izin veren ayarlar kesinlikle yasaktır.

Hata geri bildirimi, doğrulama bilgilerinin hangi kısmının yanlış olduğuna dair herhangi bir bilgi içeremez.

7.3. Erişim Standartları

- Aşağıdaki uyarı mesajı standart kullanıcı uygulamaları dışındaki sistem veya uygulamalara erişim öncesinde uyarı olarak kullanıcıların karşısına çıkmalıdır:
    - UYARI MESAJI: Şu an erişmeye çalıştığınızı sistem/uygulama v.b. Doğan Holding'e aittir. Yapacağınız her işlem kayıt altına alınacaktır. İzinsiz erişim girişimlerinde bu kayıtlar mahkemede delil olarak kullanılacaktır.

7.4. Kullanıcı Sorumlulukları

- Doğan Holding'in tüm bilgi varlıklarına erişimlerde çalışanlar sadece kendilerine özel olarak tanımlanmış olan kullanıcı adı ve şifre ile erişim sağlarlar. Çalışanlar kendilerine özel olarak tanımlanan kullanıcı hesaplarını başkalarının kullanmasına kesinlikle müsaade etmezler ve kendi hesapları ile yapılacak tüm işlemlerden sorumludurlar.

- Bütün kullanıcılar, bu politikada belirtilen şifre kısıtlamalarına uygun olarak kendilerinin kişisel şifrelerini üretirler. Şifrelerin başka kişiler ile paylaşılması kesinlikle yasaktır.

- Kullanıcılara verilen şifreler mutlaka, sadece kullanacak kişinin görebileceği yöntemler ile üretilip kullanıcıya iletimi gerçekleştirilir. İlk kez sistemlere veya uygulamalara giriş yapıldığında mutlaka şifreler değiştirilir.

- Servis hesapları sistem ve veri tabanlarında belirli işlemleri gerçekleştirmek için ortak kullanım amacıyla yaratılmış hesaplardır. Bu hesapların ortak kullanımı zorunlu olduğu için yukarıda belirtilen kişiye özel tanımlanmış hesap zorunluluğundan muaftır. Ancak bu hesaplar ilgili operasyon yöneticisinin sahipliğindedir. Bu hesabın kimler tarafından kullanılacağının belirlenmesi, yetkili kullanıcılar dışında kimse tarafından kullanılmaması, şifresinin değiştirilmesi gibi sorumluluklar operasyon yöneticisine aittir.

- Herhangi bir bilgi sistemine ve ağ kaynaklarına rol ve sorumluluğu veya iş ihtiyacı sebebi ile yetkilendirilmemiş tüm çalışanlar, oluşan hata veya teknik yetersizlikler sebebi ile bir bilgi sistemi veya ağ kaynağına erişebiliyor olsa bile giriş yapmazlar. Aksi davranışlar politika ihlali kapsamında ele alınır.

- Çalışanlar kullandıkları kişisel bilgisayarları ve sunucu sistemlerini başıboş bıraktıkları zaman mutlaka ekranları kilitli tutarlar. Ayrıca masalarını kullanmadıkları zaman, hassas bilgilerin bulunduğu basılı dokümanları kilitli dolap veya çekmecelerde bulundururlar.

8. DONANIM SORUMLULUKLARI

8.1. Kullanıcı Sorumlulukları

- Teslim aldığı PC, Laptop ve mobil cihazları temiz tutar,
- Teslim aldığı PC, Laptop ve mobil cihaz donanımlarında değişiklik yapmaz. Cihaz donanımlarında değişiklik yapma yetkisi yalnızca Bilgi Sistemleri Direktörlüğü'nde bulunur,
- Teslim aldığı PC, Laptop ve mobil cihazların güvenliğinden sorumludur,
- Teslim aldığı PC, Laptop ve mobil cihazları her üçüncü şahıslara vermemelidir.
- Bilgi Sistemleri Direktörlüğü tarafından gönderilen veya onaylanan üçüncü şahıs şirketlere PC, Laptop ve mobil cihazlar teslim edilebilir.
- İşverene ait PC, Laptop ve mobil cihazlar hiçbir şekilde yasa dışı, Doğan Holding çıkarlarıyla çelişecek veya normal operasyon ve iş aktivitelerini engelleyecek şekilde kullanılmamalıdır.
- Kullanıcı cihazların çalınma, düşürme gibi fiziksel güvenliğinden şüphe ettiği ve herhangi bir olay olduğu durumda Bilgi Güvenliği Yöneticisini bilgilendirmekle sorumludur.

9. ŞİFRE YÖNETİMİ ve KULLANIMI POLİTİKASI

9.1. Şifrelerin Seçilmesi

Kolaylıkla tahmin edilmesi mümkün şifreler seçmekten kaçınılır. Şifreler, telefon defteri, ajanda v.b. kolayca erişilebilir ortamlarda yazılı olarak bulunmamalı ve bireyin özel hayatını yansıtacak bir şey olmamalıdır. Şifre politikası aşağıdaki şekilde yapılandırılmıştır:

- Kullanıcı hesapları varsayılan şifrelerle yaratılır. Sisteme ilk kez giriş yaptıktan sonra, kullanıcıdan yeni bir şifre yaratması istenecektir.
- Şifre, harf ve rakam kombinasyonu şeklinde en az 8 karakter uzunluğunda olmalıdır.
- Oluşturulan şifre mutlaka en az bir adet küçük karakter, bir adet büyük karakter, bir adet rakam ve bir adet alfanümerik olmayan karakter (~!@#$%^&*_-=`|\(){}[]:;"'<>,.?/) içermesi gerekmektedir.
- Şifreler 5 kez yeniden kullanılmamalı veya işleme sokulmamalı ve en az her 90 günde bir değiştirilmelidir. Minimum şifre süresi 5 gündür. Kullanıcı hesapları,

her 5 geçersiz giriş teşebbüsünden sonra kilitlenir ve admin kullanıcının müdahalesi ile tekrar kullanılabilir hale gelir.

- Eğer kullanıcı, şifresinin başka bir kişi tarafından bilindiğinden şüpheleniyorsa, şifrenin hemen değiştirilmesi gerekmektedir.

Kullanıcılar, BS de dahil hiç kimseyle şifrelerini paylaşmamalıdırlar. Kullanıcıların, şifrelerinin tehlikede olduğundan şüphelenmeleri durumunda, bunu hemen BS Müdürüne bildirmeleri gerekmektedir. Şifreler, yetkili bir şifrelendirme yazılımı ile şifrelendirilmediği sürece, kullanıcılar şifrelerini herhangi bir bilgisayar dosyasında veya bilgisayar programında saklamamalıdırlar. Şifreler herhangi bir yere yazılmamalıdır.

Kullanıcıların, masalarını terk ettikleri her zaman, çıkış yaptıklarından veya bilgisayarlarını emniyete aldıklarından emin olmaları gerekmektedir.

Eğer kullanıcı bilgisayarı terk ederse veya 15 dakikadan sonra hiç bir şey yapmazsa, Şifre korumalı ekran gözükecektir. (Kullanıcılar kendi ekran koruyucu (screen saver) ayarlarını değiştiremezler)

10. UZAKTAN ERİŞİM POLİTİKASI

10.1. Uzaktan Erişim

10.1.1. Onaylı Donanım

- Uzaktan erişim ancak, BS direktörlüğünün onayladığı bir donanım ile mümkündür.Bu tarz tüm cihazlar, BS güvenlik politikalarına uygun olarak yapılandırılmalı ve korunmalıdır. Kullanıcılar, bu cihazlar üzerindeki güvenlik konfigürasyonlarının, BS departmanının izni olmadan, herhangi yetkisiz bir şekilde değiştirilmediğinden emin olmalıdırlar.

- Donanımı BS direktörlüğü tarafından sağlanmayan uzaktan erişim yapacak olan kullanıcıların bilgisayarlarında işletim sistemi güvenlik updateleri ve lisanslı güncel bir antivirus programı olması zorunludur. Bilgi sistemleri direktörlüğü bağlantı yapacak kullanıcıların bilgisayarların da bu kontrolleri yapacak sistemleri tesis etmek durumundadır. İşletim sistemi güvenlik updateleri eksik zararlı bir program barındıran ve güncel bir antivirüsü olmayan bilgisayarlardan yapılacak uzaktan erişim istekleri otomatik olarak red edilecektir.

10.1.2. Uzaktan Erişim Onayı

- Uzaktan erişim ancak, meşru iş gereklilikleri olan kullanıcılara sağlanmaktadır. Doğan Holding Kurum ağlarına uzaktan erişim izni,

kullanıcının müdürü tarafından talep edilmekte ve Bilgi Sistemleri Direktörü tarafından onaylanmaktadır.

- Tüm uzaktan erişim kullanıcıları, uzaktan erişim kullanımı için BS tarafından hatları belirlenen şartlara uymak zorundadırlar ve bu erişimi almadan önce kısa bir eğitim almalıdırlar.

10.1.3. Uzaktan Erişimin Doğruluğunun Kanıtlanması

- Uzaktan erişimin gerçekleştirilmesi esnasında kullanıcı kimlik doğrulamasının güncel güvenlik gereksinimlerini karşılayacak şekilde oluşturulmalıdır.

10.1.4. Gizli Bilgilerin Kullanılması

- Elektronik gizli bilgiler, Doğan Holding ofislerinden, güven altına alınmamış bir şekilde çıkmamalıdır. Eğer gizli bilgilerin ofis dışına çıkması zorunlu ise, bilgi, BS departmanı tarafından onaylanan bir şifrelendirme yazılımı ile korunmalıdır. Halka açık ağlardan iletilen tüm elektronik gizli bilgiler, BS departmanı tarafından onaylanan bir şifrelendirme yazılımı ile şifrelendirilmelidir.

10.2. Güvenlik Duvarı Güvenliği

- Doğan Holding dâhili ağları ve Internet veya alenen erişilebilen diğer bilgisayar ağları arasındaki tüm bağlantılar bir güvenlik duvarı ile koruma altına alınmalıdır. Eğer istenirse, bazı özel programlar için güvenlik duvarında bir port açılır. Ancak program güvenli olmayan portlar kullanıyorsa, BS herhangi bir durum için güvenlik duvarını açmayacak ve yapılandırmayacaktır.

11. FİZİKSEL ERİŞİM POLİTİKASI

11.1. Fiziksel Erişim Güvenliği

Hassas ticari bilgi işleme araçları ve bilgilerin fiziksel olarak yetkisiz erişimlerden ve hasarlardan korunmaları amacıyla, söz konusu araçlar güvenli bir yere yerleştirilir, uygun güvenlik engelleri, giriş denetimleri ve tanımlanmış güvenli bir çevre aracılığıyla korunuyor olmaları sağlanır. Sağlanan korumanın, tanımlanmış risklerle orantılı olmasına özen gösterilir. Donanımlar, çevresel tehditler ve tehlikelerden oluşan riskleri ve yetkisiz erişimi fırsatlarını azaltmak üzere yerleştirilir ve korunur. Bilgi ve bilgi işleme araçları, yetkisiz kişilere ifşa edilmesi, yetkisiz kişilerce değiştirilmesi veya çalınması ihtimaline karşı korunur, kayıp veya hasarları en aza indirgemek için denetimler yapılır. Fiziki ve çevresel güvenlik kapsamında asgari olarak aşağıdaki hususlar göz önünde bulundurulur:

- Güvenli alanlara, sadece yetkili personelin erişimine izin verilir, yetkili personel dışında kalan kişilerin bu alanlara girmesi gerektiği durumlarda ise güvenlik ayrıca sağlanır.

- Sistem ile ilgili tesislere erişim için bir Erişim Kartı ve kişiye özel şifre bilgisi aracılığı ile gerçekleştirilir.

- Güvenli alanlara erişimler kayıt altına alınır. (loglanır).

- Sunucu odası erişimi, yalnızca erişmesi gereken personel ile sınırlandırılmalıdır.

- Yükleniciler, denetçiler, danışmanlar, geçici çalışanlar, vs. dâhil olmak fakat bunlarla sınırlı olmamak üzere sözleşmeli tüm personel, tesisteki hassas alanlara erişim sağlamadan önce ilgili müdürler tarafından önceden onaylanmalıdırlar.

- Güvenli bir alan, kilitlenmiş bir büro, kilitlenmiş dolaplar veya korumalar içeren fiziki güvenlik çevrelerinin yer seçimi ve tasarımında yangın, sel, patlama, saldırı ve diğer doğal afet ve insan saldırıları karşısında meydana gelebilecek hasarlar göz önüne alınır.

- Personel güvenli alanlarda yürütülen faaliyetlerden bilmesi gerektiği kadarıyla haberdar edilir, güvenliksiz alanlar kilitlenir, üçüncü kişiler destekle görevli personele, sadece gerekli olduğunda, sınırlandırılmış erişim verilir.

- Dağıtım ve yükleme alanları denetlenir, dışarıdan gelen malzemeler, kullanım noktasına taşınmadan önce denetlenir.

- Donanımların bakımları tedarikçinin tavsiye ettiği servis aralıklarında ve/veya teknik sorun ve arıza oluştuğundan talimatlarına uygun olarak sadece yetkili Doğan Holding personeli veya yetkili servisler aracılığı ile yapılır.

12. E-POSTA KULLANIM POLİTİKASI

12.1. Paylaşma ve İletme

- Elektronik posta hesapları, kullanıcı kimlikleri gibi bireye özeldir ve paylaşılmamalıdır. Eğer kullanıcı tatile çıkmış veya herhangi bir şekilde uzun süre e-postalarını kontrol edemeyecekse, bu kişilerin e-postaları başka bir dâhili kullanıcıya iletilebilir. E-posta uygulamalarında yapılan ayarlar ile gelen tüm e-postaların otomatik olarak dışarıda bir adrese gönderilmesi ve gizli bilgi ihtiva eden elektronik postaların Doğan Holding dışındaki adreslere iletilmesi yasaktır. Eğer elektronik posta gizli bir bilgi ihtiva ediyorsa, alıcının bu bilgiyi görmeye

yetkisi olmadığı veya orijinal mesaj sahibi, mesajın iletilmesini onaylamadığı sürece, kullanıcılar mesajı iletmemelidirler.

12.2. Gizli Bilgi

- Kullanıcılar, BS departmanı tarafından onaylanmış bir şifrelendirme yazılımı ile şifrelendirilmemiş hiç bir gizli bilgiyi, harici bir mesaj alıcısına giden bir e-posta içine koymamalıdırlar. Dâhili e-postalar erişim kontrolleri ile korunurlar ve şifrelendirme gerektirmezler.

12.3. Eklerin Saklanması

- Kullanıcılar, gelecek bir tarihte ihtiyaç duyabilecekleri önemli e-posta eklerini kaydetmekle sorumludurlar. Elektronik posta sistemleri eklerin kaydedilmesi amacıyla kullanılmamalıdır. Kullanıcılar, saklama amacıyla, önemli ekleri elektronik posta sistemlerinden bir ağ sürücüsüne taşımak zorundadırlar.

12.4. E-postaların Taranması

- Tüm e-postalar otomatik olarak, virüsler ve spam e-postalara karşı taranır. Eğer e-posta virüs ihtiva ediyorsa veya spam e-posta olarak sınıflandırılmışsa, sistem tarafından otomatik olarak engellenir ve silinir. Yine de, virüs tarama/filtreleme %100 etkili değildir. Dolayısıyla istenmeyen e-postalara ve eklentilere dikkatle yaklaşmanız gerekir ve şirket dışından gelen e-postaların yeterli güvenliğe sahip olamayabileceği bilinmelidir.

12.5. Mesajların İçeriği

- Kullanıcılar, hiç bir elektronik posta mesajında saygısız, müstehcen veya aşağılayıcı ifadeler kullanmamalıdırlar. Kullanıcılar İşle ilgili olmayan resim, video ve müzik dosyalar, vs. olan dosyalar için Doğan Holding e-posta adresini kullanmamalıdırlar.

12.6. Yalnızca Onaylı Elektronik Posta Sistemlerinin Kullanımı

- Kullanıcılar yalnızca yetkili Doğan Holding elektronik posta yazılımlarını kullanmalıdırlar (örn. MS Outlook). Kullanıcılar, herhangi bir iş mesajı için kendi elektronik posta hesaplarını, bir Internet servis sağlayıcısı veya diğer bir üçüncü şahıs ile kullanmamalıdırlar.

- Kullanıcılar, herhangi bir iş iletişimi için web tarayıcılarında bulunan elektronik posta özelliklerini kullanmamalıdırlar (örn. Yahoo mail, Hotmail, vs.). Eğer kullanırlarsa, kendi kişisel e-postalarından aldıkları ek dosyalarını açmamalıdırlar (yahoo, hotmail, mynet, vs.). Bu tür eylemlerden dolayı sisteme virüs bulaşırsa, BS'ye rapor edilecektir.

12.7. Gönderen Kimliğinin Doğrulanması

- Kullanıcılar, kaynağı ne olursa olsun, elektronik mesajlarını açarken dikkatli olmalıdırlar. Tüm ekler, açılmadan önce onaylı bir virüs koruma yazılım programı kullanılarak taranır. Kullanıcılar, mesajın geldiği yerden emin olmadıkları sürece hiç bir elektronik mesajı veya eklerini açmamalıdırlar.

12.8. Yalnızca İş Amaçlı Kullanım

- Internet erişimi tüm Doğan Holding çalışanları için sağlanmış ve yalnızca iş için kullanılması amaçlanmıştır. Kullanıcı internet erişimleri profil bazlı olarak gerçekleştirilecek olup, profil dışı erişimler kullanıcı müdürü ve bilgi güvenliği yöneticisi onayına sunulacaktır.

12.9. Yazılım Yükleme

- Internet erişimi tüm Doğan Holding çalışanları için sağlanmış ve yalnızca iş için kullanılması amaçlanmıştır. Müzik, video ve resim gibi işle ilgili olmayan dosya tiplerinin indirilmesi kesinlikle yasaktır. Kullanıcılar Internet'ten veri dosyaları yükleyebilirler, fakat bunları kullanmadan önce virüslere karşı kontrol etmelidirler.

- Kullanıcılar kendilerine verilen bilgisayarlar üzerine izin verilen yazılımlar dışında herhangi bir yazılım yüklememelidirler.

12.10.Uyarı İçeriği

- Kullanıcının, şirket dışına attığı e-postaların tümüne aşağıdaki şekilde bir yasal uyarı eklenecektir:

- “Internet uzerinden iletisimde zamaninda, guvenli, hatasiz ve viruslerden arindirilmis gonderim garanti edilemez.Gonderen taraf, hata ve unutmalardan dolayi sorumluluk kabul etmez.Mesajda yalnizca muhatabini ilgilendiren, kisiye veya kuruma ozel bilgiler yer aliyor olabilir.Mesajin muhatabi degilseniz, icerigini ve varsa ekindeki dosyalari kimseye aktarmayiniz veya kopyalamayiniz.Boyle bir durumda lutfen gondereni uyarip mesaji imha ediniz.Gostermis oldugunuz hassasiyetten dolayi tesekkur ederiz.”

- “Internet communications cannot be guaranteed to be timely, secure, error or virus-free. The sender does not accept liability for any errors or omissions. The e-mail message may contain confidential and/or privileged information. If you are not the intended recipient or have received this mail in error, please notify the sender immediately and delete this e-mail from your computer. Any unauthorized copying, disclosure or distribution of the material in this e-mail is strictly forbidden. Thank you for your cooperation.”

13. VERİ YEDEKLEME POLİTİKASI

13.1. Veri Yedekleme

- Kullanıcılar kendi bilgisayarları üzerinde yer alan değerli ve kritik bilgilerin güvenliği ve yedeklenmesinden sorumludurlar.
- Kullanıcı, yedekleme işlemini aşağıdaki kurallara istinaden, Veri Yedekleme Prosedürü dokümanında belirtildiği gibi yapmalıdırlar.
- Kullanıcının, şirket için kritik dosyalar dışında, şahsi mp3,avi,jpg vb. uzantılı dosyalarını yedekleme sunucusu üzerinde yedeklemesi kesinlikle yasaktır.
- Yedekleme sunucuları üzerinde düzenli olarak yapılan otomatik kontroller sonucu, günlük iş akışı ile ilgili olmayan ve sistemi gereksiz meşgul eden mp3,avi,jpg vb. uzantılı dosyalar, kullanıcı tarafından Bilgi Sistemleri Ve Teknolojileri Müdürlüğü sistem sorumlularından onay alınmadığı taktirde, kullanıcılara bilgi verilmeksizin silinecektir.
- Merkezdeki kullanıcının önemli verilerini yedekleyebilmesi için merkezi bir yedekleme sunucusu bulundurulmaktadır.
- Satış bölgeleri, büyük dolum tesisleri gibi kullanıcı sayısının fazla olduğu lokasyonlarda kullanıcının önemli datalarını yedekleyebilmeleri için lokal bir yedekleme sunucusu bulundurulmaktadır.
- Kullanıcı, önemli gördüğü bilgileri, yedekleme sunucusu üzerinde kendisi için ayrılmış klasöre yedeklemelidir.
- Az sayıda kullanıcısı olan lokasyonlarda, yedekleme sunucusu bulundurulamadığından, kullanıcı önemli gördüğü bilgileri, aynı lokasyonda bulunan diğer bir kullanıcının PC / Laptop'undaki bir klasöre Veri Yedekleme Prosedürü dokümanında belirtildiği gibi yedeklemelidir.
- Tek kullanıcısı olan lokasyonlarda ise kullanıcı, önemli gördüğü bilgileri, taşınabilir yedekleme cihazları (Flash memory, harici disk vb...) üzerinde yedeklemelidir.

14. İNTERNET KULLANIM POLİTİKASI

14.1. İnternet Kullanımı Kullanıcı Sorumlulukları

- Kullanıcı internete, sadece Bilgi Sistemleri Direktörlüğü'nün sağladığı internet erişim sistemleri üzerinden erişmek zorundadır. Bu erişim için gerekli ayarlar Bilgi Sistemleri Direktörlüğü tarafından ön tanımlı olarak tüm bilgisayarlar için yapılmıştır.

- Kullanıcıların internet imkânlarını iş amaçlı kullanmaları beklenmektedir.

- İnterneti kullanarak hiçbir yasa dışı faaliyette bulunulmamalıdır.

- Bir bilgisayar da oturum açmış (log-in olmuş) kişi, o bilgisayardan internet'te dolaşan kişi olarak kabul edilecektir. Masanızdan ayrılacağınız zaman, bilgisayarınızın oturumunu kapatmayı (log-out) veya ekranınızı kilitlemeyi (lock) unutmayın.

- Kullanıcı internet erişimi sırasında, kendilerine ve İşveren e ait tüm bilgileri (erişim şifreleri, şirket verileri, vs...) korumakla yükümlüdür.

- İşveren, kullanıcının internet erişimi sırasında yaptığı tüm işlemleri izleme hakkını saklı tutar.

- Kullanıcının internet çıkış izinleri, tanımlı olan internet çıkış profilleri üzerinden düzenlenir.

- Kullanıcılar profillere, bağlı oldukları gruplar ile atanırlar.

- Kullanıcı grupları, profil içerikleri ve gruplara atanmış profil tanımları Rol Bazlı Erişim Profilleri dokümanında belirtilmiştir.

- Yasaklı bir site veya site grubunun erişime açılabilmesi için kullanıcı, ekli olduğu profil adına Problem Bildirim ve Çözüm Politikası kapsamında servis masasından talebini gerçekleştirebilir.

- İzin talep edilen site Bilgi Güvenliği Yöneticisi tarafından uygun görülür ise profil erişimine açılır.

- Kullanıcı, herhangi bir internet mesaj panosuna, Firmaya gölge düşürecek ya da makul bir kişinin çirkin veya küfürlü bulacağı benzeri web tabanlı hizmetlere hiçbir mesaj iliştirilmemelidir.

- Yasaklı sitelere arasında bulunan bir site erişimi için sadece Bilgi Sistemleri Direktörlüğü ile irtibata geçiniz.

- Bu politika kapsamında ki her kişi gözledikleri ihlalleri sorumlu Sistem Operasyon ve Bilgi Güvenliği Birimi Yöneticisine rapor etmek zorundadır.

- Gerekmedikçe bir web sitesine e-posta adresinizi girmemelisiniz. Doldurduğunuz anketler veya diğer formlara adresinizi yazarsanız, istenmeyen mesajlar alma riskiyle karşılaşacaksınız.

- İşveren, kullanıcılarının internet erişimlerini hukuki boyut da ilgili kuruluşlar 5651 yasası kapsamında izler, günlüklerini tutar ve bu bilgiye erişme ve bu bilgiyi raporlama hakkını saklı tutar.

- İşveren, kullanıcının internet sisteminde gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü partilerle (kişilerle), emniyet kuvvetleriyle veya yargıyla kullanıcının izni olmadan paylaşma hakkını saklı tutar.

15. MOBİL CİHAZLARIN KULLANIM POLİTİKASI

15.1. Mobil Cihazların Kullanımı

- Mobil cihazlar üzerinde oluşturulmuş her türlü uygulama, kullanıcı kimlikleri gibi bilgiler bireylere özeldir ve paylaşılmamalıdır.

- Mobil cihazlar üzerinde bulunan usb portlarından herhangi bir depolama birimine veri çıkışı yapılmamalıdır. Bu kapsamda donanımların üzerinde bulunan usb portları kullanıma kapatılmıştır. Gerekli ve acil durumlarda usb portlarının Bilgi Sistemleri tarafından açılması için, kullanıcının yöneticisinden süreli ve onaylı bir e-posta alması gerekmektedir.

15.2. Eklerin Saklanması

- Gizli bilgiye erişim sağlayacak mobil cihazlar üzerinde verilerin kayıt altına alınması ve saklanması yasaktır. Mobil cihaz kullanıcıları yalnızca görme yetkisi olduğu bilgiye veya bilgilere erişmelidirler.

15.3. Mobil Cihazların Güvenliği

- Doğan Holding ağına erişim Bilgi Sistemleri (BS) departmanı tarafından belirlenen bağlantı yöntemi ile gerçekleştirilir. (Örn. APN, VPN)

- Doğan Holding ağına erişen tüm mobil cihazların virüs ihtiva eden uygulamalara karşı korunması sorumluluğu kullanıcılara aittir. Mobil cihaz üzerinde karşılaşılan istenmeyen e-postalara, eklentilere ve güvenilir olmayan bağlantılara dikkatle yaklaşılmalıdır ve şirket dışından gelen yeterli güvenliğe sahip olmayan bağlantılardan kaçınılmalıdır.

15.4. Mobil Cihazlar Üzerinde Elektronik Posta Sistemlerinin Kullanımı

- Kullanıcılar mobil cihazlar üzerinde, yalnızca yetkili Doğan Holding elektronik posta yazılımlarını kullanmalıdırlar (örn. MS Outlook, E-mail++). E-posta kullanım politikasında tanımlanmış kurallar mobil cihazlar aracılığı ile elektronik posta kullanımını kapsamaktadır.

15.5. Mobil Cihazlar Üzerine Yazılımazılım Yükleme

- Kullanıcılar mobil cihazlar üzerine Internet'ten veri dosyaları yükleyebilirler, fakat bunları kullanmadan önce virüslere karşı kontrol etmelidirler.

- Kullanıcılar kendilerine verilen mobil cihazlar üzerine izin verilen yazılımlar dışında herhangi bir yazılım yüklememelidirler.

16. BİLGİ GÜVENLİĞİ OLAYI RAPORLAMA ve RİAYET ETMEME DURUMLARI

- Kullanıcılar, Doğan Holding ağı ile ilgili tüm sorularını ve bilgisayar/yazılımla alakalı konuları BS Departmanına yönlendirmelidirler. Kullanıcılar, Doğan Holding BS Departmanının önceden yazılı bildirisi ve onayı olmadan şirket dışından bir uzmandan yararlanamazlar.

- Kullanıcılar, bu politikayı ihlal eden tüm şüpheli durumları ve herhangi bir elektronik bilginin kaybolması veya çalınması durumunu rapor etmek zorundadırlar. Var olduğu bilinen tüm ciddi bilgi güvenlik zayıflıkları rapor edilmelidir. Gizli bilgilerin ifşa edildiğinden şüphelenilen tüm olaylar rapor edilmelidir. Tüm bildirimler, ileri inceleme ve değerlendirme yapılması amacıyla hemen Bilgi Güvenliği Yöneticisi 'ne yönlendirilmelidir.

16.1. Riayet Etmeme Durumları

- BS Güvenlik Politikasında belirtilen politikaları yerine getirmeyen kişinin riayet etmeme durumunda olduğu varsayılır.

16.1.1. Etkileri

- Bir çalışan, politikalara riayet etmeyen kişi olarak tanımlandığında, önlemler anında yerine getirilmemişse, doğrudan bu durumdan eşit olarak sorumlu olan rapor etme müdürüne bildirilir.

- Bu durum çözülmediğinde, konuya ilişkin rapor hazırlanarak üst yönetim bilgisine sunulur.

16.2. Sorumluluklar ve Denetleme

- Denetleme – Bilgi Güvenliği Yöneticisi (veya eşdeğeri) tespit edilen tüm riayet etmeme durumlarını üst yönetime bildirmekten sorumludur.

- Devletin çıkarmış olduğu yasaların kuruluşlara getirmiş olduğu sorumlulukla birlikte gerek görülmesi durumunda kişisel kullanılan bilgisayarlar özel izlemeye alınır.

- Kullanıcı aktiviteleri ve sistemlere erişimleri ya da erişim denemeleri kayıt altına alınır, gerektiği durumlarda ilgili taraflara (yargı, emniyet v.b.) sunulur. Kullanıcıların Doğan Holding bünyesindeki sistem ve uygulamalar üzerinden gerçekleştirdiği işlemlerin kayıt altına alınır ve bu işlemler kullanıcı sorumluluğundadır.

17. DOKÜMANIN YAYINLANMASI VE SAKLANMASI

İşbu Politika basılı kağıt ve elektronik ortamda olmak üzere iki farklı ortamda saklanır. Kurum portalı ve internet sitesinde dokümanların güncel versiyonu yer alır.

Islak imzalı nüshalar Mali ve İdari İşler Başkan Yardımcılığı'nda ve kontrollü kopyalar Baş Hukuk Müşavirliği tarafından saklanır ve gerektiğinde Bölüm Yöneticisinin yazılı onayı ile Baş Hukuk Müşavirliği'nce imha edilir.

18. GÜNCELLEME PERİYODU

İşbu Politika en az yılda bir kez gözden geçirilir ve ihtiyaç halinde Dokümantasyon Yönetimi Prosedürü'nde belirlenen esaslar dahilinde güncellenir.

19. YÜRÜRLÜK

İşbu politika İcra Kurulu'nun kabulü tarihinde yürürlüğe girer.

20. YÜRÜRLÜKTEN KALDIRILMASI

Yürürlükten kaldırılmasına karar verilmesi halinde, işbu Politika'nın ıslak imzalı eski nüshaları Bölüm Yöneticisi yazılı onayı ile Baş Hukuk Müşavirliği tarafından iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve 5 yıl süre ile Mali ve İdari İşler Başkan Yardımcılığı tarafından saklanır.

DOKÜMAN KÜNYESİ

HAZIRLANMASI VEYA REVİZE EDİLMESİ					
Doküman Referans No	**Açıklama**	**Ad Soyad-Unvan**	**Bölüm**	**Revize Edilen Madde**	**Hazırlanma/ Revize Tarih**

KATKIDA BULUNULMASI				
Doküman Referans No	**Ad Soyad-Unvan**	**Katkıda Bulunan Bölüm**	**Gözden Geçirilen Sayfa / Madde**	**Tarih**

ONAY ve YÜRÜRLÜK			
Doküman Referans No	**Makam**	**Onay / Karar Tarihi-No**	**Yürürlük Tarihi**