ZİVER HOLDİNG A.Ş

BİLGİ VE İLETİŞİM TEKNOLOJİLERİNİN KABUL EDİLEBİLİR KULLANIMI POLİTİKASI

Doküman No	**KVKK_P6 VERSİYON 1.00**
Revizyon Tarihi	**-**
Yayın Tarihi	**-**
Sayfa	**3**

ZİVER HOLDİNG A.Ş.

BİLGİ VE İLETİŞİM TEKNOLOJİLERİNİN KABUL EDİLEBİLİR KULLANIMI POLİTİKASI

Ziver Holding Anonim Şirketi IT kaynaklarını kullanacak herkes aşağıda açıklanan hususları kabul etmiş sayılır:

1. IT kaynakları, Holdingin faaliyetlerinin yürütülmesi için tedarik edilen her türlü donanım, yazılım, hizmetler ve kaynakları ifade eder. Tüm bilgisayar ağları, kablolu veya kablosuz bilgisayarlar, yazıcılar, mobil cihazlar, depolama cihazları, görsel-işitsel sistemler ve Bulut hizmetleri IT kaynakları içerisinde değerlendirilir.

2. Her kullanıcı IT kaynaklarının güvenli kullanımı konusunda kendisine verilen tavsiyeleri anlayarak uygulamalı ve Bilgi Güvenliği farkındalığı eğitimlerine katılmalıdır;

3. Holdingin IT kaynaklarının kullanımı ve bu kaynakların Holding dışı kaynaklara erişim sağlanması için kullanımı sadece Holding faaliyetleri için gerekli olan araştırma, öğrenme, idari ve sair izin verilen kullanımlar ile sınırlı olmalıdır. Önceden izin alınmaksızın kişisel ticari çalışmalar için IT kaynaklarının kullanımı yasaktır;

4. Holding namına yürütülen faaliyetler sadece Holding tarafından sağlanan bilgi işlem araçları kullanılarak yerine getirilmelidir. Holding işlerini yürütmek için Holding dışı bilgi hizmetlerini kullanmak, Holding verilerini riske atar ve bu nedenle yeterli gerekçelendirme olmadan kullanılmaları yasaktır. Örneğin One Drive ve Gmail, Hotmail gibi e-mail servisleri yerine Holding e-mail servisi kullanılmalıdır.

5. Holdingin IT kaynaklarının bireysel amaçlarla kullanımı ancak Holding iş ve işlemlerini ya da diğer kullanıcıların vazifelerini yerine getirmesine engel olmadığı sürece uygundur. Holding wifi ağının eğlence amacıyla kullanımı da bu koşula tabidir.

6. Ağ anahtarları, dağıtıcı, kablosuz erişim noktaları ve yönlendiriciler gibi aktif ağ cihazlarının Holding ağına bağlanması yasaktır. Tüm IP adresleri yalnızca Holding tarafından tahsis edilecek ve yönetilecektir;

7. Çalışanlar önceden yazılı olarak açık bir şekilde izin verilmediği sürece Holding dışı misafir vb. kişilerin Holdingin bilgi işlem servislerine erişim sağlaması yasaktır;

8. Ziver Holding Anonim Şirketi, IT kaynaklarını kullanan her kullanıcı, IT Kaynaklarının Kullanım Koşulları ve ilgili tüm yasal ve diğer hükümler, düzenlemeler, kurallar ve uygulama kuralları dahil olmak üzere Holding Bilgi Güvenliği Politikasına uygun hareket etmekle mükelleftir. Özellikle, ancak bunlarla sınırlı kalmamak koşuluyla, her kullanıcı aşağıda yer alan bentlerde belirtildiği gibi hareket etmekle mükelleftir:

8.1 Holding tarafından kendisine tahsis edilen şifre ve kullanıcı adını kimseye ifşa edilmeyecek ve Şifre ve Kullanıcı Adları hakkında Uygulama Esaslarına uygun hareket edilecektir;

8.2 Holding nezdinde ya da haricinde izin verilen amaçlar haricinde IT kaynaklarına erişilmeyecek ya da diğer kişilerin izin verilmeyen amaçlarla bu kaynaklara ulaşmasına aracılık edilmeyecektir;

8.3 Ziver Holding Anonim Şirketi içerisinde ya da başka bir yerde herhangi bir IT kaynağına port taraması gibi izinsiz erişim, değişiklik, arızalandırma eylemleri gerçekleştirecek materyal ya da kaynaklar kullanılamaz ve ağın içerisine sokulamaz;

8.4 Saldırgan olarak değerlendirilebilecek veya Holdingin kurumsal itibarını zedeleyebilecek pornografik, pedofilik, cinsiyetçi, ırkçı, iftira niteliğinde, tehdit edici, karalayıcı, yasa dışı, ayrımcı veya terörist nitelikte görüntülü ya da sesli materyal içeren resimler veya metinler sergilenemez, sistem ve dosyalarda saklamaz, alınamaz veya iletmez;

8.5 Elektronik posta imzaları ve / veya başlıkları taklit edilemez, "zincirleme", "gereksiz" veya "taciz edici" e-postalar düzenlenemez ve / veya iletilemez, elektronik iletişimde başkalarının kimliğine bürünmek suretiyle başkaları adına işlem yapılamaz ve gereksiz veya saldırgan iletişimler oluşturmaz;

8.6 Ziver Holding Anonim Şirketi IT hizmetleri kapsamında sunduğu kaynaklara erişim için kullanılan tüm mobil cihazlar uygun şifreleme yazılımları kullanılarak şifrelenmiş ve pin kodu veya şifre ile korunur olması sağlanacaktır;

8.7 Holding ve üçüncü şahıslar tarafından sağlanan tüm materyallerin ve yazılımların telif hakkına saygı gösterilecek ve yazılım ve alınan veriler dâhil olmak üzere telif hakkı kapsamındaki materyaller telif hakkı sahibinin izni veya Holding tarafından sahip olunan lisan koşulları haricinde kullanılmayacak, indirilmeyecek, kopyalanmayacak, sistemde bulundurulmayacak veya tedarik edilmeyecektir;

8.8 Gerçek kişiler hakkındaki veriler işlenirken veri koruma mevzuatı hükümlerine uygun olarak işlemek (yani toplamak, kullanmak, paylaşmak ve imha etmek) için Holdingin Veri Koruma Politikasına uygun hareket edilecektir.

8.9 Holding IT kaynakları üzerinde kullanıcılar tarafından oluşturulan / sahip olunan / depolanan tüm bilgi varlıklarının, yasaklanan fiillerin işlenmesinden şüphelenilmesi durumunda, Holding veya yasal yetkililer tarafından denetime tabi tutulabileceği unutulmamalıdır. İlgili verilerin şifrelenmesi durumunda, kullanıcının şifre çözme anahtarını sağlaması zorunludur;

8.10 Herhangi bir platform aracılığıyla kullanılan her türlü materyal ve yazılım için lisans koşullarının ne olduğunu belirlenerek ilgili koşullara uygun hareket edilmelidir.

9. 56511 sayılı Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun Erişim sağlayıcının yükümlülükleri başlıklı 6. Maddesi gereği Holding, kanunda sayılan amaçlarla sınırlı olarak Holding tarafından alınan ya da gönderilen elektronik haberleşme trafik bilgilerini saklamak, bu bilgilerin doğruluğu, bütünlüğü ve gizliliğini sağlamak için gerekli tedbirleri alacaktır. Bahse

konu tedbirlerin uygulama usulleri Elektronik Haberleşme ve Elektronik Verilerin Denetlenmesi Hakkında Yönetmelik ile düzenlenmiştir.

10. Veri güvenliğini ilgilendiren bir olayın gerçekleşmesi ya da gerçekleşmesinden şüphe edildiği durumlarda IT Departman Sorumlusu, olayın bertaraf edilmesi ya da doğacak zararların azaltılması için gerekli olduğunu düşündüğü kullanıcıların sisteme erişimini engellemek ya da ağa bağlı olan cihazları incelemek gibi tedbirleri ivedilikle alabilir.

11. Daha fazla incelemenin gerekli olması durumunda, IT Departmanı, Holding Yönetim Kurulunun açık izni ile Holding ağındaki herhangi bir sistemi incelemek için gerekli tedbirleri alabilir.

12. Yürürlükteki yasal zorunluluklar haricinde, Holding, kendisi tarafından sağlanan ve / veya yönetilen herhangi bir IT kaynağının doğrudan veya dolaylı olarak kullanımından veya kullanımının önlenmesinden kaynaklanan herhangi bir kayıp, hasar veya olumsuzluktan sorumlu tutulamaz.

13. Her ne kadar Ziver Holding Anonim Şirketi kişisel ve diğer verilere yetkisiz erişim, değişiklik yapılması, verilerin ifşa edilmesi, imha veya kaza sonucu kayıplara karşı uygun güvenlik önlemlerini almakta ise de, kullanıcıya verilerin güvenliği, gizliliği veya bütünlüğü hakkında hiçbir garanti veya taahhütte bulunmaz.

14. Kullanıcıların adı, adresi, fotoğrafı, medeni durumu, e-posta adresi, oturum açma adı, takma adı, Holding kimlik kartı ve diğer ilgili bilgiler, yönetim ve sistem kullanımının denetlenmesi gibi diğer amaçlarla kullanılmak üzere bilgisayar teknolojileri ile işlenmiş ortamlarda saklanacaktır.

15. Yukarıda zikredilen koşullar Holdinge ait olmayan kişisel dizüstü bilgisayarlar, ev bilgisayarları gibi cihazların Holding ağını kullandığı süre boyunca doğrudan ve / veya VPN aracılığıyla Holding ağına bağlandıkları kullanımlar için de geçerli olacaktır.

16. Yukarıda zikredilen koşulların ihlali, tüm Holding IT kaynaklarının kullanma yetkisinin belirli süreler için askıya alınmasını ve / veya ceza verilmesi ile sonuçlanabilecek disiplin soruşturması açılmasına neden olabilir. Ağır ihlal durumlarında Holding ilgili ile akdedilen iş sözleşmesinin feshi ve ilgili kullanıcı aleyhinde hukuk ve ceza davaları açma hakkını saklı tutar.

17. Holdingin IT imkânlarını kullanan ve/veya Holding tarafından sağlanan internet bağlantısı kullanan misafirler için Holding çalışanları vekil olacaktır. Vekil olarak hareket eden çalışanlar misafirlerinin eylemlerini tespit etmeli ve sorumluluğunu almalıdır.