ZİVER HOLDİNG A.Ş

TEMİZ MASA TEMİZ EKRAN POLİTİKASI

Doküman No	**KVKK_P10 VERSİYON 1.00**
Revizyon Tarihi	**-**
Yayın Tarihi	**-**
Sayfa	**3**

1) AMAÇ

Temiz Masa Temiz Ekran Politikamızın amacı, normal çalışma saatleri süresince ve dışında bilgiye yetkisiz erişim, bilgi kaybı ve hasarı risklerini azaltmak amacıyla kâğıtlar ve kaldırılabilir depolama ortamları ve kişisel bilgisayarlar için gerekli şartları tanımlamaktır.

2) KAPSAM

Bu politika başta teknik ve idari olmak üzere Ziver Holding bünyesinde çalışan tüm personeli kapsamaktadır.

3) POLİTİKA

3.1. Ziver Holding'e ait uygulamalarda kullanılan parolalar, iş arkadaşları da dâhil olmak üzere kimse ile paylaşılmamalı, parolalar yazılı olarak post-it ya da not kâğıtlarına yazılarak pano, bilgisayar ekranı, klavye gibi donanımlara yapıştırılmamalıdır.

3.2. Evrak ve dokümanların güvenliği için çalışma saatleri dışında ofis kapılarının kilitli tutulması gerekmektedir.

3.3. Evrak ve dokümanlardaki bilgilerin farklı kişiler tarafından ele geçirilmemesi için klasörlerde saklanmalıdır.

3.4. Hassas, özel nitelikli kişisel bilgi içeren evrak klasörleri ve Holdinge ait antetli kâğıtlar kilitli dolaplarda saklanmalıdır.

3.5. Kâğıtların çöp kutularına atılması yerine, kâğıt imha makinalarında kırpılmasına dikkat edilmesi gerekir.

3.6. Hassas ve kritik bilgi içeren bilgi ve belgeler ağ üzerinden paylaşılamaz.

3.7. Masa üstü doküman sayısını artırmamak için mümkün olduğu kadar elektronik dokümanların yazıcıdan çıktılarının alınmamasına dikkat edilmelidir.

3.8. Masa üzerinde kartvizit kutuları, kişisel ajandalar, değerli bilgilere sahip dokümanlar bırakılmaz ve bunların kilitli çekmecelerde muhafaza edilmesi gerekir.

3.9. Masa çekmecelerinin anahtarları, ev ve araba gibi özel anahtarlar, kasa anahtarları masa üzerinde bırakılmamalıdır.

3.10. Ziver Holding'e ait kritik bilgi içeren dokümanlar başkaları tarafından fark edilmeyecek şekilde muhafaza edilmelidir.

3.11. Çalışanlarımızın maaş bordrosu gibi kişisel gizli bilgileri başkaları tarafından fark edilmeyecek şekilde muhafaza edilmelidir.

3.12. Çalışanlarımız telefon konuşmaları sırasında hassas bilgilerin açığa çıkmaması için tedbirli davranmalıdır.

3.13. Bilgi ve veri alışverişinden önce dış tarafların kimliklerinin tespit edilmesi gerekir.

3.14. Ziver Holding bünyesinde kullanılan toplantı salonlarında gizli ve kritik bilgi içeren dokümanları toplantı sonrasında ilgili salonlarda bırakmamalı ve salonlardaki tahtalara alınmış notlar silinmelidir.

3.15. Gizlilik içeren bilgilerin umumi yerlerde konuşulmaması gerekir.

3.16. Gizlilik içeren bilgiler, telefonlarda dışarıya ses açık olarak görüşülmemelidir. Faks yoluyla gizlilik içeren herhangi bir bilgi gönderilmemelidir.

3.17. Bilgisayar gibi elektronik ortamlarda bulunan bilginin korunması için çalışma saatleri dışında ofis kapılarının kilitli tutulması gerekir.

3.18. Kısa süreli ayrılmalarda dahi, cep telefonu, taşınabilir bellek, harici hard disk, CD, DVD gibi eşyalar çalışma masası üzerinde bırakılmamalıdır.

3.19. Bilgisayarlar gözetimsiz bırakıldığında kapatılmalı veya parola kullanılarak korunmalıdır. Ekran koruyucu 5-10 dakika arasında devreye girmelidir ve şifre koruması olmalıdır.

3.20. Yazıcıların üzerinde kişisel bilgileri ve gizli bilgileri içeren dokümanlar(müsvedde olsalar bile)bırakılmamalıdır.

3.21. Fotokopi cihazlarının yetkisiz kullanımı önlenmelidir.

3.22. Fotokopi cihazlarının belleğinde bulunan kritik ve hassas bilgiler silinmelidir.

3.23. Hassas ve sınıflandırılmış bilgi içeren ortamlardaki bilgiler yazıcıdan çıktı alındıktan sonra hemen silinmelidir.

3.24. Parolalar yazılı olarak saklanmamalı ve gizli tutulmalıdır.

3.25. Kullanılan parolalar tahmin edilebilir olmamalıdır. Parolayı oluşturan kişi ile ilgili bilgiler içermemelidir. Ardışık, tümü sayısal ya da tümü alfabetik karakterlerden oluşmamalıdır. Holdingimizin Kullanıcı Şifrelerinin Belirlenmesi, Kullanımı Ve Korunmasına İlişkin Usul Ve Esaslar Hakkında Yönetmelik kurallarına göre belirlenmelidir.

3.26. Personel; bilgisayarındaki, taşınabilir belleğindeki, harici diskte ve benzeri depolamanın mümkün olduğu ortamlardaki gizlilik dereceli bilgi içeren her türlü belgenin güvenliğini sağlamakla yükümlüdür. Taşınabilir bellek veya harici diske gizli veya önemli veri konulması gerekiyorsa şifrelenerek korunması gerekmektedir.

3.27. Gizli belgelerin, parolaların, adreslerin, özellikle taşınabilir bellek, e-posta, sosyal medya gibi alanlarda paylaşılmamasına dikkat edilmelidir.

3.28. Bilinmeyen e-posta ve haber gruplarına üye olunmamalıdır.

3.29. Elektronik posta ortamında kişisel parola bilgileri paylaşılmamalıdır.

3.30. Silinebilir ortamlara kaydedilmiş olan gizli bilgilerin kullanımdan sonra etkin yöntemler kullanılarak geri dönülmeyecek şekilde silinmesi gerekir.

3.31. Kurumsal işlerin yapıldığı bilgisayarlar personelin kendi sorumluluğundadır. Kurum bilgisayarlarını personel haricinde yetkisiz kullanıcılara teslim edilmemelidir.

4) YAPTIRIM

İşbu Politika kapsamında vazedilen hususlara uygun hareket etmek noktasında ihmal sergileyen çalışanlar görevde ağır ihmal göstermiş sayılarak Disiplin Tüzüğünde belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.

Hazırlayan	**Kontrol Eden**	**Onaylayan**