**STEP MEDİA REKLAM ve PAZARLAMA DANIŞMANLIĞI**

**TEMİZ EKRAN VE TEMİZ MASAÜSTÜ POLİTİKASI**

1. **AMAÇ**

Bu politika, **STEP MEDİA REKLAM ve PAZARLAMA DANIŞMANLIĞI** bünyesindeki kâğıtlar, taşınabilir depolama ortamları ve kişisel bilgisayar için mesai saatleri içinde ve dışında bilgiye yetkisiz erişim ve bilginin hasar görmesi gibi riskleri azaltmak amacıyla gerekli olan şartları tanımlamak amacıyla hazırlanmıştır.

1. **KAPSAM**

Bu politika, **STEP MEDİA REKLAM ve PAZARLAMA DANIŞMANLIĞ** bünyesinde çalışan tüm personeli kapsamaktadır.

1. **POLİTİKA**
2. **ÇALIŞMA MASALARI**
	1. Kullanıcılar kendi çalışma masası ve bilgisayarından sorumludur.
	2. Masa üzerinde kartvizit kutuları, kişisel ajandalar, değerli bilgilere sahip dokümanlar bırakılmaz ve bunların kilitli çekmecelerde muhafaza edilmesi gerekir.
	3. Masa çekmecelerinin anahtarları, ev ve araba gibi özel anahtarlar, kasa anahtarları masa üzerinde bırakılmamalıdır.
	4. Kuruma 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. **OFİSLER VE ÇALIŞMA ODALARI**
	1. Evrak ve dokümanların güvenliği için çalışma saatleri dışında ofis kapılarının kilitli tutulması gerekmektedir.
	2. Evrak ve dokümanlardaki bilgilerin farklı kişiler tarafından ele geçirilmemesi için klasörlerde saklanmalıdır.
	3. Hassas bilgi içeren evrak klasörleri ve kuruma ait başlıklı kâğıtlar kilitli dolaplarda saklanmalı, bunların saklanmasında ve paylaşılmasında “ÖZEL VERİ GİZLİLİK POLİTİKASI” ilkeleri dikkate alınmalıdır.
	4. Şirkete ait kişisel bilgi içeren dokümanlar başkaları tarafından fark edilmeyecek şekilde muhafaza edilmelidir.
	5. Bilgisayar gibi elektronik ortamlarda bulunan bilginin korunması için çalışma saatleri dışında ofis kapılarının kilitli tutulması gerekir. Kısa süreli ayrılmalarda dahi, cep telefonu, taşınabilir bellek, harici hard disk, CD, DVD gibi eşyalar çalışma masası üzerinde bırakılmamalıdır.
	6. Personelin kişisel gizli bilgileri maaş bordrosu gibi başkaları tarafından fark edilmeyecek şekilde muhafaza edilmelidir.
4. **ÇÖP KUTULARI VE KAĞIT ORTAMINDAKİ BELGELERİN İMHASI**
	1. Kâğıtlar kesinlikle çöp kutularına atılmamalı, kâğıt imha makinalarında kırpılmalıdır.
	2. Her türlü verinin silinmesi, imhası konusunda “**KİŞİSEL VERİLERİN SİLİNMESİ VE İMHASI**” politikası kuralları uygulanmalıdır.
5. **YAZICILAR VE FOTOKOPİ MAKİNELERİ**
	1. Masa üstü doküman sayısını artırmamak için mümkün olduğu kadar elektronik dokümanların yazıcıdan çıktılarının alınmamasına dikkat edilmelidir.
	2. Yazıcılar şifre ile korunmalı, kullanıcı ancak şifresini girdikten sonra ortak alandaki yazıcıdan çıktı alabilmelidir.
	3. Yazıcılarda çıktı alan personel, işlem sona erdikten sonra, bunun üzerinde kağıt bırakmadığına emin olmalı ve kontrol etmelidir.
	4. Fotokopi cihazlarının yetkisiz kullanımı önlenmelidir. Fotokopi cihazlarının belleğinde bulunan kritik ve hassas bilgiler silinmelidir.
6. **TELEFON KONUŞMALARI VE FAKS**
	1. Personel telefon konuşmaları sırasında hassas bilgilerin açığa çıkmaması için tedbirli davranmalıdır. Bilgi ve veri alışverişinden önce dış tarafların kimliklerinin tespit edilmesi gerekir.
	2. Gizlilik içeren bilgilerin umumi yerlerde konuşulmaması gerekir.
	3. Gizlilik içeren bilgiler, telefonlarda dışarıya ses açık olarak görüşülmemelidir.
	4. Faks yoluyla gizlilik içeren herhangi bir bilgi gönderilmemelidir.
7. **BİLGİSAYARLAR**
	1. Bilgisayarlar gözetimsiz bırakıldığında kapatılmalı veya parola kullanılarak korunmalıdır.
	2. Ekran koruyucusu aktif hale getirilmelidir.
	3. Güvenlik politikası gereği bilgisayarlar, şifre korumalı ekran koruyucu ile korunurlar. Bu doğrultuda kullanıcılar bilgisayarları başında olmadıkları zamanlarda bilgisayar ekranlarını kilitlemelidir. (Bilgisayarlar “Ctrl+Alt+Delete” ya da “  + L” tuş kombinasyonlarından biri kullanılarak kilitlenebilir).
	4. Parola korumalı ekran koruyucu ile korunmadığını fark eden kullanıcılar, BGYS Sorumlusuna durumu haber vermekle yükümlüdür.
	5. Hassas bilgi içeren ortamlardaki bilgiler yazıcıdan çıktı alındıktan sonra hemen silinmelidir.
	6. Parolalar yazılı olarak saklanmamalı ve gizli tutulmalıdır.
	7. Kullanılan parolalar tahmin edilebilir olmamalıdır. Parolayı oluşturan kişi ile ilgili bilgiler içermemelidir. Bu konuda “Bilgi Güvenliği Politikası” ilkeleri ve kuralları uygulanmalıdır.
	8. Personel bilgisayarındaki, Taşınabilir belleğindeki, harici diskte ve benzeri depolamanın mümkün olduğu ortamlarda ki gizlilik dereceli bilgi içeren her türlü belgenin güvenliğini sağlamakla yükümlüdür. Taşınabilir bellek veya harici diske gizli veya önemli veri konulması gerekiyorsa kriptolayarak korunması gerekmektedir.
	9. Gizli belgelerin, parolaların, adreslerin, özellikle taşınabilir bellek, e-posta, sosyal medya gibi alanlarda paylaşılmamasına dikkat edilmelidir. Bilinmeyen e-posta ve haber gruplarına üye olunmamalıdır.
	10. Elektronik posta ortamında kişisel parola bilgileri paylaşılmamalıdır.
	11. Kurum dışında bilgisayar ekranından veya basılı dokümanlardan hassas bilgilerin başkalarınca izlenme riskinin daha yüksek olduğu unutulmamalı, halka açık mekânlarda hassas bilgiler görüntülenmemelidir.
	12. Silinebilir ortamlara kaydedilmiş olan gizli bilgilerin kullanımdan sonra etkin yöntemler kullanılarak geri dönülmeyecek şekilde silinmesi-imha edilmesi gerekir. Bu konuda Şirketin “Kişisel Verilerin Silinmesi Ve İmha Edilmesi“ politikası ilke ve kuralları uygulanır.
	13. Kurumsal işlerin yapıldığı bilgisayarlar personelin kendi sorumluluğundadır. Şirket bilgisayarlarını personel haricinde yetkisiz kullanıcılara teslim edilmemelidir.
8. **TOPLANTI SALONLARI VE ORTAK ALANLAR**
	1. Toplantı salonlarında, tahta gibi alanlarda yazılan bilgiler toplantı bitiminde mutlaka silinmelidir.
	2. Toplantı salonlarında sunum yapılan araçlarda ve bu araçların üzerinde veri kesinlikle bırakılmamalıdır.
9. **YAPTIRIMLAR**

“**TEMİZ EKRAN VE TEMİZ MASAÜSTÜ**” politikasına aykırılık durumunda, İşveren ihlalin ağırlığına göre iş sözleşmesinin haklı nedenle tazminatsız olarak feshi de dahil olmak üzere, disiplin cezası uygulama yetkisine sahiptir.

İşverenin, Bilgi güvenliği ihlalleri nedeniyle ortaya çıkan zararı çalışana rücu hakkı saklıdır.