UZAKTAN ÇALIŞAN PERSONEL İÇİN BİLGİ GÜVENLİĞİ VE KAYIT YÖNETİMİ REHBERİ

Dünya genelinde bütün şirketler COVID-19 pandemisi sebebiyle daha önce eşi görülmemiş zorluklarla karşı karşıya kalmıştır. Çok sayıda personelin uzaktan çalıştığı şu günlerde, Iron Mountain olarak, özel bilgilerinizin güvenliği ve gizliliğinin sağlanması adına uyulması gereken iyi örnekleri sizlerle paylaşıyoruz.

İster ofisinizden, ister evinizden olsun; kayıt ve bilgi yönetimi tek bir şekilde yapılır ve bu da bütün çalışanların şirket kural ve politikalarına uyumundan geçer. Şartlar göz önünde bulundurulduğunda; çalışanlar mevcut kriz yönetimi ile meşgulken ihtiyaçları olan açık bir iletişimin yanında, kurallar ve prosedürlerle ilgili hatırlatmalardır.

"UZAKTAN ÇALIŞAN PERSONELİNİZE BİLGİ YÖNETİMİ VE GÜVENLİĞİ KONUSUNDAKİ İYİ UYGULAMALAR HAKKINDA HATIRLATMALARDA BULUNMAK BÜYÜK ÖNEM TEŞKİL ETMEKTEDİR. STRESLİ ZAMANLARDA İNSANLAR BASİT ÇÖZÜMLERE İHTİYAÇ DUYARLAR. BU YÜZDEN İLETİŞİMİNİZİ OLABİLDİĞİNCE AÇIK, NET VE ÖZ TUTUN."
ARLETTE WALLS
Iron Mountain, Global Kayıtlar & Enformasyon Müdürü

KURUM POLİTİKALARI

Kurum politikalarınızın bütün çalışanlarınız tarafından ulaşılabilir olduğundan emin olun ve bu bilgilerin kurum içi ağınızda nerede saklandığı konusunda çalışanlarınızı güncel tutun. Emin olamadığınız konularla ilgili aşağıdaki başlıklara başvurabilirsiniz:

Kayıt ve bilgi yönetimi
Güvenlik
Gizlilik
İK uzaktan çalışma rehberi
Aygıt güvenliği:

- Kullanılabilecek cihazlar ve bilgi ve belgelerin doğru kullanım şekli
- Kişisel cihazlara kopyalanan kayıtlar
- Kişisel e-posta hesabınıza gönderdiğiniz şirket kayıtları
- Kişisel yazıcıların kullanımı
- Harici disk ve flash disk kullanımı

Yukarıda bahsi geçen konularla ilgili gelebilecek soruları cevaplamak üzere ilgili kontakt bilgisini de bilgilendirme e-postalarında çalışanlarınızla paylaşmayı unutmayınız.

GÜVENLİK

Uzaktan çalışan personel, kullandıkları cihazlar ve bilgi güvenliği konusunda çok daha dikkatli davranmalıdır.

- Cihazlarınızı kullanmadığınız zamanlarda güvenli bir yerde saklayarak, yetkisi olmayan kişilerin erişiminden koruyun.
- Hane halkınızdaki kişilerle cihazlarınızı ve hesaplarınıza ait kullanıcı bilgilerini paylaşmayın.
- Bütün belge ve içerikleri masaüstünüz yerine şirketinizin güvenli ağı üzerinde saklayın. Masaüstünüze kaydettiğiniz bilgilerin güvenli bir şekilde saklanmasının mümkün olmadığını unutmayın.
- Kayıt ve belgeleri yazdırmaktan kaçının.
- Mutlaka yazdırmanız gereken belgeler varsa bunları güvenli bir yerde saklayın; şirketinize ait kağıt belge ve evrakları çöpe veya geri dönüşüm kutusuna atmayın. Yazdırdığınız belgeleri aşağıda belirtilen imkanlara erişim sağlayana kadar güvenli bir yerde saklayın; ofisinize döndüğünüzde kağıt öğütücü kullanın. Şirketinizin kağıt imha politikasına uygun olmak koşuluyla ofisinizde kişisel kağıt öğütücünüzü kullanın. Güvenli kağıt imha hizmeti sunan bir firmadan yardım alın.
- Evinizden veya halka açık alanlardan (COVID-19 kısıtlamalarının izin verdiği çerçevede) internete bağlanırken ortak ağ bağlantıları yerine bildiğiniz güvenli ağları tercih edin.
- Bilgisayarınızdaki verileri korumak amacıyla ekran gizlilik filtresi kullanın.
- Çalışanlarınızı siber saldırı, korsan yazılımlar ye oltalama (phishing) saldırılarına karşı uyanık olmaları konusunda bilinçlendirin ve Koronavirüs salgınının yayılmasını fırsat bilerek siber saldırı ve korsanlık faaliyetlerinin artabileceği konusunda uyarın.

GİZLİLİK

Kişisel veri içeren bilgi ve belgelerle çalışırken uyumluluk konusundaki gereklilikleri göz önünde bulundurmalısınız. Bu bilgiler yetkili olmayan kimselerle hiçbir şekilde paylaşılmamalıdır. Kişisel ve hassas verilerin yanı sıra, fikri mülkiyet de dahil, herhangi bir veri ihlali veya kötüye kullanım riskine maruz bırakılmamalıdır.