Çalışanın yaşam döngüsü

ve BT yöneticisinin rolü

Digital Security
Progress. Protected.

İşe alımdan günlük çalışmaya ve nihayetinde işten ayrılmaya kadar, her çalışanın bir kuruluştaki yolculuğu, her biri kendine özgü BT gereksinimleri olan farklı aşamaları kapsar. Şirketinizin sorunsuz ve güvenli bir şekilde çalışmasını sağlamak için BT ekibinin her adımda iyi hazırlanmış olması çok önemlidir.

Her aşama için net bir yol haritanız var mı? BT süreçlerinizin en iyi uygulamalarla uyumlu olduğundan emin misiniz? Bu kontrol listesi, çalışanların çeşitli iş hayatı aşamalarında BT uzmanlarına rehberlik etmek ve sorumluluklarını etkili bir şekilde yerine getirmelerine yardımcı olmak ve kurumlarının dijital ortamını korumak için tasarlanmıştır.

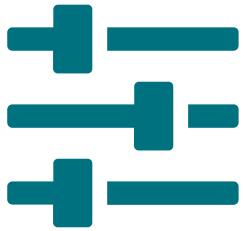
Kontrol listesi nasıl kullanılır?

İşe alma ve işten çıkarma kontrol listesi, kuruluşunuzun dijital altyapısı, güvenlik ve verimliliğini korumak için değerli bir referans noktasıdır. Çalışanların yaşam döngüsünün her aşaması için gerekli tüm adımları göz önünde bulundurmanıza yardımcı olacağından, hızlı bir referans için belgeyi yazdırabilirsiniz. Önemli bir şeyi unutmamak için kontrol listesini tekrar gözden geçirin.

İşe alırken

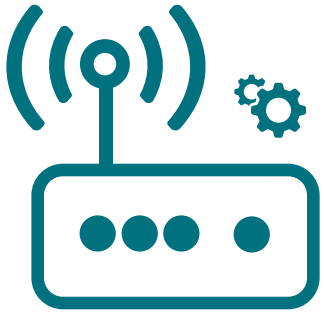
Digital Security
Progress. Protected.

1. Yeni çalışanlar için cihazların hazırlanması:



- Donanım varlıklarını atayın ve uygun şekilde etiketleyin.
- Monitörler, yerleştirme istasyonları, klavyeler ve fareler dahil olmak üzere gerekli tüm aksesuarları bulun.
- Söz konusu cihazları yeni çalışanlar için hazırlayın:
  - ☐ Gerekli tüm donanım ve yazılımın kurulması ve sağlanması
  - ☐ E-posta hesaplarını ve erişim izinlerini yapılandırma
  - ☐ Güvenlik önlemlerini ve kullanıcı profillerini ayarlama
  - ☐ Cihazı kullanıcının rolü ve gereksinimleri ile uyumlu olacak şekilde özelleştirme

2. İlk gün devir teslim:



- Yeni çalışanlara sahadaki ilk oturum açma işlemlerinde yardımcı olun.
- Çalışanların parolalarını ayarlamalarına yardımcı olun.
- Her şeyin düzgün çalıştığından emin olmak için kullanıcıyla birlikte bir cihaz kontrolü yapın.
- Güvenlik, Wi-Fi kurulumu ve diğer temel konuları kapsayan temel bir talimat sayfası hazırlayın.
- Yeni çalışanın devir teslim protokolünü imzaladığından emin olun.

3. Yönetmelikler ve kılavuzlar:

- Çalışanların kullanması gereken uygulamalar ve yazılımlar için bir liste ve yönergeler paylaşın.
- Örneğin, çalışanlarınızı çeşitli şirket politikaları hakkında bilgilendirin:
  - ☐ BT/Siber Güvenlik Politikası
  - ☐ KVKK/Veri Koruma Politikası
  - ☐ Uzaktan Çalışma Politikası
  - ☐ Sosyal Medya Politikası
  - ☐ BYOD (Kendi Cihazını Getir) Politikası

BYOD (Kendi Cihazını Getir) Politikası

BYOD sistemi günümüzde oldukça popülerdir, bu da çalışanlarınıza şirketinizin güvenliğini tehlikeye atmadan cihazlarını kişisel ve iş amaçlı kullanmaları konusunda talimat vermeniz gerektiği anlamına gelir. İşte BYOD politikasının kapsaması gereken bazı konular:

- ☐ **BYOD programına kimler katılabilir?**
- ☐ **İlke kapsamında izin verilen ve desteklenen cihazların, işletim sistemlerinin ve platformların listesi**
- ☐ **Parola gereksinimleri**
- ☐ **Veri şifreleme gereksinimleri**
- ☐ **Uzaktan silme işlemi açıklaması**
- ☐ **Veri erişimi ve kullanım sınırlamaları**
- ☐ **Kişisel cihazlar için sağlanan BT desteğinin seviyesinin netleştirilmesi**
- ☐ **İzleme ve denetim özellikleri**
- ☐ **Güvenlik ve uyumluluk açısından çalışan sorumlulukları**
- ☐ **Cihazın kaybolması veya çalınması durumunda yapılması gerekenler**
- ☐ **İş sona erdiğinde ne yapılmalı**

İstihdam süresince

Digital Security
Progress. Protected.

1. Siber güvenlik eğitimi:

- Çalışanları siber güvenlik tehditleri ve en iyi uygulamalar konusunda sürekli olarak eğitin.

Siber farkındalık kültürü nasıl oluşturulur ve güvenlik yorgunluğu nasıl önlenir?

- ☐ Eğitimi interaktif ve faydalı hale getirmek için İK departmanı ile işbirliği yapın.
- ☐ Genellikle yıllık tek bir eğitim etkinliğinden daha etkili olan daha kısa, daha sık eğitim oturumları uygulayın.
- ☐ İçeriği ilişkilendirilebilir kılmak için deneyimlerinizden gerçek hayat hikayeleri ve örnekler paylaşın.
- ☐ Çalışanların ilgisini çekmek için oyunlar, testler ve simülasyonlar gibi eğlenceli formatlardan yararlanın.
- ☐ Çalışanları korkutarak siber farkındalıklarını artıramazsınız. Bu yaklaşımı kullanırsanız, herhangi bir hatayı veya potansiyel siber tehdidi bildirmekten korkmaları daha muhtemel olacaktır.
- ☐ Sorulara açık olun ve çalışanlarınızın size ihtiyaç duyduklarında yardım etmek için orada olduğunuzdan emin olun.

2. En az ayrıcalıklı erişim:

- En az ayrıcalıklı erişim ilkesine uyulduğundan emin olun.
- Erişim izinlerini düzenli olarak gözden geçirin ve buna göre ayarlayın.
- Veri sızıntılarını önlemek için dosya paylaşımını ve harici adreslere e-posta yönlendirmeyi devre dışı bırakın.

3. Cihaz bakımı:

- Çalışanların cihazlarının en son güvenlik yamaları ve yazılım güncellemeleriyle güncel olduğunu düzenli olarak doğrulayın. Buna hem şirket tarafından verilen hem de iş için kullanılan kişisel cihazlar dahildir.

4. Uzaktan çalışma kuralları:

- Şirketiniz BYOD sistemini takip etmiyorsa, iş görevleri için kişisel cihazların kullanılmamasını tavsiye edin.
- Güvenli bağlantılar için Sanal Özel Ağ (VPN) kullanımını teşvik edin.
- Hassas veriler için şifreleme kullanımını teşvik edin.
- Yetkisiz erişimi önlemek için güçlü Wi-Fi parolasının önemini vurgulayın.
- Tüm uzak cihazlarda uç nokta korumasının etkin ve güncel olduğundan emin olun.

İşten ayrılırken

Digital Security
Progress. Protected.

1. Hesap ve erişim yönetimi:

- Ayrılan çalışanın erişiminin olduğu tüm uygulama ve hizmetlerin izinlerini iptal edin.
- Çalışanın kullandığı tüm şirket cihazlarındaki parolaları sıfırlayın.

2. Fiziksel erişim ve donanım:

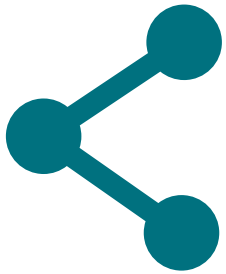
- Erişim kartları ve anahtarlar da dahil olmak üzere bina erişimini iptal edin.
- Dizüstü bilgisayarlar, akıllı telefonlar ve diğer donanımlar da dahil olmak üzere ayrılan çalışana verilen tüm şirket cihazlarını toplayın ve geri alın.

3. İzleme ve veri koruma:

- İşten ayrılma süreci boyunca davranışlarını izlemek için ayrılan çalışanla düzenli iletişim kurun.
- Ayrılan çalışanın hesapları ve sistemleriyle ilişkili olağandışı veya yetkisiz faaliyet olup olmadığını kontrol etmek için izleme ve kayıt araçlarının son bir incelemesini yapın.
- İşe alım sırasında veya sonrasında cihazlara veya verilere yetkisiz erişimi ortadan kaldırmak için bir Veri Kaybı Önleme (DLP) çözümü kullanmayı düşünün.

4. Son gün prosedürleri:

- Donanım devir tesliminin tamamlandığından emin olun.
- Daha fazla erişimi önlemek için çalışanın hesaplarını engelleyin.
- Şirket verilerini kaldırmak için çalışanların cihazlarında güvenli bir silme işlemi gerçekleştirin.



ESET Hakkında

ESET®, 30 yılı aşkın süredir dünya çapında işletmeleri, kritik altyapıları ve tüketicileri giderek karmaşıklaşan dijital tehditlere karşı korumak için sektör lideri BT güvenlik yazılımları ve hizmetleri geliştirmektedir. Uç nokta ve mobil güvenlikten uç nokta algılama ve müdahaleye, şifreleme ve çok faktörlü kimlik doğrulamaya kadar ESET'in yüksek performanslı, kullanımı kolay çözümleri, kullanıcıları güvende tutmak ve işletmelerin kesintisiz çalışmasını sağlamak için savunmaları gerçek zamanlı olarak güncelleyerek 7/24 dikkat çekmeden korur ve izler. Gelişen tehditler, teknolojinin güvenli kullanımını sağlayan gelişen bir BT güvenlik şirketi gerektirir. Bu, ESET'in dünya çapında ortak geleceğimiz için çalışan Ar-Ge merkezleri tarafından desteklenmektedir. Daha fazla bilgi için www.eset.com.tr adresini ziyaret edin ve bizi LinkedIn, Facebook ve Twitter (X) üzerinden takip edin.

ESET'ten işletmeler için yenilikçi yeni nesil dijital güvenlik

İhlalleri sadece durdurmuyoruz - önlüyoruz

KEŞFEDİN

Digital Security
Progress. Protected.