Amaç

Bu politikanın amacı **MERSİN TEKNOLOJİ GELİŞTİRME BÖLGESİ KURUM VE İŞLETİCİ TİC. A.Ş.** Girişimcilerinin belirtmiş ve belirtmemiş olduğu gizli bilgisinin mahremiyeti hususunda personelimizin uyulması gereken kuralları tanımlamaktır. Girişimcinin gizli bilgisi kapsamına ticari, tasarım, imalat, fatura vs gibi girişimciyi rahatsız edebilecek konular girmektedir.

Kapsam

Bu politika, **MERSİN TEKNOLOJİ GELİŞTİRME BÖLGESİ KURUM VE İŞLETİCİ TİC. A.Ş.** girişimcisine karşı yerine getirmekle görevli olduğu gizlilik prensibini ve tüm çalışan personeli kapsamaktadır.

Sorumluluk

Bu politikanın kontrolünden **Genel Müdür** ve **Kalite Yönetim Temsilcisi**, uygulanmasından ve dokümanların muhafazasından **MERSİN TEKNOLOJİ GELİŞTİRME BÖLGESİ KURUM VE İŞLETİCİ TİC. A.Ş.** içindeki tüm bölümler ile birlikte **Kalite Yönetim Temsilcisi** sorumludur.

Tanımlar ve Kısaltmalar

MERSİN TEKNOPARK: MERSİN TEKNOLOJİ GELİŞTİRME BÖLGESİ KURUM VE İŞLETİCİ TİCARET ANONİM ŞİRKETİ

UYGULAMA

Genel Kurallar

Girişimcilerimizin bütün kişisel ve kurumsal bilgilerin (ticari, idari, mâli vb.) güvenliğinin sağlanması için aşağıda belirtilen hususlara dikkat edilmektedir.

Veri güvenliği konusunda üç temel prensibin göz önüne alınması gerekmektedir. Bunlar; gizlilik, bütünlük ve erişilebilirliktir.

Kurumda kimin hangi yetkilerle hangi verilere ulaşacağı çok iyi bir şekilde tanımlanmıştır. Rol bazlı yetkilendirme yapılmakta ve yetkisiz kişilerin bilmemesi gereken kayıtlarına erişmesi mümkün olmamaktadır.

Girişimci bilgileri ticari amaçlı olarak da üçüncü şahıslara iletilemez.

Şirket içinde ve dışında telefon ile konuşurken girişimci ile ilgili ticari ve girişimci zora sokabilecek bilgilerin üçüncü şahısların eline geçmemesine azami özen gösterilmektedir.

Sistem Güvenliği

Veriye erişirken dört temel prensibin gerçekleştirilmesi gerekmektedir. Bunlar; İzlenebilirlik, kimlik sınama, güvenirlik ve inkar edilememedir.

Bilgi sistemlerinde güvenlik veriye erişim bazında olmaktadır. Bunun için bu sistemin özellikle yazılım ve veritabanı erişim katmanlarında özel uygulamalar oluşturulmaktadır.

Veriye erişecek kişiler aşağıdaki şekilde tanımlanmıştır.

Sisteme giriş için tanımlanmış girişimci ve çalışanlarımız bu bilgilere erişebilmektedir.

Firmamızda çalışan personel işten ayırılırken ona verilmiş olan parola gibi bilgiler değiştirilmektedir.

Gerektiğinde saat ve/veya gün bazında belirlenen bir sure için bazı kullanıcı ve istemci makinelerin sisteme oturum açmalarına kısıtlama getirilmektedir.

Aynı kullanıcı kodu ile aynı anda birden fazla oturum açılmasına izin verilmemektedir.

Sadece yetkisi olan kullanıcılar için veri girişi ve/veya verinin elde edilmesi için erişim izni verilmektedir.

Birçok kullanıcının veri tabanında sadece belirli bir veri setine erişim yetkisinin denetlenebilmesini sağlamak için çok katmanlı denetim mekanizmaları oluşturulmuştur.

Veri tabanında tutulacak verilerin tutarlılığı tam ve kesin bir şekilde sağlanmaktadır. Bunu sağlamak için en azından, veri onay (validation), çapraz sorgulama (cross-checking) ve mükerrer kayıt önleme gibi ölçütler uygulanmaktadır.

Kullanıcı aktiviteleri (yapılan tüm işlemler ve erişimler) izlenebilmektedir. Veri tabanı üzerinde yapılan şüpheli işler denetlenebilmektedir. Sistemin hem etkin bir şekilde yönetilmesi, hem de yetkisiz erişimlerin engellenmesi ve izlenmesi anlamında gelişmiş bir kontrol mekanizması oluşturulmuştur. Sistem, hangi kullanıcının sistemin hangi kısmına ne zaman ve nereden eriştiğine dair (zaman damgası-date stamp, işlem, kullanılan istemci bilgisayar tanımı gibi bilgileri de içeren) kayıt tutulmaktadır.

Sistemlere erişim için tek yönlü şifreleme kullanılmaktadır.

Firma içerisinde veya firma ile başka ağlar arasındaki tüm haberleşme şifreli yapılmaktadır.

İlgili Kayıtlar

Bu politika için herhangi bir doküman ve kayıt bulunmamaktadır.