KİŞİSEL VERİ BİLGİ GÜVENLİĞİ İHLAL PROSEDÜRÜ

Bu prosedürün amacı, DIRUI RNA LABORATUAR SİSTEMLERİ VE SAĞLIK ÜRÜNLERİ SANAYİ TİCARET LİMİTED ŞİRKETİ (Dirui Ltd. Şti.) bilgi güvenlik ihlallerinin önlenmesi ve eğer ihlal gerçekleşirse alınacak önlemleri açıklamaktır. Bu prosedürün oluşturulmasından Veri İşleme ve Koruma Komitesi, Uygulanmasından tüm departmanlar sorumludur.

1. Bilgi Güvenliği İhlal Olayı

Dirui Ltd. Şti.'nin bilgilerinin gizliliğini, bütünlüğünü veya kullanılabilirliğini herhangi bir biçimde etkileme potansiyeline sahip herhangi bir olaydır. Aşağıdaki hususlardan kaynaklanacak ihlaller Bilgi Güvenliği İhlali Olarak kabul edilmiştir.

- Kullanılan bilgi varlıklarının çalınması, kaybolması ya da kırılması
- Bilginin Gizlilik, Bütünlük, Erişilebilirlik beklentilerindeki ihlaller
- İnsan hatalarından kaynaklanan ihlaller
- Fiziksel Güvenlik düzenlemelerinin ihlali
- Kontrolsüz sistem değişiklikleri
- Yazılım ya da donanım arızaları
- Erişim ihlalleri (yetkisiz erişim), yetkisiz bilgi kullanımına izin veren uygun olmayan erişim denetimleri
- Siber saldırılar (Virüs, izinsiz giriş, Truva atı, casus yazılım vb. bulgular için, sistem sunucu servis problemleri için)
- Gizli bilginin yetkisiz kişilerce ifşa edilmesi

2. Prosedür

Mevcut oturmuş düzenin ya da oturtulmaya çalışılan yeni bir düzenin tam işlememesi sistemin sürekliliğini etkiler, yanlış ya da eksik sürdürülebilirliliğini sağlar. Dirui Ltd. Şti. olarak mevcut düzenimizin veya oluşturmaya çalıştığımız düzenin sürekliliğini gerektiği şekilde sağlamak için bu prosedürü oluşturmuş bulunmaktayız.

Herhangi bir ihlal olayı durumunda yani yapılması gereken bir işleyişin uygun işlememesi ya da eksik işlemesi durumunda bu yanlış ya da eksik düzenin belirtilmesi için oluşturulan ihlal formu doldurmak ve bu formu gerekli birime ulaştırmak tüm personelimizin sorumluluğudur.

Tüm personel bilgi güvenliği ihlallerini ve zayıflıklarını farkına vardıkları zaman hemen Bilgi Güvenliği Yöneticisine rapor edeceklerdir. Bilgi Güveliği Yöneticisi de durumu hemen Kişisel Veri İşleme ve Koruma Komitesine bildirecektir.

İhlal personel bazlı ise İş hukuku mevzuatı da dikkate alınarak süreç işletilecektir. Tedarikçi bazlı ise çift taraflı gizlilik sözleşmesi hükümlerine göre işlem başlatılacaktır. Müşteri bazlı ise iş ve gizlilik sözleşmelerindeki hükümler değerlendirilecektir.

Hukuki süreçlerin işletilmesi kararı Genel Müdüre aittir.

İhlal ve zayıflık olayları yılda en az 2 kez değerlendirilerek eğilimler belirlenir. Alınması gereken önlemler varsa risk değerlendirmesine bağlı olarak gözden geçirilir.

3. Sorumluluklar

- Kullanıcılar tarafından kullanılan bilgisayar ya da bilişim cihazlarının fiziki (veri) güvenliği kullanıcının kendisine aittir. Kullanıcının şifre güvenliği ise kullanıcı ilk kez sisteme giriş yapana kadar söz konusu duruma göre Bilgi Güvenliği Yöneticisi veya idari işler sorumlusuna, sisteme dahil olup şifresini değiştirdikten sonra kullanıcının kendisine aittir.

- Sisteme ilk defa giren kullanıcı, genel güvenlik talimatı gereği şifresini uygun protokoller dahilinde değiştirmeli ve kimseye söylememelidir.

- Kullanıcı bilgisayara giriş yaptıktan sonra, bilgisayarının başından kısa ya da uzun süreli ayrıldığında güvenlik ihlaline sebep olmamak için pc'yi kilitleme (lock) moduna almalıdır.

- Şirket içi mail adresi yalnızca iş takibinde kullanılmalı, gereksiz olan mailler, kaynağı bilinmeyen email ya da spam'lar Bilgi Güvenliği Yöneticisi tarafından anında imha edilmelidir.

- Standart bir bilgisayar kullanıcısı, ağ ortamında daha önce tanımlanan standart kullanıcıların sahip oldukları genel bilgilere ulaşabilirler. Dosya, doküman ya da yazıcı gibi çevresel cihazlara erişimde, kullanıcıların tanımlı olduğu gruptan gelen haklar dışında hiçbir işlem yapamazlar. Eğer kullanıcının ilgili dosya ya da dokümana erişim hakkı yok ise erişim istemek için ağ yöneticisine başvurmalıdır.

- Kullanıcı yetkisi dışındaki klasörlere, dosyalara ya da ağ paylaşımlarına erişebiliyorsa bunu en kısa sürede Bilgi Güvenliği Yöneticisine bildirmekle sorumludur. Aksi takdirde güvenliği ihlal etmiş olur. Kullanıcının yetkisi olmayan alanlara erişimin engellenmesinden veya kullanıcıya erişim tanımlaması yapılmasından Bilgi Güvenliği Yöneticisi sorumludur.

- Sistemde her bilgisayarın birbirinden farklı bir fiziksel adresi (Mac Adress) ve network IP adresi (Internet Protocol) vardır. Kullanıcılar, gerekli olan ağ kaynaklarına düzgün bir şekilde bağlanıp gerekli olan bilgi ve paylaşılan kaynaklara erişebilirler.

- Kullanıcıların internette yasaklanan sitelere girmeleri ve internette güvenliğinden kesin emin olmadıkları kaynakları kullanmaları, güvenlik ihlaline sebep olduğu için uygun değildir.

- Uygunsuz ya da yasadışı internet sitelerine giren kullanıcılar network izleme cihazları ile takip edilip tespit edilirler. Tespit edilen kullanıcılar öncelikle uyarılır ve bu personel adına İhlal Formu doldurulur. Tekrar eden güvenlik ihlallerinden sonra iş mevzuatı gereği işlem yapılır.

- Sanal ortamda tanımadığı kimse ya da kimselerden bilmediği doküman ya da dosyaları "Güvenlik Talimatı" gereği almamalı, şirket içindeki bilgileri de şirketin bilgi gizliliği kapsamında dışarıya çıkartmamalıdır.

- Yetkisiz personel ya da kullanıcıların program yükleme, güncelleme ve silme gibi genel güvenliğe ve talimata aykırı davranmaları kesinlikle yasaktır.

- Kullanıcılar, mecbur kalmadıkça şirket içindeki diğer bilgisayarları ve Bilgi Güveliği Yöneticisinin bilgisi olmadan veri taşıma disklerini (usb memory), genel güvenlik talimatı gereği kullanmamalıdır. Sadece Bilgi Güvenliği Yöneticiisnin onayı ile şirket içinde kullanılması gereken usb ya da harici diskler her kullanımda sistemde kullanılan antivirüs programı sayesinde otomatik olarak test edilmelidir.

- Kullanıcılar, bilgisayarların kurumsal olduğunu unutmamalı, bütün müzik ve resim dosyaları kısıtlanmalıdır. Bilgisayarlarda müzik, resim vs. dosyaları bulundurulmamalı var ise silinmelidir.

- Kullanıcılar, istenmeyen postalara uyarak hiçbir şey satın almamalı ve hiçbir hayır kurumuna bağış yapmamalıdır.

- Kullanıcılar zincir e-postaları iletmemelidir.

- Bilgisayarlara hiçbir şekilde lisanssız program kurulumu gerçekleştirilmemelidir.

- Kullanıcılara evde kullanılmak üzere bilgisayar veya bilgi işlem ekipmanı verilmeyecektir.

- Çalışanlar sistem ve bilgi işlem genel güvenliği kapsamında, mesai sonunda usb bellek, cd, dvd, disket, harici harddisk ya da gizli bilgi içeren şirket dökümanlarını (dosya,klasör,gizlilik içeren yazılı doküman vb..) masada ya da açıkta bulundurmamalıdır.