Revizyon Takip Tablosu

REVİZYON NO	TARİH	AÇIKLAMA
00		İlk yayın.

1. AMAÇ

Bu prosedürün amacı , bilgi güvenlik ihlallerinin önlenmesi ve eğer ihlal gerçekleşirse alınacak önlemleri açıklamaktır.

2. SORUMLULUKLAR

Bu prosedürün oluşturulmasından Bilgi İşlem Müdürlüğü uygulanmasından tüm birimler sorumludur.

3. TANIMLAR

İhlal olayı; Uygulanması gereken bir düzenin gerektiği şekilde uygulanmamasıdır.

4. UYGULAMA

Mevcut oturmuş düzenin ya da oturtulmaya çalışılan yeni bir düzenin tam işlememesi sistemin sürekliliğini etkiler, yanlış ya da eksik sürdürülebilirliliğini sağlar. Karabağlar Belediyesi 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. İhlal olaylarına mesai saatleri içerisinde yasaklı sitelere girmek, izin formu doldurmadan kurumdışına çıkmak ya da herhangi bir birimin görevini aksatması, personele bildirisinin yapılmış olmasına rağmen gerekli usulleri uygulamaması gibi örnekler verilebilir. Örneğin aşağıda belirtilen uygulamaların yerine getirilmemesi bir ihlal olayıdır ve bu ihlal olayına ilişkin gerektiğinde ihlal formu ihlal olayına tanık olan tarafından doldurulmalıdır.

Bilgi güvenliği olaylarının yönetilmesi BGYS Temsilcisi sorumluluğundadır. BGYS Temsilcisi görev tanımı içinde bu sorumluluklar tanımlanmıştır.

Hazırlayan	**Kontrol Eden**	**Onaylayan**
SELİME YILMAZ TOPRAK MÜHENDİS	AYLA GÜZELDERE BİLGİ İŞLEM MÜDÜRÜ	DENİZ DAYANGAÇ BAŞKAN YARDIMCISI

Tüm personel bilgi güvenliği ihlallerini ve zayıflıklarını farkına vardıkları zaman hemen Bilgi Güvenliği Yöneticisine rapor edeceklerdir. İhlal personel bazlı ise disiplin talimatına göre süreç işletilecektir. Tedarikçi bazlı ise çift taraflı gizlilik sözleşmesi hükümlerine göre işlem başlatılacaktır. Hukuki süreçlerin işletilmesi karar Başkan Yardımcısına aittir.

İhlal ve zayıflık olayları yılda en az 2 kez değerlendirilerek eğilimler belirlenir. Alınması gereken önlemler varsa risk değerlendirmesine bağlı olarak Yönetimin Gözden Geçirilme(YGG) toplantısında gözden geçirilir.

İç tetkik esnasında bulgulanan ihlal veya zayıflık kayıtları iç tetkik raporuna aktarılır. YGG toplantılarında görüşülür.

- 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 bgys temsilcisne veya erişim 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.**

- Şifresi geçersiz olan (süresi dolan) ya da şifresini unutan kullanıcı Belediyemizde kullanılan Şifre Yönetim Sistemine giriş sağlayarak şifrelerini yeniden oluşturabilirler sistemde kayıtlı olmayan kullanıcılar ise, en kısa sürede ilgili sistem sorumluları ile irtibata geçmeli ve durumu iletmelidir.

- Yanlış şifre üzerinde güvenlik ihlali oluşturacak gereksiz tekrarlamalardan kaçınılmalıdır.

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

- Kurum içi mail adresi yalnızca iş takibinde kullanılmalı, gereksiz olan mailler, kaynağı bilinmeyen email ya da spam'lar Bgys temsilcisi tarafından anında imha edilmelidir.

- Standart bir bilgisayar kullanıcısı, ağ ortamında daha önce tanımlanan standart kullanıcıların belirli haklara sahip oldukları bilgilere ulaşabilirler.Bu 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 sıralı amirlerden alınan onay ile Bilgi İşlem Müdürlüğüne yazı ile başvurulmalıdır ."

Hazırlayan	Kontrol Eden	Onaylayan
SELİME YILMAZ TOPRAK MÜHENDİS	AYLA GÜZELDERE BİLGİ İŞLEM MÜDÜRÜ	DENİZ DAYANGAÇ BAŞKAN YARDIMCISI

- Kullanıcı yetkisi dışındaki klasörlere,dosyalara ya da ağ paylaşımlarına erişebiliyorsa bunu en kısa sürede bgys temsilcisine bildirmekle sorumludur. Aksi takdirde güvenliği ihlal etmiş olur. Kullanıcının yetkisi olmayan alanlara erişimin engellenmesinden veya kullanıcıya erişim tanımlaması yapılmasından Bgys temsilcisi sorumludur. Kurum bünyesinde kullandığımız Programlar için ise erişim tanımlaması çalıştığı birimin müdürüne aittir.

- 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 kurumumuzca bu sitelere erişim engellenmektedir.

- Uygunsuz ya da yasadışı internet sitelerine çeşitli yazılımlar ile 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 kurum içi disiplin yönetmeliği gereği uygulanır.

- Kullanıcı erişim hakkına sahip yazıcı, dosya ya da dökümana erişip gerekli işlemleri yaptıktan sonra o kaynakla bağlantısını kesmeli, gereksiz yere ağı (networku) meşgul etmemelidir.Böylece bilgi güvenliği ihlal edilmemiş olur.

- Sanal ortamda tanımadığı kimse ya da kimselerden bilmediği doküman ya da dosyaları "Güvenlik Talimatı" gereği almamalı, **kurum içindeki bilgileri de kurumun 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 kurum içindeki diğer bilgisayarları ve Bgys Temsilcisinin bilgisi olmadan veri taşıma disklerini (usb memory), genel güvenlik talimatı gereği kullanmamalıdır.

- Sadece Bgys temsilcisinin onayı ile kurum 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.(Sistem merkezden yönetilebilir durumdadır, bir süre sonra bu işler sistem tarafından otomatik yapılacaktır.

Hazırlayan	Kontrol Eden	Onaylayan
SELİME YILMAZ TOPRAK MÜHENDİS	AYLA GÜZELDERE BİLGİ İŞLEM MÜDÜRÜ	DENİZ DAYANGAÇ BAŞKAN YARDIMCISI

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

- Kullanıcılar zincir e-postaları iletmemelidir.E-posta adreslerinin kimler tarafından görüleceği ve bunu denetleyemeyeceğimiz gibi asılsız haberlerin veya virüslerin yayılmasına maruz kalabiliriz.

- Gönderilecek e-postaların boyutu bir defada 6 mb'ı geçmemelidir. Bu boyuttan büyük e-postalar sistemde yavaşlığa ve aynı zamanda mail kotalarının dolmasına sebep olacağından azami dikkatli olunmalıdır.

- Bilgisayarlara hiçbir şekilde lisanssız program kurulumu gerçekleştirilmemelidir.Lisanssız yapılan kurulumların, kurulumu yapan kişiye hukuki anlamda hapis cezasına kadar varan yaptırımları bulunmaktadır.

- Kurum içinde yaşanan bilgisayar ya da yazılımlar ile ilgili sorunlar çok önemli ve ciddi değil ise ilgili bölüme email yolu ile bildirilmelidir.

- Kullanıcılara Bgys Temsilcisinin bilgisi olmaması durumunda herhangi bir şekilde 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 kurum dökümanlarını (dosya,klasör,gizlilik içeren yazılı doküman vb.) masada ya da açıkta <u>bulundurmamalıdır.</u>**

- Yönetim, kurum içinde kullanılan bilgi işlem cihazlarından ve güvenliğinden, kurum içi bilgilerin gizliliğinden ve bilgi güvenliği ihlalinde yapılması gereken işlemlerden müştereken sorumludur.

5. İLGİLİ DOKÜMANLAR

5.1. İç Kaynaklı Dokümanlar

5.1.1.Bilgi Güvenliği Politikası

5.1.2. Disiplin Prosedürü

5.2. Dış Kaynaklı Dokümanlar

5.2.1. 657 Sayılı Kanun