Bu prosedürün amacı Hastanemiz kapsamı dâhilinde, bilgi ve bilgi sistemlerini etkileyen güvenlik olaylarının tanımlanması, olayların nasıl ele alındığı ve / veya alınması gerektiğini, ihlal olaylarının sorumlularının belirlenmesi, olayların raporlanması ve işlenmesi için rehberlik sağlamaktır. Tüm çalışanlar tarafından bilgi güvenliği ihlal olaylarının rapor edilmesi; güvenlik ihlallerinin sonuçlarının hafifletilmesi ve gelecekteki güvenlik ihlallerinin azaltılması için önemli rol oynamaktadır.

2. **KAPSAM**

Bu prosedür Hastanemiz ve bağlı tesisler bünyesindeki bilgi ve bilgi sistemlerini etkileyen güvenlik olaylarını kapsamaktadır.

3. **TANIMLAR**

3.1 Bilgi Güvenliği İhlal Olayı

Kurumun bilgilerinin gizliliğini, bütünlüğünü veya kullanılabilirliğini herhangi bir biçimde etkileme potansiyeline sahip herhangi bir olaydır. Kurumumuzda aşağıdaki hususlardan kaynaklanacak ihlaller Bilgi Güvenliği İhlali Olarak kabul edilmiştir.

1. Kullanılan bilgi varlıklarının çalınması, kaybolması ya da kırılması
2. Bilginin Gizlilik, Bütünlük, Erişilebilirlik beklentilerindeki ihlaller
3. İnsan hatalarından kaynaklanan ihlaller
4. Genel Müdürlük ve Bakanlık tarafından yayımlanmış Bilgi Güvenliği Yönergesi, Politikalar ve Prosedürlere göre iş ve işlemlerin yürütülmemesi
5. Fiziksel Güvenlik düzenlemelerinin ihlali
6. Kontrolsüz sistem değişiklikleri
7. Yazılım ya da donanım arızalan
8. Erişim ihlalleri (yetkisiz erişim,) yetkisiz bilgi kullanımına izin veren uygun olmayan erişim denetimleri
9. Siber saldırılar (Virüs, izinsiz giriş, Truva atı, casus yazılım vb. bulgular, sistem sunucu servis problemleri)
10. Gizli bilginin yetkisiz kişilerce ifşa edilmesi

3.2. Kurumda güvenlik olaylarının belirlenmesi, raporlanması ve kayıt altına alınmasına ilişkin süreçleri ayrıntılarıyla açıklayan net bir olay raporlama mekanizması_bulunmaktadır. Tüm çalışanlar, ihlal olaylarının ele alınması için gerekli tespit, raporlama ve eylemin önemi hakkında BGYS Birimi tarafından sürekli olarak bilgilendirilir. Bu prosedürün ele aldığı Olay türleri şunları içerir, ancak bunlarla sınırlı değildir:

1. Servis Dışı Bırakma (DDOS)

Çoklu sistemlerde hedef sistemin kaynakları ya da bant genişliği istilaya uğradığı zaman oluşur, bunlar genellikle bir veya birden fazla web sunucusudur. Bu sistemler saldırganlar tarafından çeşitli yöntemler kullanılarak bağdaştırılır.

2. Bilgi Sızdırma (Data Leakage)

Kurumun bilişim teknolojileri ile kullandığı, işlediği ya da ürettiği verilerin bilinçli ya da bilinçsiz bir şekilde kurum dışına taşınarak, belirlenmiş “bilgi güvenliği” politikalarının ihlali.

3. Zararlı Yazılım (Malware)

Bilgisayar sistemlerine zarar vermek, bilgi çalmak veya kullanıcıları rahatsız etmek gibi amaçlarla hazırlanmış yazılımlara genel olarak verilen ad.

4. Dolandırıcılık (Fraud)

Aldatma amacı ile yapılan kasıtlı eylemdir.

5. Port Tarama

Sunucu üzerinde çalışan servislerin hizmet verdiği mantıksal bağlantı noktalarını ve durumlarını tespit etmek için yapılan işlemdir.

6. Veri Tabanı Saldırısı

Veri tabanı yazılımlarının kullanımından oluşabilecek zafiyetlerinden veri tabanının ele geçirilmesi, yönetilmesi ya da yetki yükseltilmesi şeklindeki saldırılardır.

7. Web Uygulamaları Güvenlik ihlalleri

ARP sızdırma, işlevselliğin kötüye kullanımı, içeriğe sızma, DNS çalınması vb. metotlar ile web sitesinin güvenliğinin tehdit edilmesi veya sağlanamaması durumlarıdır.

8. Sosyal Mühendislik

İnternette insanların zafiyetlerinden faydalanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye çalışmaktır. İnsanların karar verme süreçlerini değiştirmeye yönelik teknikler içerir.

Gizli bilgilerin e-posta aracılığı ile iletimi, ağ üzerinden iletilen bilgilerin yetkisiz ya da yanlış alıcıya iletimi, internet üzerinden güvenli olmayan kanallar aracılığıyla veri iletimi, ortak kullanım yazıcılarından alınan çıktıların sahiplenilmemesi ya da güvenliğine önem verilmemesi, masa üstü ya da ortak alanlarda basılı kopyaların denetimsiz bırakılması vb. durumlarda tüm çalışanlar verilerin güvenliğini ve bütünlüğünü korumanın önemini göz önünde bulundurarak bilinçli hareket etmeli, ihlal durumlarını rapor etmesi gerekir.

9. Zararlı Elektronik Posta (Spam)

İsteğiniz olmadan, size gönderilen ticari içerik, politik bir görüşün propagandasını yapmak ya da bir konu hakkında kamuoyu oluşturmak amacı ile gönderilen e-posta iletileridir.

10. Parola ele geçirme

Depolanmaması gereken bir yerde depolanan parolaların tespiti ya da sızması durumudur.

Ya da herhangi bir saldın yöntemi ile parolaların ele geçirilmesidir.

11. Taşınır Cihaz Kaybı

CD / DVD, DAT (manyetik ses bandı,) veri depolamak için USB taşınabilir veri depolama / HD sürücüler gibi taşınabilir ortamların kullanılması, kullanıcının bu tür cihazları kullanma sorumluluklarının tamamen farkında olmasını gerektirir. PC'lerin, dizüstü bilgisayarların, tabletlerin ve diğer taşınabilir aygıtların kullanılması, verilerin izinsiz erişime açık hale

gelmesine neden olabilir. Kasıtlı ya da kazayla, herhangi bir taşınabilir aygıtın yetkili kullanıcısı (taşınabilir medya dahil) dışında kullanımı, kaybı veya bulunması durumunda İhlal Olay Raporlama prosedürleri aracılığıyla BGYS Birimine bildirilir.

12. Kimlik taklidi

Kişilerin fiziksel, telefon ya da dijital ortamda olmadığı bir kişi gibi davranıp, onun yetkilerini bilgisi dışında kullanmasıdır.

13. Oltalama

Dolandırıcıların kullanıcı hesaplarına rastgele e-posta göndererek bilgi sızdırmaya yönelik çevrimiçi saldırı türüdür.

14. Kişisel bilgilerin kötüye kullanımı

Tüm kişisel nitelikteki bilgileri görüntülemek, ifşa etmek veya dağıtmak 6698 sayılı Kişisel Verilerin Korunması Kanunu (Dış Kaynaklı Doküman Listesi) usul ve esaslarına aykırıdır. Herhangi kasıtlı ya da hata ile oluşacak kişisel bilgilerin kötüye kullanımı durumların raporlanması zorunludur.

3.2.15. Diğer ihlal olayları

Yukarıda tanımlanan ihlal olaylarının dışında bilgi güvenliğini tehdit eden diğer ihlallerdir.

4.KISALTMALAR

5.SORUMLULAR

Başhekimlik, Bilgi Yönetim Sistemi Sorumlusu ve Çalışanları, Tüm Çalışanlar

6. **UYGULAMA**
   1. İhlal bildirimleri, Olay Bildirim Formu aracılığı ile gerçekleştirilir.
   2. Web üzerinden yapılan bildirimler, BGYS yetkilileri saglik.gov.tr uzantılı e-mail hesaplarına otomatik eş zamanlı mail olarak iletilir.
   3. BGYS yetkilileri bildirimin bilgi güvenliği ihlal olayı olup olmadığını tespit eder, analizini yapar veyayılmasını önlemek için alınması gereken acil eylem gerekli ise süreci başlatır. Olayın ciddiyeti değerlendirilip yasal işlem öngörülmekte ise, ilgili hukuki ya da güvenlik otoriteleri sürece dâhil edilir.
   4. İhlal olayının çözümü için kullanılacak bildirim yöntemi e-posta ya da telefondur.
   5. BGYS yetkilileri tarafından yapılan değerlendirme sonucunda ihlal olayının çözümü için ilgili sorumlu tarafa (Birimin bağlı olduğu Daire Başkanına ve üst yönetime) ivedi bir şekilde iletişime geçerek olayın çözümü için harekete geçilir.
   6. Kapsam dâhilinde ya da taşra teşkilatından bildirilen ihlal olayları web sitesi üzerinden sadece yetkilendirilmiş BGYS ekibi tarafından izlenmek ve rapor edilmek üzere saklanır.
   7. Bildirilen ihlal olayının çözümü için atılan adımlar her bir ihlal olay kaydı için ayrı ayrı yazılarak olay kapatılır.
   8. Bildirilen ihlal olayları çerçevesinde yapılan bildirimler sonucu çözümleri, her hangi bir maliyet gerektiriyor ise sorumluluk ihlalin çözümünü üretecek birime aittir. BGYS Birimi sadece olayı ilgili taraflara bildirmek suretiyle çözülmesini sağlayacaktır.
   9. Bilgi Güvenliği ihlal olayları, BGYS yetkilileri tarafından kaydedilerek, gerekli ise Düzeltici Faaliyet planlanır ve /veya farkındalık e-postaları gönderilir. Ayrıca, yılda bir kez yapılan BGYS farkındalık eğitimleri için olay kayıtları girdi oluşturur.

7. **İLGİLİ DOKÜMANLAR**
    1. **Olay Bildirim ve Müdahale Formu**