TC Sağlık Bakanlığı

T.C
SAĞLIK BAKANLIĞI
DİYARBAKIR İL SAĞLIK
MÜDÜRLÜĞÜ
BİLGİ GÜVENLİĞİ POLİTİKASI

2018

BİLGİ GÜVENLİĞİ YETKİLİSİ: BİLGİSAYAR MÜHENDİSİ ERSİN ÇAĞLAR

Bu kılavuz çevre duyarlılığı kapsamında kâğıt ortamda basılmayarak; elektronik ortamda kullanıma sunulacak olup, revizyonların hızla gerçekleştirilmesine ve yayınlanmasına katkı sağlayacaktır.

ÖNSÖZ

Günümüzde bilişim sistemleri ve teknolojileri hızla gelişmekte ve değişmektedir. Bunun sonucunda çeşitli ağ yapıları, işletim sistemleri ve iş uygulamaları ortaya çıkmaktadır. Bu çeşitlilik içerisinde

kurumlar bilişim sistemlerini organize ederken bilginiz bütünlüğü, erişilebilirliği ve gizliği konusunda

özel dikkat sarf etmelidirler. Günümüzde kurumlar bilgilerinin büyük bir kısmını elektronik ortamda bulundurmakta ve bu bilgileri bilişim sistemleri altyapısı kullanarak işlemektedir. İş ve işlemlerin elektronik ortama taşınması, kamu hizmetlerinin etkinleştirilmesi, yasa dışı faaliyetlerin tespit edilebilmesi ve önlenmesine yönelik olarak kişisel bilgilerin de elektronik ortamda bulunması ve işlenmesi yoğun bir şekilde artmıştır. Ancak bu durum, kişisel bilgilerin sahiplerinin isteği dışında ilgisiz ve yetkisiz tarafların eline geçmesi, kişisel bilgi sahibini rahatsız edecek veya onlara zarar verecek şekilde yasa dışı olarak kullanılması ve kişi mahremiyetinin ihlali tehlikesini de doğurmaktadır. Dolayısı ile gelişen bilişim teknolojileri bilgi güvenliği olgusunu da beraberinde önce ihtiyaç sonra zorunluluk haline getirmiştir.

Sağlık sektöründe güncel teknolojinin hissedilir şekilde kullanılmasıyla birlikte teknolojinin taşıdığı bazı risklerle de yüz yüze gelinmiştir. Elektronik ortamdaki tüm veriler gibi, kişisel sağlık bilgilerini tehdit eden riskler için güvenlik önlemlerinin alınması zorunlu hale gelmiştir. Kişisel sağlık bilgileri, kişinin doğum öncesinden ölüm sonrasına kadar geçen süreyi kapsayan sağlık bilgilerinin tümüdür. Sağlık kayıtlarının sayısallaştırılması etkin sağlık hizmeti için yadsınamayan ciddi bir hamledir. Güncel teknolojilerin kişisel sağlık bilgilerinin gizlilik, bütünlük ve erişilebilirlik risklerini artırmasından dolayı sağlık bilgilerinin güvenliği zedelenmektedir. Kişisel sağlık bilgilerinin mahremiyeti esastır. Bu nedenle önlemlerin alınması, risklerin saptanıp indirgenmesi zorunlu hale gelmiştir...

Bilgi güvenliği, "bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak" tanımlanır. Bilgisayar teknolojilerinde güvenliğin amacı ise "kişi ve kurumların bu teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin analizlerinin yapılarak gerekli önlemlerin önceden alınmasıdır.

Bilgi güvenliği temelde üç unsuru hedefler: • Gizlilik • Bütünlük • Süreklilik

Bu kavramları biraz daha açacak olursak gizlilik, bilginin yetkisiz kişilerin erişimine kapalı olması şeklinde tanımlanabilir. Bir diğer tarif ile gizlilik bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir. Bütünlük, bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır. Bütünlük için kısaca kazara veya kasıtlı olarak bilginin bozulmaması diyebiliriz. Kullanılabilirlik, bilginin her ihtiyaç duyulduğunda kullanıma hazır durumda olması demektir. Herhangi bir sorun ya da problem çıkması durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Bu erişim kullanıcının hakları çerçevesinde olmalıdır. Kullanılabilirlik ilkesince her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir.

Bu doküman Sağlık Bakanlığı Bilgi Güvenliği Politikası baz alınarak,

1. Bilgi Sistemlerinde paylaşılmakta olan idari, mali ve klinik verilerin güvenliğini sağlamak
2. İş devamlılığını sağlamak ve güvenlik ihlalinden kaynaklanabilecek kanuni riskleri minumum seviyeye indirmek
3. Yatırımları korumak
4. Kurum ve personelinin itibarını güven altına almak

Temel amaçları ile Bilgi Sistemlerinin güvenliğinin sağlanması için minumum uyulması gereken standartları belirlemektir.

Bu doküman en üst düzey yöneticiden en alt düzey çalışana kadar bütün kurum çalışanlarını ilgilendirmektedir.

I. Parola Güvenliği Politikası

Bu politikanın amacı güçlü bir şifreleme oluşturulması şifrenin korunması ve şifrenin değiştirilme sıklığı hakkında bir standart oluşturulmasıdır.

- Bütün sistem seviyeli şifreler (root, admin, enable vs) 3 ayda bir değiştirilmelidir.
- Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.
- Kullanıcı seviyeli şifreler(eposta, masaüstü pc, web vs) 6 ayda bir değiştirilmelidir.
- Kullanıcıların şifreleri en az 8 karakterli harf-rakam-büyük-küçük harf kombinasyonları içerecek şekilde alınmalıdır. Harflerin yanı sıra, rakam ve "?.@,!, #, %, +, -, *, %" gibi özel karakterler içermelidir.
- Şifreler herhangi bir şekilde e posta ve elektronik formlaraeklenmemelidir.
- Şifreler ilgili kişiye " kişiye özel" olarak gönderilmelidir.
- Şifreler hiç kimseyle paylaşılmamalıdır.
- Basit bir kelimenin içerisindeki harf veya rakamları benzerleri ile değiştirilerek güçlü bir parola elde edilebilir.
- Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş parolalar kullanılmamalıdır.

2.İnternet ve Elektronik Posta Güvenliği

İnternet Politikası

Bu politikanın amacı kurumlarımızın internet erişimi için gerekli olan standartlarını belirlemek,

bilerek ya da bilmeyerek kurumun imajına zarar verebilecek olumsuzlukların önüne geçmek için

yasalara ve etik kurallara uygun bir internet kullanımı sağlamaktır.

- ❖ Kurumun bilgisayar ağı erişim ve içerik denetimi yapan bir firewall aracılığıyla internete çıkmalıdır.
- ❖ Kurum ihtiyaçları doğrultusunda içerik filtreleme kuralları oluşturulmalı (oyun,şiddet,pornografik vb)

siteler istisnasız bütün kullanıcılar için yasaklanmalıdır.

- ❖ İnternete giden-gelen bütün trafik virüslere karşı taranmalıdır. Antivirüs gateway sistemleri kullanılmalıdır.
- ❖ Çalışma saatleri içerisinde internete aşırı bir yoğunluk getirecek surflere de izin verilmemelidir.
- ❖ İnternet üzerinde multimedia streaming (facebook,youtube,twitter vb)yetkilere bağlı olarak sınırlandırılmalı ve kontrol altında tutulmalıdır.
- ❖ Kurum tarafından onaylanmamış yazılımların pc lere kurulması engellenmelidir.
- ❖ Üçüncü şahısların kurumsal interneti kullanmaları bilgi işlem sorumlularının bilgisi dahilinde yapılmalıdır.

E Posta Politikası

- ❖ Kullanıcıya resmi olarak tahsis edilen kurumsal amaçlı e postalar kötü ve kişisel çıkar amaçlı kullanılamaz.
- ❖ İş dışı konulardaki haber grupları kurumun e posta adres defterine eklenemez.
- ❖ Kurumun içinden ve dışından herhangi bir kişiye bu şahsi epostalar kullandırılamaz ve şifreleri paylaşılamaz.
- ❖ Kurum içi ve dışı herhangi bir kişiye bu epostalar aracılığıyla hakaret ve zarar verici nitelikte eposta gönderilemez.
- ❖ Kimliği belirsiz ve konu alanı boş olan e postalar açılmamalıdır.
- ❖ Spam, zincir sahte vb zararlı olduğu düşünülen e postalar açılmadan silinmelidir.
- ❖ Kurumsal mesajlara iş akışını aksatmayacak şekilde kısa süre içerisinde cevap verilmelidir.
- ❖ Kişi başka bir birime geçtiğinde birim adına açılan e posta devredilmeli ve devralan kişi yeni şifre oluşturmalıdır.
- ❖ Kaynağı bilinmeyen e-posta ekinde gelen dosyalar

  kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen epostalar Sistem Yönetimine haber verilmelidir.
- ❖ Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e- postalardan doğacak hukuki işlemlerden sorumlu olup, parolasının kırıldığını fark ettiği anda Sistem Yönetimine haber vermelidir.

3. İnsan Kaynakları ve Zafiyetleri Yönetimi

- ❖ Çalışan personele ait şahsi dosyalar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde olmamalıdır.
- ❖ Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmelidir.
- ❖ ÇKYS üzerinden kişiyle ilgili bir işlem yapıldığında(izin kağıdı gibi) ekranda bulunan kişisel bilgilerin diğer kişi veya kişilerce görülmesi engellenmelidir.
- ❖ Diğer kişi, birim veya kuruluşlardan telefonla ya da sözlü olarak çalışanlarla ilgili bilgi istenilmesi halinde hiçbir suretle bilgi verilmemelidir.
- ❖ İmha edilmesi gereken (müsvedde halini almış ya da iptal edilmiş yazılar vb.) kağıt kesme makinasında imha edilmelidir.
- ❖ Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.
- ❖ Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.
- ❖ Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.
- ❖ Görevden ayrılan personelin kimlik kartı alınmalı ve yazıyla idareye iade edilmelidir.

2. Mal ve Hizmet Alım Güvenliği

Mal ve hizmet alımlarında İlgili kanun, genelge, tebliğ ve yönetmeliklere aykırı olmayacak ve rekabete engel teşkil etmeyecek şekilde gerekli güvenlik düzenlemeleri Teknik Şartnamelerde belirtilmelidir.

Belirlenen güvenlik gereklerinin karşılanması için aşağıdaki maddelerin anlaşmaya eklenmesi hususu dikkate alınmalıdır:

- ❖ Bilgi güvenliği politikası,
- ❖ Bilgi, yazılım ve donanımı içeren kuruluşun bilgi varlıklarının korunması prosedürleri,
- ❖ Gerekli fiziki koruma için kontrol ve mekanizmalar,
- ❖ Kötü niyetli yazılımlara karşı koruma sağlamak için kontroller,
- ❖ Varlıklarda oluşan herhangi bir değişimin tespiti için prosedürler; örneğin, bilgi, yazılım ve donanımda oluşan kayıp veya modifikasyon,
- ❖ Anlaşma sırasında, sonrasında ya da zaman içinde kabul edilen bir noktada, bilgi ve varlıkların iade veya imha edildiğinin kontrolü,
- ❖ Varlıklarla ilgili gizlilik, bütünlük, elverişlilik ve başka özellikleri,
- ❖ Bilgilerin kopyalama ve ifşa kısıtlamaları ve gizlilik anlaşmalarının kullanımı,
- ❖ Kullanıcı ve yönetici eğitimlerinin methodu, prosedürü ve güvenliği,
- ❖ Bilgi güvenliği sorumluluğu ve sorunları için kullanıcı bilinci sağlama,
- ❖ Uygun olduğu yerde personel transferi için hüküm,
- ❖ Donanım ve yazılım kurulumu ve bakımı ile ilgili sorumluluklar,
- ❖ Açık bir raporlama yapısı ve anlaşılan raporlama formatı,
- ❖ Değişim yönetimi sürecinin açıkça belirlenmesi,
- ❖ Erişim yapması gereken üçüncü tarafın erişiminin nedenleri, gerekleri ve faydaları,
- ❖ İzin verilen erişim yöntemleri, kullanıcı kimliği ve şifresi gibi tek ve benzersiz tanımlayıcı kullanımı ve kontrolü,
- ❖ Kullanıcı erişimi ve ayrıcalıkları için bir yetkilendirme süreci,
- ❖ Korumanın bir gerekliliği olarak mevcut hizmetleri kullanmaya yetkili kişilerin ve hakları ile ayrıcalıkları gibi kullanımları ile ilgili olan bir bilgilerin bir listesi,
- ❖ Erişim haklarının iptal edilmesi veya sistemler arası bağlantı kesilmesi için süreç,
- ❖ Sözleşme de belirtilen şartların ihlali olarak meydana gelen bilgi güvenliği ihlal olaylarının ve güvenlik

ihlallerinin raporlanması, bildirimi ve incelenmesi için bir anlaşma,

- Sağlanacak ürün veya hizmetin bir açıklaması ve güvenlik sınıflandırması ile kullanılabilir hale getirilmesini tanımlayan bir bilgi,
- Hedef hizmet seviyesi ve kabul edilemez hizmet seviyesi,
- Doğrulanabilir performans kriterlerinin tanımı, kriterlerin izlenmesi ve raporlanması, Kuruluşun varlıkları ile ilgili herhangi bir faaliyetin izlenmesi ve geri alınması hakkı,
- Üçüncü bir taraf tarafından yürütülen denetimler için sözleşmede belirtilen denetleme sorumlulukları hakkı ve denetçilerin yasal haklarının sıralanması,
- Sorun çözümü için bir yükseltme sürecinin kurulması,
- Bir kuruluşun iş öncelikleri ile uygun elverişlilik ve güvenilirlik de dahil olmak üzere hizmet sürekliliği gerekleri,
- Anlaşmayla ilgili tarafların yükümlülükleri,
- Hukuki konularla ilgili sorumlulukları ve yasal gereklerin nasıl karşılanması gerektiğinden emin olunmalıdır, (örneğin, veri koruma mevzuatı, anlaşma diğer ülkelerle ile işbirliği içeriyorsa özellikle farklı ulusal yargı sistemleri dikkate alınarak)
- Fikri mülkiyet hakları (İPRs), telif hakkı ve herhangi bir ortak çalışmanın korunması,
- Üçüncü tarafların alt yüklenicileri ile birlikte bağlılığı ve altyüklenicilere uygulanması gereken güvenlik kontrolleri,

Anlaşmaların yeniden müzakeresi ya da feshi için şartlar,

- Taraflardan birinin anlaşmayı planlanan tarihten önce bitirmesi durumunda bir acil durum planı olmalıdır.
- Kuruluş güvenlik gereklerinin değişmesi durumunda anlaşmaların yeniden müzakere edilmesi,
- Varlık listeleri, lisanslar, anlaşmalar ve hakların geçerli belgeleri ve onlarla ilişkisi.

3. Bilgi Kaynakları Atık ve İmha Yönetimi

- Bakanlık ve bağlı kuruluşlar kendi bünyelerinde oluşturacakları arşivden sorumludur. Evraklar idari ve hukuki hükümlere göre belirlenmiş Evrak Saklama Planına uygun muhafaza edilmesi gerekmektedir.
- Yasal bekleme süreleri sonunda tasfiyeleri sağlanmalıdır. Burada Özel ve Çok Gizli evraklar «Devlet Arşiv Hizmetleri Yönetmeliği» hükümleri gereği oluşturulan «Evrak İmha Komisyonu» ile karar altına alınmalı ve imha edilecek evraklar kırpma ve ya yakılarak imhaları yapılmalıdır. İmha edilemeyecek evrak tanımına giren belgeler geri dönüşüme devirleri yapılmalıdır.
- Bilgi teknolojilerinin (disk storage veri tabanı dataları vb.) 14 mart 2005 Tarihli 25755 sayılı Resmi Gazetede yayımlanmış, sonraki yıllarda da çeşitli değişikliklere uğramış katı atıkların kontrolü yönetmeliğine ve Basel Sözleşmesine göre donanımların imha yönetimi gerçekleşmelidir. Komisyonca koşullar sağlanarak donanımlar parçalanıp, yakılıp imha edilmelidir.
- İmha işlemi gerçekleşecek materyalin özellik ve cinsine göre imha edilecek lokasyon belirlenmelidir.
- Uygun şekilde kırılması ve kırılma sürecinden önce veri ünitelerinin adet bilgisi alınmalıdır.
- Yetkilendirilmiş personel tarafından imhası gerçekleşen atıklara data imha tutanağı düzenlenmesi ve bertaraf edilen ürünlerin seri numaraları ve adet bilgisinin data-imha tutanağı düzenlenmelidir.
- Kırılan parçaların fiziksel muayene ile tamamen tahrip edilip edilmediğinin kontrolü yapılmalıdır.
- Son ürünlerin gruplar halinde fotoğraflanarak ilgili kişi ve kuruma iletilmesi gereklidir.

- ❖ Çıkan metallerin sınıflarına göre ayrılarak, biriktirildikten sonra eritme tesislerine iletilmesi gerekmektedir.

6. Sosyal Mühendislik Zafiyetleri

Sosyal Mühendislik: Normalde insanların tanımadıkları biri için yapmayacakları şeyleri yapmalarını sağlama sanatıdır.

Teknoloji kullanımından çok insanların hile ile kandırılarak bilgi elde edilmesidir.

Sosyal Mühendisin Özellikleri

- **Teknolojiyi kullanarak ya da kullanmadan bilgi edinmek için insanlardan faydalanırlar.**
- **Etkileme ve ikna yöntemlerini kullanırlar.**
- **Kullandığı en büyük silahı, insan zafiyetleridir.**
- **Çalışkandır, araştırmacıdır.**
  - **Senaryo yazar, iyi rol yapar.**
  - **İnsan psikolojisinden iyi anlar.**
  - **Ağzı iyi laf yapar.**
  - **Zekidir.**

SOSYAL MÜHENDİSLİK SALDIRI TEKNİKLERİ

- ➢ **Omuz Sörfü**
- ➢ **Çöp Karıştırma**
- ➢ **Rol Yapma**
- ➢ **Truva Atları**
- ➢ **Tersine Sosyal Mühendislik**

Bu sebeplerle;

- ❖ Taşınan ve işlenen verilerin öneminin bilincinde olunmalıdır.
- ❖ Kötü niyetli kişilerin eline geçince oluşabilecek zararların düşünülerek hareket edilmesi gerekmektedir.
- ❖ Arkadaşlarla paylaşılan bilgiler seçilirken dikkat edilmelidir.
- ❖ Özellikle telefonda, eposta ve sohbet yoluyla yapılan haberleşmelerde şifre gibi özel bilgiler paylaşılmamalıdır.
- ❖ Oluşturulan dosyaya erişecek kişiler ve hakları <bilmesi gereken> prensibine göre belirlenmelidir.
- ❖ Erişecek kişilerin hakları yazma, okuma, değiştirme ve çalıştırma yetkileri göz önüne alınarak oluşturulmalıdır.

- ❖ Verilen haklar belirli zamanlarda kontrol edilmeli, değişiklik gerekiyorsa yapılmalıdır.
- ❖ İlgili olmayan kişilerin erişimi için özel verilerin tutulduğu yerler açılırken etrafa dikkat edilmelidir.

7. Sosyal Medya Güvenliği Politikası

- ❖ Sosyal medya hesaplarına giriş için kullanılan şifreler ile kurum içinde kullanılan şifreler farklı olmalıdır.
- ❖ Kurum içi bilgiler sosyal medyada paylaşılmamalıdır.
- ❖ Kuruma ait hiçbir gizli bilgi, yazı sosyal medyada paylaşılmamalıdır.
- ❖ Kurumsal yazışmalar ve belgeler sosyal medya aracılığıyla iletilmemelidir.

8. İhlal Bildirim ve Yönetimi

Bilginin gizlilik, bütünlük ve kullanılabilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumlarında mutlaka kayıt altına alınmalıdır.

- ❖ Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci oluşturulmalıdır.
- ❖ Bilgi güvenliği ihlâli oluşması durumunda kişilerin tüm gerekli faaliyetleri hatırlamasını sağlamak maksadıyla bilgi güvenliği olayı rapor formatı hazırlanmalıdır.
- ❖ Güvenlik olayının oluşması durumunda olay anında raporlanmalıdır.
- ❖ İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.
- ❖ Güvenlik ihlaline neden olan çalışanlar, üçüncü taraflarla ilgili resmi bir disiplin sürecine başvurulur.
- ❖ Tüm çalışanlar, üçüncü taraf kullanıcılarıve sözleşme tarafları bilgi güvenliği olayını önlemek maksadıyla güvenlik zayıflıklarını doğrudan kendi yönetimlerine veya hizmet sağlayıcılarına mümkün olan en kısa sürede rapor edilir.
- ❖ Bilgi sistemi arızaları ve hizmet kayıpları, zararlı kodlar, dos atakları, tamamlanmamış veya yanlış iş verisinden kaynaklanan hatalar, gizlilik ve bütünlük ihlâlleri, bilgi sistemlerinin yanlış kullanımı gibi farklı bilgi güvenliği olaylarını bertaraf edecek tedbirler alınır.
- ❖ Normal olasılık planlarına ilave olarak olayın tanımı ve sebebinin analizi, önleme, tekrarı önlemek maksadıyla düzeltici tedbirlerin planlanması ve uygulanması, olaylardan etkilenen veya olaylardan kurtulanlarla iletişim, eylemin ilgili otoritelere raporlanması konuları göz önüne alınır.
- ❖ İç problem analizi, adli incelemeler veyaüretici firmadan zararın telafi edilmesi için aynı türdeki olayların izleme kayıtları (log) toplanır ve korunur.
- ❖ Güvenlik ihlallerinden kurtulmak için gereken eylemler, sistem hatalarının düzeltilmesi hususları dikkate alınır.
- ❖ Bilgi güvenliği olaylarının değerlendirilmesi sonucunda edinilen bilgi ile edinilen tecrübe ve yeni kontrollerin oluşturulması, aynı olayın tekrar etmesini önleyecek veya yüksek etkili olayların oluşmasını engelleyecektir.
- ❖ Kanıt toplama; kuruluş içerisinde disiplin faaliyeti için delil toplanırken uygulanacak genel kurallar şunlardır;

- Kanıtın mahkemede kullanılıp kullanılamayacağı ile ilgili kabul edilebilirlik derecesi,
- Kanıtın niteliği ve tamlığını gösteren ağırlığı.

❖ Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, kurum Personel Yönetmeliği gereğince aşağıdaki yaptırımlardan bir ya da birden fazla maddesini uygulayabilir:

- Uyarma,
- Kınama,
- Para cezası,
- Sözleşme feshi

BİLGİ GÜVENLİĞİ POLİTİKASI ONAYI

Bu form Diyarbakır İl sağlık Müdürlüğü'nce hazırlanan Bilgi Güvenliği Politikasının okunduğu, anlaşıldığı ve kabul edildiğinin onaylandığı bir dokümandır. Bilgi işlemden sorumlu Memur, Bilgi İşlemden sorumlu Müdür Yardımcısı ve Kurumun en üst amiri bu politikanın uygulanabilirliğinden sorumludur.

İzlenecek Prosedür'de aşağıdaki adımlar takip edilmelidir.

1. Bilgi güvenliği politikasını okuyunuz.
2. Aşağıda belirtilen bölümlere tarih atınız ve imzalayınız.
3. Bu sayfayı birim amirine iletiniz.

Sağlık Bakanlığı Bilgi Güvenliği Politikası baz alınarak hazırlanmış olan Diyarbakır İl Sağlık Müdürlüğü Bilgi Güvenliği Politikasının bir kopyasını okudum ve anladım.

Çalışanın Adı ve Soyadı:

Görevi:

Tarih:

Birimi:

Not:Bu sayfayı çıktı olarak alıp çalışanlara imzalatınız.