

T.C.DİYARBAKIR DİCLE ÜNİVERSİTESİ HASTANESİ
HASTANE BİLGİ YÖNETİM SİSTEMLERİ MERKEZİ
BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ(BGYS) POLİTİKASI



AMAÇ:

BGYS politikası, Diyarbakır Dicle Üniversitesi Hastanesinin sahip olduğu hassas bilgi varlıklarının korunması ve yönetilebilmesi amacıyla kapsam dâhilindeki bilgi varlıklarımızın gizliliği, bütünlüğü ve gerektiğinde yetkili kişilerce erişilebilirliğini sağlayarak, Diyarbakır Dicle Üniversitesi Hastanesi bünyesinde çalışanların ve ilgili tarafların uyması gereken bilgi güvenliği şartlarının çerçevesini çizmek ve yazılı kuralları belirlemektir.

KAPSAM VE SORUMLULUKLAR:

- Diyarbakır Dicle Üniversitesi Hastanesi bünyesinde bulunan ve denetlenebilir nitelikte olan bilgi varlıklarını, bilişim sistemlerini, bunlara erişim sağlayan kullanıcıları ve ayrıca, sistem ve ağ altyapısı, yazılım geliştirme, malzeme ve hizmet tedariki ile bilgi güvenliği yönetimi iş süreçlerini kapsamaktadır.
- Bilgi Güvenliği Yönetim Sistemi Politikası, bilişim teknolojileri ile ilgili önlemlere ek olarak fiziksel ve çevresel güvenlik, insan kaynakları güvenliği, yasal mevzuata uyum ve üçüncü taraf ilişkilerinin yönetimi gibi birçok konuda çeşitli kontrollerin uygulanması ve belirli aralıklarla gözden geçirilmesi hususunda BGYS çalışmalarının genel bir özetini teşkil etmektedir. BGYS çalışmalarında üst doküman niteliği taşıyan BGYS Politikası, Diyarbakır Dicle Üniversitesi Hastanesi Üst Yönetimi tarafından onaylanarak, Diyarbakır Dicle Üniversitesi Hastanesi personelinin bilgisine sunulmak ve üçüncü taraflara duyurulmak üzere yayınlanmaktadır.
- BGYS Politikasında yapılacak güncellemeler Bilgi Güvenliği Komitesi toplantılarında belirlenmekte ve BGYS Sorumluları tarafından dokümanlarda gerekli güncellemeler yapılarak Diyarbakır Dicle Üniversitesi Hastanesi Üst Yönetiminin onayına sunulmaktadır.
- Bilgi Güvenliği Yöneticisi, politikanın sürdürülmesi ve uygulanması sırasında destek ve danışmanlık sağlamakla sorumludur.
- Tüm yöneticiler politikanın uygulanmasından ve ilgili bölümlerinde personel tarafından anlaşılmasından doğrudan sorumludur. Bilgi Güvenliği Politikası ile uyum, Diyarbakır Dicle Üniversitesi Hastanesi ile işbirliği içerisinde olan ya da çalışan herkes için anlaşılması zorunlu bir dokümandır.

BGYS HEDEFLERİ VE PRENSİPLERİ:

BGYS Politikası, Diyarbakır Dicle Üniversitesi Hastanesi personeline Diyarbakır Dicle Üniversitesi Hastanesinin bilgi güvenliği gereksinimlerine uygun şekilde hareket etmesi konusunda yol göstermek, personelin bilinç ve farkındalık seviyelerini artırmak ve bu şekilde Diyarbakır Dicle Üniversitesi Hastanesinde oluşabilecek riskleri asgari düzeye indirmek, Diyarbakır Dicle Üniversitesi Hastanesinin itibarını ve bilgi güvenliği imajını korumak, üçüncü taraflarla yapılan sözleşmelerde belirlenmiş gizlilik ve uygunluğu temin etmek, teknik açıdan bilgi güvenliği tedbirlerini almak, kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamayı hedeflemektedir.

POLİTİKA:

Hastanelerimizde temel ve destekleyici iş faaliyetlerinin sürekliliğinin sağlanması sürecinde, tüm iç, dış, kasıtlı veya kazara tehditlere karşı Diyarbakır Dicle Üniversitesi Hastanesi 'nin bilgi varlıklarını¹ korumak için;

- ✓ Bilgi herhangi bir **yetkisiz erişime** karşı korunacaktır¹;
- ✓ Bilgilerin **gizliliği** sağlanacaktır;
- ✓ Bilgi **bütünlüğü** muhafaza edilecektir;
- ✓ Muhafaza edilen İş süreçlerine ait bilgiye **ulaşılabilirlik** sağlanacaktır;
- ✓ **Yasal ve Mevzuat gereksinimleri**, üçüncü taraflar (iş ortakları, müşteriler, tedarikçiler) ile yapılan sözleşmelerde yer alan hükümler sürekli izlenecek ve karşılanacaktır;
- ✓ **İş Sürekliliği Planları** geliştirilmiş, muhafaza edilmiş ve test edilmiş olacaktır²;
- ✓ **Bilgi Güvenliği Eğitimi** tüm çalışanlar için geçerli olacaktır;
- ✓ **Tüm fiili veya şüpheli bilgi güvenliği ihlalleri** Bilgi Güvenliği Yöneticisine rapor edilecek ve araştırılması sağlanacaktır.
- ✓ Talimatlar politikayı destekleyici şekilde hazırlanacaktır (Virüse karşı korunma, şifreleme ve süreklilik planları, vb.);
- ✓ İş gereksinimleri için bilgi ve sistemlerin ulaşılabilirliği sağlanacaktır.

16.03.2020
BAŞHEKİM

¹ Bilgi farklı formatlarda var olabilir; herhangi bir manyetik ortam (DVD, bellek çubuğu, vb.), basılı ya da yazılı kağıt, faks, sözlü konuşmalar (tele konferans, video konferans, vb.)

² Bu plan gerektiğinde kullanıcıların bilgileri ve temel hizmetlere erişim sağlar.

*** Politika, Bilgi Güvenliği Komitesi tarafından yıllık olarak gözden geçirilmektedir.***