# **1.AMAÇ**

BuPolitikaZara Devlet Hastanesi bünyesinde kurulacakolanBilgiGüvenliğiYönetimSisteminin(BGYS)kapsamınagirenhizmetlerinuygulanması sırasındakullanılanvekazanılanbilgilerinGizliliğine,BütünlüğüneveErişilebilirliğineyönelikrisklerindeğerlendirilmesi içinkullanılanmetodoloji, Politika vesorumluları tanımlar.

# **2.KAPSAM**

Zara Devlet Hastanesi bünyesindebelirlenen kapsamdâhilinde uygulanacaktır.

**3. KISALTMALAR:** YGG: Yönetim Gözden Geçirme, BGYS: Bilgi Yönetim Sistemi

**4.TANIMLAR:**

# **5. SORUMLULAR**

BuPolitikalarınsorumluluğuBGYSkomisyonunaaittir.BukomisyonTSISO/IEC27001BilgiGüvenliğiYönetim SistemiStandardıbağlamındayılda1keztoplanarak**RiskAnaliziTablosu**’nugözdengeçirilmesiplanlanan kontrolleringerçekleştirilipgerçekleştirilmediğinintespiti,oluşabilecekyeniriskdeğerlerininbelirlenmesi,kararlarının alınması,artık**RiskAnaliziTablosu**ndayeralanrisklerindeğerlendirilmesi,riskişlemeveriskizlemetablolarının güncellenmesi gibi konuları görüşür.

ButoplantısonucundaRiskYönetimiileilgiliçıkanraporlarveBGYSkomisyonutoplantıtutanağıYGG(Yönetim Gözden Geçirme)toplantısıiçinbirer girdiolacaktır.

BGYSkomisyonukapsamdaveişlemdeönemlibirdeğişiklikolduğundaveyaönemlibirgüvenlikihlalolayında toplanacaktır.

BGYSkomisyonuBGYSkapsamındabelirtilenüretilen,gerçekleştirilenvekazanılanbilgilereyönelikrisklerin yönetilebilmesi için,gereklipolitika,talimatlar v.boluşturur veyayınlar.

İşlemlerdensorumlutümpersonelpolitikalarauygundavranırlarveolayraporlamasistemini kullanarak sapmalarıveyaolaylarıBGYS Birimine bildirme görevlerivardır.

KararalmasürecindeönemliolabilecektümbilgileriBGYSbiriminesunmaktümZara Devlet Hastanesi çalışanlarınıngörevidir.

Bu,var olanyada önerilen kontrolleri/karşıönlemleri vemümkünsefarklıgüvencederecelerinealternatifleriveya seçenekleri içerebilir.

# **6. FAALİYET AKIŞI**

**6.1 RİSK YÖNETİMİ**

Zara Devlet Hastanesi verimliveekonomikfaaliyetgöstermesi gereklidirvebuyüzdenbirürünün/hizmetinteslimatınıetkileyebilecekkurumaaitbilgilerinitehlikeyeatacakbirolayın olasılığınakarşıalınacakgüvenlikönlemlerininzamanvemaliyetsonuçlarınıdengeleyenyönetimkararlarıverilmektedir.

***BGYSkomisyonu,birriskinyönetimindekabuledilebilirriskderecelerinideğerlendirirkenaşağıdakihususları dikkatealır:***

Kurumun fizikselkonumuyangın, arıza, su baskını gibikazaniteliğindeki hasardanoluşacakolasırisklereetkieder.

*Mevcut güvenlik*-Mevcut fiziksel,mantıksalve personel güvenlikönlemleri.

*Saldırgansayısı*–Saldırgansayısınekadaryüksekse,maruzkalma/nüfuzedilmeriskiokadarfazladır.Potansiyel saldırgansayısının, bilgininalgılanandeğeriyleorantılıolduğudüşünülmektedir.

*Kullanılanaraçlar*-Birsaldırganınkullanabildiğiaraçlarnekadargelişkinse,saldırınınbaşarıolasılığıokadar yüksektir.Bu, saldırganınuzmanlığını daiçerir.

*Toplamfırsat*-Farkedilmedenöncesaldırganınsaldırıiçinkullanabildiğizaman(veenönemlisi,karşıönlemalma süresi)veya denemesayısıriskeönemliölçüdeetkieder.

*Tanınmışlıkseviyesi*- 'Bilinmesigerekli'mantığı.Bir sistemin/bilgininvarlığıveyaneredeolduğuyada hangişekilde olduğugenelolarak bilinmiyorsasaldırılar(saldırganın) arama becerisineveya şansına dayanır ve spekülatifolur.

*İşdevamlılığıplanlaması*-Birolaylabaşetmekiçinmevcutişdevamlılığıönlemlerininvedevamplanlamasının becerisi.

Riskanalizisonucunda,sistemietkileyebilecektehditlerve oluşturduklarırisklerbulunur.Riskanalizininson kısmındabulunanriskdeğerlerinigösterentablokullanılarakriskyönetimiyapılır.Tablodabulunanriskpuanlarısistemin hâlihazırdakidurumundavarolantabanriskdeğerleridir.YapılacakolançalışmalarRiskDeğerlendirme Politikalarına uygunolarakyapılır.

Kabuledilebilir(istenen)riskdeğeri,kurumunvarlıklarıiçin,öngördüğüvekabulettiğiriskmiktarıdır.Kabul edilebilirriskseviyesine,Kurumçalışanlarıveüstyönetimilekonuşulduktansonrakararverilir.Kabuledilebilirrisk seviyesininbelirlenmesi,riskyönetimininçekirdeğinioluşturur.Çünkügerçekriskseviyesinden,kabuledilebilirrisk seviyesininçıkarılmasıilebulunandeğer,karşıönleminalınmaönceliğinibelirler.Riskyönetimindesistemdevarolan kabuledilebilirriskseviyesininüzerinderiskiolanvarlıklarişaretleniraldığıdeğeregörevarlıküzerindeişlemkararıalınır.

Belirlenenrisklerekarşıalınacakönlemlerekararverilmesiriskyönetimininasılamacıdır.Sonuçayrıntılıolarak kurumunenüstyöneticisineraporlanır.Yönetimtarafında onaylandıktansonra, karşıönlemler alınır.

Karşıönlemleralındıktan sonraikincibirriskanaliziyapılır.Böylece,alınangüvenlikönlemlerisonucunda,sistemde kalanriskmiktarıbulunur.Kalanriskmiktarının,kabuledilebilirriskmiktarıileaynıyadataşınabilirriskmiktarından düşük olması gerekir.

# **RİSKYÖNETİM SÜRECİ**



Zara Devlet Hastanesi kapsamıdâhilindeRiskyönetimsüreciyukarıda gösterildiğigibidir.RiskYönetiminiüçadımdagerçekleştirilecektir.

# **UzmanTavsiyesi**

Gerekliolduğu tespitedilen durumlarda bilgi güvenliğine ilişkin uzman tavsiyesi içinBilgiGüvenliği Yönetim Temsilcisine başvurulur. Yönetim Temsilcisiuzmanlıkalanıdışındakalandurumlardagerekligörüldüğütakdirdedışarıdanuzmangörevlendirilmesinikurum politikalarınauygunolarak yapar.

# **Kayıtlar**

Birriskiyönetmekiçinönlemalmakgerektiğinde,yönetimkararlarıYGGtoplantınotlarındadokümanteedilirve kontrolün/karşıönleminuygulanmasıiçinBGYSKomisyonuveüstyönetimonayındansonrailgilibirimyöneticilerine iletilir.Bu türkararlaryenibir politika bildirisiveyamevcut politikanındeğiştirilmesinigerektirebilir.

Risktanımlandığında,ancakmali,çevresel,teknolojik,kültürel,zamanlailgiliveyabaşkanedenlerdolayısıyla kontrolün/karşıönlemlerinuygulanmasıuygunolmadığında,kararBGYStoplantısınotlarınınparçasıolarakkaydedilirve kararıngeçerliliğini korumak içindüzenli olarak gözdengeçirilir.

# **6.2.YAPTIRIM**

Zara Devlet Hastanesi kapsamındauygulanacakolanriskyönetimi Politikalarıgerekliliklerineuyulmadığıtakdirdebu Politika sorumluları **Disiplin Politikalarına** uygun olarak değerlendirilir.