İş Sürekliliği Yönetim Sistemi Politikası

1. Amaç ve kapsam

İşbu "ISYS (İş Sürekliliği Yönetim Sistemi) Politikası Hakkında Bilgilendirme Metni'nin amacı; HEALTHİS ASSISTANCE SAĞLIK HİZMETLERİ ANONİM ŞİRKETİ ("Şirket") tarafından yürütülen sağlık turizmi faaliyetleri kapsamında, Şirketin hizmetlerinin ve bilgi işlem altyapısının **kesinti, olağanüstü durum, kriz ve felaket senaryoları** karşısında belirli bir düzen ve plan çerçevesinde sürdürülebilmesine ilişkin yönetim yaklaşımımız hakkında genel bilgilendirme yapmaktır.

Bu metin; internet sitesi, başvuru/iletişim formları, çağrı merkezi süreçleri, randevu/bilgilendirme süreçleri, Şirketin dahili bilişim altyapısı ve hizmet alınan üçüncü taraf sistemleri (barındırma, e-posta, yazılım, çağrı merkezi, danışmanlık vb.) dâhil olmak üzere iş sürekliliğiyle ilişkili bileşenler hakkında genel prensipleri kapsar.

Önemle belirtmek gerekir ki; bu bilgilendirme metni, KVKK kapsamındaki **Aydınlatma Metni** veya açık rıza metinlerinin yerine geçmez. Kişisel verilerin işlenmesine ilişkin ayrıntılı açıklamalar için lütfen "Kişisel Verilerin Korunması ve İşlenmesi Aydınlatma Metni"ni inceleyiniz.

2. Tanımlar (kısa açıklamalar)

- ISYS (İş Sürekliliği Yönetim Sistemi): Şirketin kritik iş süreçlerinin; kesinti, siber olay, altyapı arızası, doğal afet, tedarikçi kesintisi, iletişim kesintisi, insan kaynağı kısıtı ve benzeri durumlarda belirli bir plan dâhilinde sürdürülebilmesini hedefleyen yönetim yaklaşımıdır.
- Felaket Kurtarma (Disaster Recovery): Kritik bilgi sistemlerinin ve verilerin, ağır kesinti hâllerinde yeniden çalışır hâle getirilmesini amaçlayan teknik/operasyonel süreçler bütünüdür.
- Kritik süreç: Hizmetin niteliği gereği kesintiye uğraması hâlinde ilgili kişilerin güvenliği, hizmet kalitesi, yasal uyum veya operasyonel bütünlük üzerinde önemli etki doğurabilecek iş süreçlerini ifade eder.
- Kritik varlık: Kritik süreçleri destekleyen bilgi varlıkları (sunucular, veri tabanları, uygulamalar, ağ bileşenleri, yedekler, erişim altyapısı vb.) ile fiziksel/organizasyonel kaynakları ifade eder.

3. Hukuki uyum prensibimiz ve ISYS'nin veri güvenliği ile ilişkisi

Şirket, iş sürekliliği uygulamalarını; bilgi güvenliği ve kişisel verilerin korunması yaklaşımıyla birlikte ele alır. Kişisel verilerin güvenli şekilde muhafazası, erişilebilirliğinin sağlanması ve veri kaybı riskinin azaltılması, KVKK kapsamındaki "uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler" yaklaşımının bir parçası olarak değerlendirilir.

Sağlık turizmi faaliyetleri kapsamında, mevzuat gereği kayıt ve arşivleme süreçleri ile yetkili kurumlara bildirim/aktarım yükümlülükleri söz konusu olabildiğinden; kritik sistemlerin sürekliliği, veri bütünlüğü ve izlenebilirlik Şirket açısından önem arz eder.

4. ISYS yaklaşımımız (yönetim taahhüdü ve organizasyon)

Şirket, iş sürekliliğini yalnızca bilgi işlem biriminin sorumluluğu olarak değil; ilgili tüm birimlerin katılımını gerektiren bir yönetim konusu olarak ele alır. Bu kapsamda:

1. Rol ve sorumluluklar: İş sürekliliği süreçlerine ilişkin sorumlulukların (kriz yönetimi, IT/felaket kurtarma, iletişim, tedarikçi yönetimi, veri koruma ve uyum) görev tanımları içinde belirlenmesi hedeflenir.
2. Planlama ve dokümantasyon: İş sürekliliği planları, felaket kurtarma planları ve kritik iletişim listeleri gibi dokümanların güncel tutulması amaçlanır.
3. İyileştirme yaklaşımı: Olaylardan öğrenme, tatbikat sonuçlarına göre iyileştirme ve risk değerlendirmeleriyle güncelleme yapılması hedeflenir.

Kuruluş, iş sürekliliği planlamasında; hizmetin türüne ve risk seviyesine göre değişen seviyelerde önlemler uygulayabilir.

5. Risk değerlendirmesi, iş etki analizi (BIA) ve süreklilik hedefleri

ISYS kapsamındaki planlama faaliyetleri; kritik süreçlerin belirlenmesi ve bu süreçlerin kesintiye uğramasının olası etkilerinin analiz edilmesi esasına dayanır. Şirket şu adımları uygulamayı hedefler:

- İş Etki Analizi (BIA): Kritik süreçlerin kesinti hâlinde doğurabileceği etkiler (hizmet kalitesi, hasta/başvuru sahibi deneyimi, yasal uyum, finansal/itibari etki) değerlendirilir.
- Önceliklendirme: Kritik süreçler ve kritik bilgi varlıkları, risk ve etki düzeyine göre önceliklendirilir.
- Süreklilik hedefleri: Teknik ve operasyonel hedefler (ör. belirli süre içinde geri dönüş, belirli periyotta yedekleme, alternatif iletişim kanalları) işin niteliğine göre belirlenir.

Bu hedefler belirlenirken; Şirketin kullandığı sistemler, hizmet alınan tedarikçilerin taahhütleri ve mevzuat gereklilikleri birlikte değerlendirilir.

6. Teknik ve operasyonel süreklilik tedbirleri (genel çerçeve)

Şirket iş sürekliliği kapsamında –hizmetin ve riskin niteliğine göre– aşağıdaki tedbirleri uygulamayı hedefler:

1. Yedekleme ve geri yükleme: Kritik sistem ve veriler için düzenli yedekleme yapılması; yedeklerin güvenli şekilde saklanması ve geri yükleme testleriyle doğrulanması amaçlanır.
2. Alternatif altyapı / arıza toleransı: Kritik bileşenlerde tek noktadan arıza riskini azaltmaya yönelik mimari tedbirler (ör. yedekli internet, yedekli donanım, güvenli uzaktan erişim) değerlendirilebilir.

3. Siber olaylara hazırlık: Zararlı yazılım, kimlik avı, yetkisiz erişim veya hizmet dışı bırakma (DoS/DDoS) gibi olayların iş sürekliliğine etkisini azaltmaya yönelik güvenlik önlemleri ve olay müdahale süreçleri işletilir.

4. Fiziksel güvenlik ve çevresel riskler: Sunucu odası/altyapı bileşenleri, güç kesintisi, yangın, su baskını gibi çevresel riskler bakımından değerlendirilir.

5. Kritik kayıtların korunması: Sözleşmesel/operasyonel kayıtlar ile kritik süreç kayıtlarının (loglar, erişim kayıtları, işlem kayıtları) süreklilik kapsamında korunması hedeflenir.

Bu tedbirler, Kuruluşun BGYS/KVYS yaklaşımıyla birlikte ele alınır ve gerektiğinde güncellenir.

7. Üçüncü taraflar (tedarikçiler) ve dış hizmet bağımlılıkları

Sağlık turizmi hizmetlerinde; barındırma altyapısı, yazılım tedarikçileri, çağrı merkezi hizmetleri, seyahat/transfer koordinasyonu, tercümanlık veya danışmanlık gibi hizmetlerde üçüncü taraf bağımlılıkları oluşabilir.

Şirket, iş sürekliliği bakımından kritik görülen tedarikçiler için:

- hizmet kesintisi senaryolarını,
- iletişim ve eskalasyon mekanizmalarını,
- sözleşmesel hizmet seviyelerini (SLA) ve olası alternatifleri

değerlendirmeyi hedefler.

Kişisel verilerin Kuruluş adına üçüncü kişilerce işlenmesi söz konusu olduğunda, KVKK kapsamındaki veri güvenliği yaklaşımı çerçevesinde sözleşmesel ve teknik tedbirlerin işletilmesi amaçlanır.

8. Olay, kriz ve iletişim yönetimi

Kesinti veya olağanüstü durumlarda; doğru ve zamanında iletişim, hizmetin güvenli şekilde sürdürülmesi açısından önemlidir. Şirket, olay ve kriz hallerinde:

- olayın sınıflandırılması ve ilgili ekiplerin bilgilendirilmesi,
- gerekli ise ilgili kişilere/iş ortaklarına bilgilendirme yapılması,
- hizmetin güvenli şekilde kademeli geri dönüşünün sağlanması,
- kök neden analizi ve düzeltici/önleyici faaliyetlerin planlanması

gibi adımları içeren bir yaklaşım benimsemeyi hedefler.

Bu kapsamda; kişisel veri ihlali şüphesi doğuran olaylarda ayrıca KVKK kapsamındaki değerlendirme ve gerekli bildirim süreçleri işletilir.

9. Güncellemeler

Şirket , ISYS uygulamalarını; mevzuat değişiklikleri, teknolojik gelişmeler, risk değerlendirmeleri, tedarikçi yapısındaki değişiklikler ve tatbikat sonuçları doğrultusunda güncelleyebilir. Bu bilgilendirme metni de gerektiğinde revize edilebilir ve güncel sürüm web sitesinde yayımlanır.

10. İletişim

ISYS yaklaşımımız ve iş sürekliliği uygulamalarımız hakkında sorularınız için bizimle aşağıdaki kanallardan iletişime geçebilirsiniz:

- Unvan: HEALTHİS ASSISTANCE SAĞLIK HİZMETLERİ ANONİM ŞİRKETİ
- Adres: İzzet Paşa, Yeni Yol Cd. Nurol Tower No:3 İç Kapı No:32, 34381 Şişli/İstanbul
- E-posta: info@healthis.com.tr
- Telefon: (0212) 809 99 07