1.Amaç

Bu politika, kurumun insan, fiziksel, dijital, soyut ve operasyonel varlıklarını etkin bir şekilde yönetmek, bilgi güvenliğini sağlamak ve varlıkların değerini korumak amacıyla oluşturulmuştur. Varlıkların envanter takibi, risklerine göre sınıflandırılması, korunması, izlenmesi ve sorumlulukların belirlenmesine ilişkin esasları içerir.

2.Kapsam

Bu politika, üniversitenin BGYS kapsamında yer alan tüm bilgi güvenliği varlıklarını, insan kaynaklarını, iş süreçlerini ve kişisel verileri kapsar.

3.Dayanak:

3.1. KTÜN TS ISO/IEC ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ YÖNERGESİ

3.2. 06.07.2019 tarih ve 30823 sayılı Resmi Gazete'de 2019/12 sayılı Cumhurbaşkanlığı Genelgesi gereği CBDDO Başkanlığı tarafından yayımlanan Bilgi ve İletişim Güvenliği Rehberi.

3.3. 6698 Sayılı Kişisel Verilerin Korunması Kanunu Teknik Tedbirleri.

3.4. İlgili diğer mevzuat.

4.Tanımlar

4.1. **Varlık yönetimi**: bir kurumun bilgi varlıklarını tanımlaması, sınıflandırması, koruması ve yönetmesi sürecidir.

4.2. **Varlık Envanteri**: Bilgi güvenliğine dair korunması gereken tüm varlıklarının tespit edilmesi, sınıflandırılması ve yönetilmesi için tür, sahiplik ve risk seviyeleri ile birlikte oluşturulan detaylı bir kayıttır. Varlık envanteri, BGYS'nin temel adımlarından biri olup risklerin doğru değerlendirilmesi, varlıkların değerinin hesaplanması ve uygun güvenlik önlemlerinin alınması için temel oluşturur.

5.Sorumlular

Bu politikanın oluşturulmasından BİDB, onaylamasından BGYS komisyonu ve uygulanmasından tüm kullanıcılar sorumludur.

6.Hedefler

6.1. **Veri Kaybını Önlemek:** Önemli bilgi varlıklarının korunmasını sağlamak.

6.2. **Yetkisiz Erişimi Engellemek:** Kimlerin hangi varlıklara erişebileceğini sınırlamak.

6.3. **Regülasyonlara Uygunluğu Sağlamak:** ISO 27001, KVKK ve GDPR gibi standartlarla uyumlu hale gelmek.

6.4. **Siber Saldırılara Karşı Koruma Sağlamak**: Kritik varlıkların güvenlik risklerini azaltmak.

6.5. **Risk Yönetimini Kolaylaştırmak:** Risklerin daha net belirlenmesine ve önceliklendirilmesine

yardımcı olmak.

6.6. **Etkili Kaynak Yönetimi:** Hangi varlıkların korunması gerektiğini ve hangi güvenlik seviyelerinin uygulanacağını belirlemek.

6.7. **Standartlaştırma:** Farklı ekiplerin aynı güvenlik diliyle iletişim kurmasını sağlamak.

6.8. **Sahiplikleri belirlemek:** Varlık sahipliği ve sorumluluklarının belirlenmesini sağlamak.

7.Varlık Gruplarının Belirlenmesi

7.1. Varlık grupları, benzer türdeki varlıkların aynı kategoride toplanarak yönetilmesini ifade eder. Varlık grupları belirlenirken aşağıdaki hususlar sağlanmalıdır:

7.1.1. Tüm kurumsal varlıkların hangi varlık grubu ana başlığı altında yer alacağının belirlenmesi.

7.1.2. Tüm varlıkların en az bir varlık grubunda ve mümkün olduğunca tek bir varlık grubunda yer almasının sağlanması (Birden fazla varlık grubu tarafından adreslenmesi gereken kurumsal varlıklar, kritiklik derecesi en yüksek olan varlık grubu üzerinden değerlendirilmeli ve dâhil edildiği tüm varlık grupları ile ilgili tedbirler bu varlıklar için ele alınmalıdır.).

7.1.3. Varlık gruplarının tanımlanması için kullanılacak alt kırılımların kurumsal ihtiyaçlar doğrultusunda belirlenmesi (kurum hizmet alanları, kurum organizasyon yapısı, teknolojiler,uluslararası iyi örnekler, BT altyapıları vb.).

7.1.4. Aynı güvenlik izolasyonunda yer alan varlıkların mümkün olduğunca aynı varlık grubuna dâhil edilmesi.

7.1.5. Farklı güvenlik seviyesine sahip olması gereken varlıkların farklı varlık gruplarında olacak şekilde gruplandırılması.

7.1.6. Aynı seviyede güvenlik tedbirlerinin uygulanacağı düşünülen varlık gruplarının birleştirilerek varlık grubu sayısının azaltılması.

7.1.7. Her bir varlık grubu ana başlığı altında yer alan alt varlık gruplarının sayılarının yönetilebilecek sayıda olması.

7.2. Varlıklar CBDDO'nun BİG Rehberinde belirtilen ana kategorilere(Ağ ve Sistemler, Uygulamalar, Taşınabilir Cihaz ve Ortamlar …) ayrılmalıdır.

8.Varlık Envanterinin Oluşturulması

8.1. Veri saklama, işleme ve iletme yeteneği olan tüm unsurların güncel envanteri tutulmalıdır

8.2. Tüm varlıklar için bulunduğu lokasyon(konum) ve bulunduğu(bağlı olduğu) sistem bilgisi, varlığın envantere eklenme tarihi tutulmalıdır.

8.3. Tüm cihaz ve yazılımlarda konfigürasyon bilgisi de envantere dahil edilmeli ve güvenli olarak kabul edilmeyen ve/veya varsayılan konfigürasyon ile çalışmaları engellenmelidir.

8.4. Envantere alınan tüm unsurlar için hangi güvenlik tedbirlerinin uygulandığı bilgisi de envantere girilmelidir. (Örneğin zafiyet taramasından geçirilmiş midir? Farkındalık çalışması yapılmış mıdır? Varsayılan ayarlarında güvenlik sıkılaştırmaları yapılmış mıdır? Güvenlik güncellemeleri/yamaları zamanında yapılmakta mıdır? İhtiyaç olmayan ve onaylanmamış servislerin, port ve protokollerin çalışıp çalışmadığı kontrol edilmiş midir? Antivirüs yazılımı

yüklü ve güncel midir? IP telefonlar dahil tüm unsurların iz kayıtları tutulmakta mıdır? vb.)

8.5. Kurum ağlarına ait fiziksel ve mantıksal topolojiler, vlanlar ve aktif/pasif tüm ağ ürünleri de envantere dahil edilmelidir.

8.6. İş süreçleri ve her süreçte işlenen kişisel verilerin envanteri, KVKK gerekliliklerine uygun şekilde varlık envanterinde yer almalıdır. Bu envanter, KTÜN KVK Koordinatörlüğü'nün talimatları doğrultusunda hazırlanacaktır.

8.7. Kurumda aktif olarak kullanılan/kullanılmayan tüm kriptografik ürünler ve bu ürünlerin hangi işlemler için hangi amaçla kullanıldıkları tanımlanmalıdır.

8.8. Kimlik doğrulama sistemleri ve bu sistemler tarafından düzenlenen tüm hesapların envanteri tutulmalıdır.

8.9. Aktif bağlantı portları, servisler ve protokoller donanım ve yazılım varlık envanterinde yer alan varlıklar ile eşleştirilmelidir. (Kurum sistemlerinin tümünü kapsayacak şekilde port, servis ve protokol taramaları gerçekleştirilmeli, açık ve kullanımına ihtiyaç olmayan portların tespit edilmesi durumunda alarm üreten mekanizmalar devreye alınmalıdır.)

8.10. Yedekleme medyalarının envanteri tutulmalıdır.

8.11. Her varlık grubu için "Tehditler, Tehlikeler, Riskler ve Alınan Önlemler"in de yer aldığı risk analiz ve risk işleme kayıtları tutulmalıdır.

8.12. Tüm BGYS Dökümanları varlık envanterinde tutulmalıdır.

8.13. Varlık envanteri tek bir yazılım üzerinden oluşturulabileceği gibi birden fazla yazılımın (manuel ya da otomatik) entegrasyonu ile de sağlanabilir. Her bir yazılımda hangi varlıkların envanter takibinin yapıldığı detaylı olarak dokümante edilmelidir.

8.14. **Donanım envanteri oluşturulurken aşağıdaki hususlara dikkat edilmelidir:**

8.14.1. Donanımlar için en az şu bilgiler tutulmalıdır: her bir donanımın ağ adresi, donanım adresi(MAC), makine adı, seri numarası, markası, modeli, destek alınan tedarikçi sözleşme bilgileri (bakım süresi, kapsamı vb.), donanım sorumlusu, sorumlu kişinin birimi ve donanımın kurum tarafından onaylı olup olmadığı bilgisi.

8.14.2. Yeni tedarik edilen ya da ağa yeni bağlanacak donanımların, donanım varlık envanterine kaydı yapılmadan kurum ağına bağlanmaması sağlanmalıdır (Buna yönelik politika ve prosedürler oluşturulmalı ve uygulanmalıdır.). Sadece onaylı donanımların kurum ağına bağlanabilmesi için, 802.1x standardı veya NAC çözümleri kullanılarak kurum ağına bağlanan cihazlara kimlik denetimi yapılmalıdır.

8.14.3. Kurum ağına bağlı cihazları tanımlamak ve donanım varlık envanterindeki değişiklikleri takip etmek için aktif keşif araçları kullanılmalıdır. Güncelliği sağlamak için DHCP sunucularında ya da IP adres yönetim araçlarında kayıt mekanizmasının kullanımı da sağlanmalıdır.

8.14.4. KTÜN tarafında kayıt altında alınan paydaşlara ait veriler de (sözleşmeler dahil) varlık envanterinde bulunmalıdır.

8.15. **Yazılım envanteri oluşturulurken aşağıdaki hususlara dikkat edilmelidir:**

8.15.1. Kurumda kullanılan tüm yazılımların (işletim sistemleri, donanım yazılımları, üçüncü parti yazılımlar, uygulama yazılımları vb.) envanterde yer alması sağlanmalıdır.

8.15.2. Yazılım envanter yönetim araçlarında, kurum tarafından yetkilendirilen işletim sistemleri dâhil olmak üzere en az; yazılımların adı, sürümü, yayımcısı, destek alınan tedarikçi sözleşme

bilgileri (bakım süresi, kapsamı vb.), lisans bilgileri ve edinim tarihi bilgileri, yazılımın yüklendiği donanımlar veya sanallaştırma ortamları kayıt altına alınmalı ve izlenebilir olmalıdır.

8.15.3. Envantere alınan yazılımlar için mümkün olduğunca güncelleme desteği devamlılığı sağlanmalıdır. Üreticisi tarafından sunulan destek hizmeti sona ermiş ancak iş gereksinimleri sebebi ile kullanılması gereken yazılımlar, yazılım envanterinde "üretici tarafından desteklenmeyen" olarak belirtilmelidir.

9.Varlık Sahipliği ve Emanetçiliği

9.1. Varlık Sahipliği ve Emanetçiliği, kurumun bilgi varlıklarının güvenli ve etkin bir şekilde yönetilmesi, korunması ve kullanımından sorumlu kişilerin rollerini ve sorumluluklarını tanımlayan kavramlardır. Bu çerçevede, Varlık Sahibi ve Varlık Emanetçisi iş birliği içinde çalışarak varlıkların güvenliğini, sürekliliğini ve uygun şekilde kullanılmasını sağlar.

9.2. **Varlık Sahibi**: Bir varlığın korunmasından, yönetilmesinden, erişim yetkilendirmesinden ve doğru kullanımından sorumlu kişi, birim veya rol.

9.3. **Varlık Emanetçisi(Kullanıcısı)**: Bir varlığı geçici olarak kullanan ancak mülkiyetine sahip olmayan kişi, birim veya rol. Emanet edilen varlığın güvenli kullanımı ve belirlenen kurallar(politika, prosedür vb.) çerçevesinde korunmasından sorumludur. Örneğin, üniversitenin dizüstü bilgisayarını geçici olarak kullanan bir akademisyen varlık emanetçisidir. Emanetçi birçok varlık için kullanıcı anlamında gelmektedir (Bazı varlıklar için ise varlık sahibi ile emanetçisi aynı kişi/rol olabilir.) .

9.4. Her varlık için **bir sahip atanmalı veya zimmet yapılmalı** ve sorumlulukları belirlenmelidir.

9.5. Sahiplik ve emanetçi belirtilirken kişi adı yerine ünvanı (veya rolü) kullanılması tercih edilmeli ve hangi ünvanda hangi tarih aralıklarında hangi kişilerin olduğu bilgileri ayrıca takip edilmelidir.

10.Varlıkların (Kritiklik Derecelerine Göre) Sınıflandırılması:

10.1. Kritiklik derecelerine göre sınıflandırma kurumun sahip olduğu varlıkların iş süreçlerine etkileri ve güvenlik gereksinimlerine göre önceliklendirilmesini ifade eder. Kritiklik derecesi, her bir varlığın kurum için ne kadar hayati olduğunu belirlemeye ve bu doğrultuda uygun güvenlik önlemleri almaya yardımcı olur.

10.2. **Varlık Değerinin(Kritiklik Derecesinin) Hesaplanması**

10.2.1. Bilgi güvenliği açısından varlığın değeri bilgi güvenliğinin temel unsurları olan "gizlilik, bütünlük ve erişilebilirlik" olarak ölçülebilecek değerlerle hesaplanacaktır. **Gizlilik:** Bilginin yetkisiz kişilerin erişimine karşı korunmasıdır. **Erişilebilirlik:** Bilginin yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olmasıdır. **Bütünlük:** Bilginin tam ve doğru olma durumunun korunmasıdır.

10.2.2. Varlık değeri belirlenirken kullanılacak metrik sisteminde minimum 3 kademe bulunmalıdır. Örneğin derece 1-derece 2-derece 3 veya düşük-orta-yüksek şeklinde olabilir.

10.2.3. Varlıkların(veya varlık gruplarının) her birinin Gizlilik, Bütünlük ve Erişilebilirlik değeri verildikten sonra bunların "toplamı, ortalaması veya çarpımı alınır" ve varlığın toplam değeri bulunur.

10.2.4. Varlık değeri belirlenirken, varlığın gizlilik, bütünlük ve erişilebilirlik boyutlarına zarar

verebilecek olası en kötü senaryo(varlık grubu içerisinde yer alan en kritik ve en etkili varlık için en kötü durumun oluşması durumu) meydana geldiğinde neler olabileceği belirlenir. Belirlenen senaryoya göre minimum aşağıdaki faktörler baz alınarak varlığın gizlilik bütünlük ve erişilebilirliği için (makul bir metrik sistemi kullanılıp) puanlama yapılarak kritiklik derecesi hesaplanır:

10.2.4.1. **Kurumsal Sonuçlar:**

Kurumsal sonuçlar için aşağıdaki unsurlar değerlendirilir:

- **Kurumsal İmaj Değeri**: Kurumun kamuoyu, paydaşlar, öğrenciler ve çalışanlar nezdindeki saygınlığını, güvenilirliğini ve prestijini temsil eder.
- **İtibar Değeri**: Finansal olmayan ancak stratejik açıdan çok önemli bir değerdir. **Finansal Değer**: Varlığın maliyet ve potansiyel kayıp değeri.
- **Hukuki ve Uyumluluk Riski**: Yasal yükümlülüklere ve mevzuata uyum açısından taşıdığı önem ele alınır.

10.2.4.2. **Etkilenen kişi sayısı:**

Varlık grubu ile ilgili meydana gelen bilgi güvenliği olayı sonucu doğrudan etkilenebilecek kişi sayısı değerlendirilir.

10.2.4.3. **Toplumsal Sonuçlar:**

Toplumsal kargaşa olup olmaması, yazılı görsel basına intikal edip etmemesi, can kaybı meydana gelip gelmemesi vb.

10.2.4.4. **Sektörel Etki:**

Varlık grubunun hizmet verdiği sektöre etkisi değerlendirilir.

10.2.4.5. **Bağımlı Varlıklar**

Bağımlılığı olan varlıkların(Ör: entegre olan diğer yazılımlar, sunucular vb.) çalışmasının etkilenip etkilenmeyeceği, oluşabilecek zararlar ve faaliyetlerine devam edip edemeyecekleri değerlendirilir.

11.Varlıkların Etiketlenmesi:

11.1. Varlıkların hangi kritiklik derecesinde olduğunun bir bakışta ilgili kişisi tarafından anlaşılması gerektiği durumlarda varlıkların üzerine kritiklik derecelerini belirten belirteçler koyulur. Bu

belirteçler fiziki varlıklar için renkli/yazılı etiketler, dijital varlıklar için de benzer işlevi görecek unsurlar (örneğin renkli yazılar, klasörlemeler vb.) şeklinde olmalıdır.

11.2. Her varlık üzerinde sınıflandırma etiketlerinin kullanılması gerekmemektedir. İş süreçlerinin gereklerine göre güvenlik dikkate alınarak ihtiyaç duyulan varlıklara etiketleme yapılması yeterlidir.

11.3. Kullanılan sınıflandırma ve etiketlendirmenin sınırlı düzeyde, basit ve anlaşılır olması sağlanmalıdır. Kurum tarafından geliştirilmiş sınıflandırma ve etiketleme kurallarına uygun olması tercih edilmelidir.

11.4. Uygulanan etiketleme sistemi ile ilgili kurum personeline eğitimler verilmelidir.

12.Varlık Değişikliklerinin Yönetilmesi

12.1. Kurumsal ihtiyaçlar ve gelişmeler dikkate alınarak varlık grupları ile uygulama ve teknoloji ya da sıkılaştırma tedbirleri kapsamında gerçekleşecek bir değişiklik tespit edildiğinde varlık gruplarının güncellenmesi gerekmektedir. Bu kapsamda oluşabilecek değişiklikler aşağıdakilerle sınırlı olmamakla birlikte sürekli izlenmelidir:

12.1.1. Yeni varlık gruplarının oluşturulması

12.1.2. Varlık gruplarında yer alan varlıkların değişmesi

12.1.3. Mevcut varlık grupları yerine farklı varlık gruplarının tanımlanması

12.1.4. Varlık gruplarının kritiklik derecelerinin değişmesi

12.1.5. Varlık gruplarına uygulanacak uygulama ve teknoloji alanlarının değişmesi

12.1.6. Varlık gruplarını etkileyen mevzuat, standart veya ikincil düzenlemelerin değişmesi

13.Varlıkların Korunması ve Güvenliği

13.1. Kurumsal ve kişisel veriler, kurumun itibarı ve iş süreçleri, politika ve prosedürlerle korunmalıdır. Bu kapsamda gerekli dökümantasyon(Politikalar, prosedürler vb.) hazırlanıp ilgililerine duyurulmalıdır.

13.2. Envantere yalnızca yetkilendirilmiş personelin erişimi mümkün kılınmalıdır.

13.3. Varlıkların "Kabul Edilebilir Kullanımı / İadesi / İmhası" politikaları ve diğer ilgili dökümanları(prosedür, talimat vb.) oluşturulmalıdır.

13.4. BGYS kapsamında hazırlanan tüm dökümantasyon esasında varlık yönetimi ile ilişkili olup etkin bir varlık yönetimi için varlık sorumlularının ilgili BGYS dökümanlarına hakim olması gerekmektedir.

14.Yaptırım

Bu politikanın ihlal edilmesi durumunda KTÜN BİLGİ GÜVENLİĞİ POLİTİKASI'nda belirtilen "POLİTİKANIN İHLALİ VE YAPTIRIMLAR" başlığı altındakiler geçerlidir.

15.Yürürlük

Bu politika, BGYS komisyonu tarafından onaylandıktan sonra Bilgi İşlem Daire Başkanlığının web sayfasında yayımlanarak duyurusu yapıldığı tarihte yürürlüğe girer.

16.Yürütme

Bu politika, Bilgi İşlem Daire Başkanlığı tarafından yürütülür.