1. Amaç

Kurumun insan, fiziksel, dijital, soyut ve operasyonel varlıklarına yönelik meydana gelebilecek siber olaylar için olay "öncesi, esnası ve sonrasında" yapılması gereken çalışmaları tanımlayarak, kurum içi/dışı paydaşlarla iletişim esaslarını belirleyip siber olayları tespit etmek; doğru, hızlı ve etkili müdahalede bulunmak ve olay sonrasında iyileştirme adımlarını belirlemektir.

2. Kapsam

Bu politika, üniversitenin BGYS kapsamında yer alan tüm bilgi varlıklarını, insan kaynaklarını, iş süreçlerini, kişisel verileri ve iç/dış paydaşları(bilişim kaynakları kullanıcıları, çalışanlar, idari/akademik birimler, tedarikçiler vb.) 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. "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ" uyarınca UDHB'ce hazırlanan "Kurumsal SOME Kurulum ve Yönetim Rehberi".

3.4. 6698 Sayılı Kişisel Verilerin Korunması Kanunu Teknik Tedbirleri.

3.5. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı

3.6. İlgili diğer mevzuat.

4. Tanımlar

4.1. **UDHB:** Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. Yeni adı "Ulaştırma ve Altyapı Bakanlığı" olup Türkiye Cumhuriyeti Cumhurbaşkanlığına bağlı olarak çalışan, ulaştırma ve altyapı işlerinden sorumlu olan bakanlıktır.

4.2. **Kurum:** Konya Teknik Üniversitesi

4.3. **Siber Olay:** Kurumun bilgi varlıklarına yönelik, "gizlilik, bütünlük ve erişilebilirlik" açısından "risk oluşturan" veya "ihlal eden" her türlü olay (Güvenlik ihlalleri, veri ifşaları, bilişim süreçlerinde olağandışı durumlar, zafiyet tespiti vb.) .

4.4. **USOM:** "Ulusal Siber Olaylara Müdahale Merkezinin Kuruluş, Görev ve Yetkilerine Dair Usul ve Esaslar"ına göre UDHB'ye bağlı Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesinde kurulmuş olup temel görevi ulusal düzeyde siber güvenliğin sağlanmasına yönelik faaliyetler yürütmek olan "Ulusal Siber Olaylara Müdahale Merkezi".

4.5. **SOME(**Siber Olaylara Müdahale Ekibi**):** 11 Kasım 2013 tarihli ve 28818 sayılı Resmi Gazete'de yayımlanan "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ" uyarınca Kurumsal SOME kurma yükümlülüğü olan kurumlar için "UDHB" tarafından hazırlanan "Kurumsal SOME Kurulum ve Yönetim Rehberi"(SOME Rehberi) esaslarına göre kurulmuş olan ve bu kapsamda çalışmalarını yürüten uzman ekip.

5. Sorumluluklar

5.1. Üst Yönetim:

5.1.1. Bu politikanın uygulanmasından nihai olarak sorumludur.

5.1.2. "SOME Rehberi"ne uygun kaynak ve bütçe tahsis eder.

5.1.3. Temel hedefi "bilişim sistemlerinin yönetimini yapmak ve sürekliliğini sağlamak" olan Bilgi İşlem Biriminin sistem işletimi fonksiyonları ile Kurumsal SOME fonksiyonlarının "görevler ayrılığı" ilkesine uygun olarak farklı personel tarafından yapılması için bu alandaki personel kapasitesinin artırılması ve iyileştirilmesi için Üst Yönetim imkânların elverdiği ölçüde gerekli tedbirleri alır.

5.2. SOME Ekibi:

5.2.1. İlgili mevzuat gereği, KTÜN Bilgi İşlem Dairesi'nde bir birim olarak kurulmuş olup temel görevi Kurum'da bulunan siber güvenlik risklerini azaltacak faaliyetler yapmak ve Siber olayların tespit, müdahale ve raporlama süreçlerini yönetmektir.

5.2.2. Siber güvenlik ihlali durumunda USOM'a ve mevzuat gereği bilgilendirilmesi gerekli diğer ilgililerine bildirimler yapar ve koordinasyonu sağlayarak süreci yönetir.

5.2.3. Siber olay öncesi güvenlik denetimleri/testleri vb. çalışmaları yapar/yaptırır,

5.2.4. Loglama sistemi (veya SİEM) üzerinden olağan dışı durumları tespit edip gerekli aksiyonların alınması için ilgililerini bilgilendirir.

5.2.5. Tüm kullanıcılara(akademik, idari, öğrenci vb.) yönelik bilgi güvenliği farkındalığı çalışmaları yapar/yaptırır.

5.2.6. SOME işbu dökümanda belirtilmeyip de "Kurumsal SOME Kurulum ve Yönetim Rehberi"nde geçen tüm görevleri yerine getirmekle sorumludur.

5.3. Bilgi İşlem Dairesi:

5.3.1. Altyapının güvenliğini ve sürekliliğini sağlar.

5.3.2. İşbu politikanın oluşturulmasını ve güncel kalmasını sağlar.

5.4. Koruma ve Güvenlik Şube Müdürlüğü:

5.4.1. Olayın fiziksel güvenlik boyutuyla ilgili olarak SOME ve diğer ilgili birimlerle işbirliği içinde aşağıdaki konularda yardımcı olur:

5.4.1.1. Siber olayın gerçekleştiği yer KTÜN sorumluluğundaki fiziksel alanlar olarak tespit edildiğinde (bilgisayar laboratuvarı, personel odası vb.) **yetkisiz kişilerin alana girişini engellemek**, fiziksel delillerin zarar görmesini önlemek, yetkisiz kişilerin olayla ilgili bilgiye erişimini sınırlamak.

5.4.1.2. Olay anında güvenlik personelinin tuttuğu gözlem raporları ve **resmî tutanaklar** ile olayın belgelenmesine yardımcı olmak, güvenlik raporlarını ve gözlemleri ilgili birimlere zamanında iletmek.

5.4.1.3. Kolluk kuvvetlerine veya resmi kurumlara yönlendirme gerektiğinde süreçte destek sağlamak.

5.4.1.4. Olayla ilgili elde edilen bilgilerin sadece yetkili kişilerle paylaşılması konusunda "koruma ve güvenlik personelini" bilgilendirmek ve denetlemek.

5.4.1.5. Olayın yaşandığı tarih ve saat aralığına ait CCTV kamera kayıtlarını SOME ile paylaşmak,

5.4.1.6. Gerekli durumlarda görüntüleri adli bilişim analizine sunmak üzere muhafaza etmek.

5.5. **Birimler/Kullanıcılar/Çalışanlar/Paydaşlar:**

5.5.1. Kurumun bilgi güvenliği politikalarına uyar.

5.5.2. Şüpheli durum, zafiyet veya saldırı tespitinde derhal SOMEi'ye bildirimde bulunur.

5.5.3. SOME'nin mevzuat gereği yapması gereken çalışmalar için ihtiyaç duyduğu bilgi ve belgeyi sağlar ve gerekli güvenlik tedbirleri alır.

BGYS komisyonu:

5.5.4. İşbu politikanın mevzuat ve Kurum ihtiyaçlarına uygunluğunu denetleyip onaylanmasını sağlar.

6. Siber Olay Öncesi

6.1. Siber olay öncesi yapılacak çalışmalarda aşağıdaki temel prensipler dikkate alınmalıdır:

6.1.1. Etkili siber güvenlik önlemlerinin alınması ve siber "caydırıcılığın" sağlanması

6.1.2. Tasarımdan itibaren güvenlik ilkesi gözetilerek sıfır güven yaklaşımının benimsenmesi

6.1.3. Bilgi ve iletişim teknolojileri tasarımı ve kullanımında siber güvenliği odak noktası olarak ele alan "siber hijyen" anlayışının yerleştirilmesi

6.1.4. Saldırganlara karşı proaktif bir yaklaşım sergilenmesi,

6.1.5. Siber güvenlik altyapılarında katmanlı ve kademeli mimarilerin kullanılması,

6.1.6. Siber güvenlik risklerinin yönetilebilir ve kabul edilebilir düzeylerde tutulabilmesi,

6.1.7. "Kamuda Açık Kaynak Kodlu Yazılım Kullanımı" Konulu Cumhurbaşkanlığı Genelgesi gereği siber güvenliğin artırılması için açık kaynak ürünlere öncelik verilmesi.

6.2. "KTÜN Varlık Yönetim Politikası"na uygun olarak oluşturulan envanterdeki tüm varlıklar için "CBDDO BİG Rehberi"nde belirtilen ilgili güvenlik tedbirlerinden uygulanabilir olanlar için gereği yapılmalıdır.

6.3. ISO-27001 Ek-A kontrol maddelerinde belirtilenler için gereği yapılmalıdır.

6.4. Alınması gerekli teknik tedbirlerle ilgili KTÜN tarafından oluşturulan politika ve prosedürlere uyulmalıdır.

6.5. Kuruma ait tüm zafiyet bildirimleri, ihlaller, parolası çalınanlar ve diğer bilgi güvenliğine yönelik risk oluşturan tüm unsurlar SOME tarafından merkezi olarak kayıt altına alınarak, ilgililerine

bilgilendirmeler yapılıp takibi yapılmalıdır.

6.6. Bilgi güvenliği tehditlerine ilişkin bilgiler toplanmalı ve tehdit istihbaratı oluşturmak için analiz edilmelidir. USOM ve diğer paydaşlar tarafından hazırlanan bülten, duyuru gibi bilgilerin takibi yapılarak Kurum ile ilgili olabilecekler ilgilisine iletilerek takibi yapılmalıdır.

6.7. SOME'de istihdam edilecek personelin sistemli bir şekilde kayıt(iz veya log) analizi ve yönetimi ile adli bilişim analizi yapabilmesi, kurumun bilişim sistemlerindeki önemli güvenlik zafiyetlerini tespit edebilmesi ve siber olay müdahale koordinasyonu yapabilmesi için gerekli olan temel yetkinlikleri vermeyi hedefleyen eğitimler alması ve bilgilerini periyodik olarak güncellemesi sağlanmalıdır.

6.8. Siber olayların yönetimi aşamalarında görev alacak personelin rol ve sorumlulukları tanımlanmalı, olay müdahale için gerekli teknik alt yapı personele sağlanmalı ve belirlenen personel ilgili taraflara bildirilmelidir. Siber olay yönetimi kapsamında görev alacak personel Kurumsal SOME Kurulum ve Yönetim Rehberi kriterlerine mümkün mertebe uygun olmalıdır.

6.9. Organizasyon tarafından kullanılan bilgi işleme sistemlerinin saatleri, onaylanmış zaman kaynaklarıyla senkronize edilmelidir.

6.10. Kritik alanlara personelin fiziksel erişimini iş gereksinimleri doğrultusunda sınırlayan, tüm giriş/çıkışları kayıt altına alan kimlik kontrol mekanizması olmalıdır. Mümkünse yetkisiz erişimi engellemek için bilgi işleme olanaklarının bulunduğu alanlar(Ör: Bilgi İşlem Personeli odaları) diğer alanlardan(Ör: Ziyaretçi, öğrenci alanları) ayrılmalıdır.

6.11. Siber olayların korelasyon kuralları doğrultusunda tespiti ve detaylı analizi için siber tehdit ve olay yönetim sistemleri veya kayıt analizi araçları(Ör: SİEM) kullanılmalıdır.

6.12. SOME, kayıtların İçişleri Bakanlığı tarafından hazırlanan "Olay Sonrasında İncelenmek Üzere Güvenilir Delillerin Elde Edilmesi İçin Tutulacak Kayıtların Asgari Nitelikleri" dokümanına uygun olarak, merkezi bir şekilde tutulmasını ve yönetilmesini sağlamalıdır. Görevler ayrılığı prensibi çerçevesinde, merkezi iz kayıt sistemi yönetiminin, iz kayıtlarını üreten bilişim sistemlerinin sorumlularından bağımsız olarak yapılmasını imkanlar dahilinde sağlanmalıdır.

6.13. Tüm kullanıcılara "Bilgi Güvenliği Farkındalığı" kapsamında: Şüpheli durumları bildirme ve temel güvenlik önlemleri hakkında düzenli eğitimler verilmeli, kurum içi bültenler hazırlanmalı, hatırlatma e-postaları gönderilmeli, siber güvenlikle ilgili ekran koruyucuları ve arka plan resimleri hazırlanmalı, yemekhane, toplantı odaları gibi ortak kullanılan bölgelerine bilgi güvenliğiyle ilgili posterler asılmalı, bilgi güvenliği farkındalığını ölçecek anketler yapılmalıdır.

6.14. SOME ekibi ve tüm kullanıcıların bilinçlenmesi ve olaylara hızlı ve etkili müdahale edebilmesi için düzenli olarak Simülasyonlar ve Tatbikatlar yapılmalıdır. Yapılan çalışmalar sonucu "siber olay yönetim sürecinin" etkinliği belirlenerek eksik yönler düzeltilmelidir.

6.15. Siber olay bildirimi yapılacak resmi kurumlara ilişkin iletişim bilgileri dokümanı oluşturulmalı ve periyodik olarak gözden geçirilmelidir. İletişim bilgileri dokümanı, iletişim kurulacak konu kapsamında iletişim kurulacak kişileri tanımlamalıdır.(Bakınız: "SİBER OLAY İLETİŞİM BİLGİLERİ YÖNETİM PROSEDÜRÜ" ve "SİBER OLAY İLETİŞİM BİLGİLERİ TABLOSU")

6.16. SOME'nin siber olay öncesi, esnası ve sonrasında, siber güvenliği yönetmek amacıyla kurumdaki Bilgi İşlem, Hukuk, Kurumsal İletişim, KVK Koordinatörlüğü ve ilgili diğer birimler(Ör: Personel

Dairesi, İdari Mali İşler, Koruma ve Güvenlik Şubesi vb.) ile birlikte çalışması için gerekli altyapı kurulum ve bilgilendirme işlemleri yapılmalıdır.

6.17. Kurum web sitesinde yayımlanan "**Siber Olaylara Müdahale İş Akış Süreci**"nin ilgili personel tarafından anlaşılarak uygulanması sağlanmalıdır.

7. Siber Olay Esnası

7.1. SOME olay müdahale esnasında bilişim sistemlerine yetkisiz erişim yapılmaması için gerekli tedbirleri alır/aldırır. Kurum içi ve dışı paydaşlara gerekli bilgilendirmeleri yaparak koordinasyonu sağlar. (Siber olay müdahale akışı içinde suç unsuruna rastlanması halinde savcılık, kolluk makamı vb. makamlara haber verilmesi hem kanuni yükümlülüğün yerine getirilmesi, hem de ulusal siber güvenlik kapsamında caydırıcılığın sağlanması açısından önem arz etmektedir.)

7.2. Siber Olay Bildirimi

7.2.1. Siber olay olduğu düşünülen bir durumun oluşması ile "Siber Olay Müdahale Süreci" başlar. İlk yapılması gerekenlerden biri siber olayı KTÜN SOME'ye bildirmektir.

7.2.2. Bildirimler SOME personelinin yönettiği "Sürekli İzleme ve Alarm Sistemleri" (SIEM, IDS/IPS gibi araçlarla ağ trafiği, sistem/uygulama logları vb.) üzerinden ya da SOME personelinin kendi gözlem ve araştırmalarından gelebileceği gibi SOME harici kaynaklardan da gelebilir.

7.2.3. Siber olay bildirim kanalları: Kurumumuz zafiyet bulma programları(Ör: bug bounty, VDP vb.), e-posta(Ör: some@ktun.edu.tr), yazılı(Ör: Dilekçeler, resmi yazılar vb.), sözlü(Ör: telefon, yüzyüze vb.) veya web sitemizde yer alan "Son Kullanıcı Siber Olay Bildirim Formu" ile veya mevzuat gereği takibinin yapılması zorunlu olan platformlar(ULAKNET OLTA, USOM SİP vb.) üzerinden yapılabilir. Bildirimlerin ve bildirimlerle ilgili bilgi alışverişinin mücbir sebepler dışında sözlü olmaması gerekmektedir. Zorunlu nedenlerle sözlü yapılan bildirimler daha sonra mutlaka yazılı hale getirilmelidir.

7.2.4. Bildirim yapılırken olayla ilgili bulunabilen her türlü bilgi(ekran görüntüleri, sistem bilgileri, zaman, yapılan işlemler vb.) belirtilmelidir.

7.2.5. Bildirim hangi kanaldan gelirse gelsin SOME tarafından olaya dair her türlü "bilgi ve yapılan işlem" kayıt altına alınmalı ve takibi yapılmalıdır.

7.3. Bildirimin Sınıflandırılması

7.3.1. Olayın gerçek olup olmadığı(sahte veya false-pozitif) araştırılır.

7.3.2. Olayın **kritiklik derecesi** belirlenir (Ör: Düşük, Orta, Yüksek, Kritik).

7.3.3. Olayın türüne göre (kimlik avı, veri sızıntısı, DDoS, fidye vb.) sınıflandırılır.

7.3.4. Hangi varlıkların etkilendiği (sunucular, ağ cihazları, veri tabanları vb.) kayıt altına alınır.

7.4. **Müdahale**

7.4.1. SOME, Bilgi İşlem Biriminin yapacağı müdahaleyi yönetir ve Bilgi İşlem Birimindeki ilgili personeli koordine eder.

7.4.2. **İlk Müdahale:** Olayın yayılmasını veya daha fazla zarar vermesini önlemek için acil aksiyonlar alınır (etkilenen sunucunun ağdan izole edilmesi, kullanıcı hesaplarının devre dışı bırakılması vb.).

7.4.3. **Analiz ve Kök Neden Belirleme:** Olayın nasıl meydana geldiği, hangi zafiyetin kullanıldığı, ne kadar süredir devam ettiği araştırılır.

7.4.4. **İyileştirme Adımları:** Sistemdeki açıkların kapatılması, yamaların yüklenmesi, yanlış yapılandırmaların düzeltilmesi gibi işlemler yapılır.

7.5. **İletişim ve Raporlama**

7.5.1. **İç İletişim:** İlgili departmanlara (Hukuk, Personel Dairesi, Üst Yönetim vb.) olay hakkında bilgilendirme yapılır.

7.5.2. **Dış İletişim:** Gerekli durumlarda USOM'a, düzenleyici kurumlara (Ör: KVK Kurulu), adli kolluğa, etkilenen paydaşlara (verisi çalınanlara, dolaylı olarak etkilenen kişilere vb.) ve basına bilgi verilir. (KVK Kurulu ile ilgili işlemler KTÜN KVK Koordinatörlüğünce yürütülür.)

7.5.3. **Raporlama:** Olayla ilgili tüm detaylar (tarih, saat, etkilenen varlıklar, müdahale adımları, sonuçlar) kayıt altına alınır.

8. Siber Olay Sonrası

8.1. **Kök Neden Analizi (Root Cause Analysis):** Olayın temel sebebi bulunur ve tekrarını önleyecek önlemler belirlenir.

8.2. **Dokümantasyon ve Öğrenme:** Olayın tüm aşamaları raporlanır, çıkarılan dersler BGYS prosedürlerine entegre edilir.

8.3. **Kurum Yönetimine Önerilerin iletimi:** Olayla ilgili olarak gerçekleştirilebilecek düzeltici/önleyici faaliyetlere ilişkin öneriler kurum yönetimine arz edilir.

8.4. **İstatistiksel verilerin tutulması:** Yaşanan siber olayların türleri, miktarları ve maliyetleri ölçülüp izlenir.

8.5. **Takip ve Denetim:** Yapılan iyileştirmelerin etkinliği düzenli olarak kontrol edilir.

9.Yaptırım

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

10.Yürürlük

Bu politika, BGYS komisyonu tarafından onaylandıktan sonra Bilgi İşlem Daire Başkanlığının web

sayfasında yayımlanarak duyurusu yapıldığı tarihte yürürlüğe girer.

11.Yürütme

Bu politika, Bilgi İşlem Daire Başkanlığı tarafından yürütülür.