1. AMAÇ

Bu politikanın amacı; Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında bilgi güvenliği, bilgi teknolojileri ve iş sürekliliğini etkileyebilecek kriz ve acil durumlarda uygulanacak temel esasları, görev ve sorumlulukları belirlemek ve kritik hizmetlerin kabul edilebilir süreler içerisinde sürdürülebilmesini veya kontrollü şekilde yeniden devreye alınmasını sağlamaktır.

2. KAPSAM

Bu politika;

- Süleyman Demirel Üniversitesi Daire Başkanlıklarını,
- Genel Sekreterliği,
- Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimini,
- Kurumun bilgi sistemlerini, bilişim altyapısını ve kritik bilgi varlıklarını,
- Bilgi güvenliği olaylarını,
- Siber saldırı, kötü amaçlı yazılım, yetkisiz erişim, bilgi kaybı veya ifşası gibi bilgi güvenliği tehditlerini,
- Donanım, yazılım, ağ ve iletişim altyapısında meydana gelebilecek kritik kesintileri,
- Yangın, su baskını, enerji kesintisi, doğal afet ve benzeri iş sürekliliğini etkileyebilecek olayları,
- Kritik hizmetlerin sürekliliğini veya yeniden devreye alınmasını gerektiren diğer kriz ve acil durumları kapsar.

3. SORUMLULUK

3.1. Bilgi İşlem Daire Başkanlığı

- Bilgi teknolojileri kaynaklı kriz ve acil durumlara müdahalenin koordinasyonundan,
- Kritik bilgi sistemlerinin ve bilişim altyapısının sürekliliği için gerekli teknik tedbirlerin alınmasından,
- Yedekleme, geri yükleme ve felaket kurtarma altyapısının işletilmesinden,
- Bilgi güvenliği olaylarının ilgili süreçler kapsamında yönetilmesinden,
- Kriz ve acil durumlarda gerekli teknik kayıtların tutulmasından sorumludur.

3.2. Birim Yöneticileri

Kendi sorumluluk alanlarındaki kritik hizmet, süreç ve bilgi varlıklarının kriz ve acil durumlara hazırlık çalışmalarına katkı sağlar ve gerekli durumlarda müdahale faaliyetlerini koordine eder.

3.3. Acil Durum / Kriz Müdahale Ekipleri

Acil durum veya kriz meydana geldiğinde kendilerine verilen görev ve yetkiler doğrultusunda müdahale, koordinasyon, iletişim, kurtarma ve yeniden devreye alma faaliyetlerini yürütür.

3.4. Çalışanlar

- Karşılaştıkları bilgi güvenliği olaylarını veya acil durumları ilgili bildirim kanallarından iletmek,
- Kendilerine verilen acil durum talimatlarına uymak,
- Yetkileri dışında müdahalede bulunmamak,
- Kriz ve acil durum sırasında kendilerine verilen görevleri yerine getirmek ile yükümlüdür.

4. UYGULAMA

4.1. Kriz ve Acil Durumların Belirlenmesi

Kurumun bilgi güvenliği, bilgi teknolojileri veya kritik hizmetlerini etkileyebilecek olaylar değerlendirilerek kriz veya acil durum niteliği belirlenir.

Bunlara örnek olarak;

- Siber saldırılar,
- Kötü amaçlı yazılım ve fidye yazılımı olayları,
- Yetkisiz erişim,
- Kritik bilgi veya veri kaybı,
- Bilgi sistemlerinde uzun süreli kesinti,
- Sunucu veya veri depolama sistemlerinin kullanılamaz hale gelmesi,
- Ağ ve iletişim altyapısı kesintileri,
- Enerji kesintileri,
- Yangın, su baskını, doğal afet ve benzeri olaylar verilebilir.

4.2. Görev, Yetki ve Sorumlulukların Belirlenmesi

Kriz ve acil durumlarda görev alacak kişiler önceden belirlenir.

Görevlendirilen kişilerin;

- Görevleri,
- Yetkileri,
- Sorumlulukları,
- İletişim bilgileri,
- Yedek görevlileri dokümante edilir ve ihtiyaç halinde erişilebilir durumda tutulur.

4.3. Kriz ve Acil Durum Bildirimi

Kriz veya acil durum meydana geldiğinde olayın niteliğine ve etkisine göre ilgili sorumlulara ve yöneticilere bildirim yapılır.

Bildirim mekanizması;

- Olayın tespiti,
- İlk bildirim,
- İlgili ekiplerin bilgilendirilmesi,
- Yönetim seviyesinde eskalasyon,
- Gerekli iç ve dış iletişim aşamalarını kapsayacak şekilde belirlenir.

4.4. Müdahale ve Koordinasyon

Kriz veya acil durumlarda müdahale faaliyetleri önceden belirlenmiş görev ve sorumluluklar çerçevesinde yürütülür.

Müdahale sırasında;

- İnsan ve bilgi güvenliğinin korunması,
- Olayın yayılmasının veya etkisinin artırılmasının önlenmesi,
- Kritik hizmetlerin önceliklendirilmesi,
- Kritik sistemlerin korunması,
- Gerekli durumlarda sistemlerin izole edilmesi,
- Yedek sistemlerin devreye alınması sağlanır.

4.5. Kritik Sistemlerin Sürekliliği

Kritik bilgi sistemleri ve hizmetler için belirlenen süreklilik gereksinimleri doğrultusunda uygun teknik ve idari tedbirler uygulanır.

İhtiyaca ve risk değerlendirmelerine bağlı olarak;

- Kümeleme,
- Yedekli sistemler,
- Uzaktan kopyalama,
- Yedek sistemler,
- Alternatif altyapılar,
- Felaket kurtarma çözümleri kullanılabilir.

Uygulanacak çözümler, kurumun iş sürekliliği ve bilgi güvenliği riskleri dikkate alınarak belirlenir.

4.6. Yedekleme ve Kurtarma

Kritik bilgi sistemleri ve veriler için belirlenen yedekleme kurallarına uygun olarak yedekleme yapılır.

Acil durumlarda gerekli olması halinde yedeklerden geri dönüş ve sistem kurtarma işlemleri gerçekleştirilir.

Yedekleme ve geri yükleme faaliyetleri ilgili yedekleme ve iş sürekliliği süreçlerine uygun olarak yürütülür.

4.7. Bilgi Güvenliği Olayları

Bilgi güvenliği ihlali veya şüphesi bulunan durumlarda Olay İhlal Prosedürü uygulanır. Olayın kriz seviyesine ulaşması halinde ilgili kriz ve iş sürekliliği süreçleri de devreye alınır.

4.8. Kayıtların ve Logların Korunması

Kriz ve güvenlik olayları sırasında oluşan;

- Sistem logları,
- Güvenlik kayıtları,
- Olay bildirimleri,
- Müdahale kayıtları,
- Yapılan işlemlere ilişkin kayıtlar olayın incelenmesi, adli süreçler ve kök neden analizleri açısından gerekli olduğu ölçüde korunur.

Kayıtların bütünlüğü, gizliliği ve yetkisiz değişikliğe karşı korunması sağlanır.

4.9. Adli ve Hukuki Süreçler

Kriz veya bilgi güvenliği olayının hukuki veya adli inceleme gerektirmesi halinde ilgili yöneticilerin değerlendirmesi doğrultusunda, yetkili kamu kurumları veya diğer ilgili makamlarla gerekli koordinasyon sağlanır. Delil niteliği taşıyabilecek kayıtların korunması ve yetkisiz şekilde değiştirilmemesi sağlanır.

4.10. Alternatif Çalışma ve Felaket Kurtarma

Kritik hizmetlerin normal çalışma ortamında sürdürülememesi durumunda, kurumun iş sürekliliği ve felaket kurtarma planlarında belirlenen alternatif çalışma ve kurtarma yöntemleri uygulanır.

Felaket kurtarma faaliyetleri;

- Öncelikli sistemlerin belirlenmesi,
- Alternatif sistemlerin devreye alınması,
- Yedeklerden geri dönüş,
- Sistemlerin kontrollü şekilde yeniden çalıştırılması,
- Hizmetlerin normal işletim ortamına geri aktarılması aşamalarını kapsayabilir.

4.11. Kriz Sonrası Değerlendirme

Kriz veya acil durum sona erdikten sonra olayın nedenleri, etkileri ve gerçekleştirilen müdahaleler değerlendirilir.

Gerekli görülen durumlarda;

- Kök neden analizi yapılır,
- Düzeltici faaliyetler başlatılır,
- Risk değerlendirmeleri güncellenir,
- İş sürekliliği ve felaket kurtarma planları gözden geçirilir,
- İlgili politika ve prosedürler revize edilir,
- Benzer olayların tekrarını önlemeye yönelik tedbirler belirlenir.

4.12. Test ve Tatbikatlar

Kriz, iş sürekliliği ve felaket kurtarma süreçlerinin uygulanabilirliğinin değerlendirilmesi amacıyla ihtiyaç ve riskler doğrultusunda test ve tatbikatlar gerçekleştirilir.

Tatbikat sonuçları kayıt altına alınır ve tespit edilen eksiklikler için gerekli iyileştirme faaliyetleri başlatılır.

4.13. İletişim

Kriz ve acil durumlarda iletişim ve bilgilendirme faaliyetleri önceden belirlenmiş iletişim kanalları ve yetkilendirmeler doğrultusunda yürütülür. Krizle ilgili kurum dışına yapılacak açıklamalar yalnızca yetkilendirilmiş kişiler tarafından gerçekleştirilir.

5. YAPTIRIM

Bu politikada belirtilen kurallara aykırı gerçekleştirilen faaliyetler ilgili EYS süreçleri kapsamında değerlendirilir. Gerektiğinde yürürlükteki mevzuat, kurum düzenlemeleri ve ilgili Disiplin Prosedürü hükümleri uygulanır.