1. Amaç

Bu doküman, Kütüphane ve Dokümantasyon Daire Başkanlığı bünyesindeki bilgi sistemlerinin güvenli işletiminin sağlanması için gerekli hususları tanımlamak amacıyla oluşturulmuştur.

2. Kapsam

SDÜ0PL09 İşletim Güvenliği Politikası, SDÜ6GE01 BGYS Kapsamı dokümanında belirtilen tüm bilgi varlıklarını kapsar.

3. Tanımlar

Kurum: Kütüphane ve Dokümantasyon Daire Başkanlığı

BGYS: Bilgi Güvenliği Yönetim Sistemi

4. Uygulama

4.1 Canlı Ortam Yönetimi

Geliştirme, test ve canlı ortamlar yetkisiz erişim ve değişiklik risklerinin azaltılması amacıyla ayrı işletilir.

Canlı ortamdaki sistemlere, yalnızca sistemin amacına uygun şekilde çalışması için gerekli yazılımlar kurulur.

Canlı ortamdaki uygulamalar, yalnızca bu konuda yetkilendirilmiş kişiler tarafından güncellenebilir.

Canlı sistemlerde geliştirmeye ilişkin kod ve derleyici uygulamalar bulundurulmaz.

Canlı sistem ve uygulamaların güncellenmesi durumunda, 2 önceki sürüme kadarki kod, parametre, kütüphane ve yapılandırma detayı saklanır.

4.2 Yazılı İşletim Talimatları

Hazırlayan	Kontrol	Onay
Öğretim Görevlisi – S. Onur ERDEM	Şube Müdürü – Şaban NALDEMİR	Daire Başkanı – Uğur BULGAN

Kuruluş bünyesindeki tüm bilgi sistemleri yazılı işletim talimatlarına göre işletilir.

Yazılı işletim talimatları aşağıdaki bilgileri içerir:

- Sistem kurulumu ve yapılandırması
- Yetkilendirme
- Diğer sistemlerle entegrasyon ve bilgi alışverişi
- Arıza durumunda sistemi yeniden başlatma
- Arıza durumunda iç/dış destek için gerekli iletişim bilgileri
- Sistem kayıtları
- Kapasite ve performans izleme

4.3 Değişiklik Yönetimi

Kritik iş süreçlerinin güvenliğini kesintiye uğratma potansiyeline sahip olan, bilgi sistemlerinde ya da bilgi sistemlerini destekleyen altyapıda yapılacak tüm değişiklikler, aşağıdaki hususlar göz önüne alınarak gerçekleştirilir.

Yapılan değişiklikler, aşağıdaki detayı içerecek şekilde kayıt altına alınır.

- Değişiklik yapılacak bilgi varlığı
- Değişikliği talep eden kişi
- Değişikliği gerçekleştirecek kişi
- Değişikliğin gerekçesi
- Değişikliğin gerekli teknik detayları da içeren açıklaması
- Değişikliğin gerçekleştirileceği tarih ve saat
- Beklenen kesinti süresi

Değişiklikler gerçekleştirilmeden önce iş etkisi analizi yapılır.

Hizmet kesintisi yaratacak değişikliklerde, iş süreci sahiplerinin onayı alınır.

Değişiklikler, iş süreci sahiplerinin onaylamaması ya da herhangi bir teknik aksaklık durumuna karşı, sistemin bir önceki kararlı yapılandırmayla çalıştırılması esasına göre planlanır.

Gerçekleştirilen değişiklikler sonrasında, ilgili sistem ve altyapıya ait olay kayıtları 2 iş günü süresince izlenir.

Dış kaynaktan destek alınan sistemlerdeki önemli değişikliklerde, destek alınan firma bilgilendirilerek, acil durumda müdahaleye hazır olması sağlanır. Yeni alınan teçhizat, test ortamında denenmeden canlı ortama alınmaz.

Değişiklikler test ortamında denenir, canlı ortamlarda test hiçbir koşulda gerçekleştirilmez.

Canlı ortamdan test ve geliştirme ortamlarına veri aktarma, gizliliği korumak amacıyla gizleme, değiştirme ve maskeleme gibi yöntemler ile gerçekleştirilir.

4.4 Yapılandırma Yönetimi

Kritik iş süreçlerinin güvenliğini kesintiye uğratma potansiyeline sahip olan, bilgi sistemleri ya da bilgi sistemlerini destekleyen altyapının yapılandırması, aşağıdaki hususlar göz önüne alınarak gerçekleştirilir.

Sistem ve altyapıların ağ şemaları, veri akış şemaları ve yapılandırma bilgileri dokümante edilir ve güncel tutulur.

Yapılandırmanın, sistem ya da altyapıya ilişkin üretici firmanın önerdiği şekilde gerçekleştirilmesine dikkat edilir.

Yapılandırma işlemleri, değişiklik yönetimi kapsamında gerçekleştirilir. Değişikliğin başarısız olması, beklenen sonucu üretmemesi ya da felaket durumunda onaylanmış son çalışan yapılandırma durumuna geri dönülür.

Yapılandırmaya ilişkin veriler düzenli olarak yedeklenir.

4.5 Kapasite Yönetimi

Kuruluş bünyesindeki kritik iş süreçlerine destek veren sistem ve altyapıya ilişkin kaynakların, kapasite ihtiyacının önceden belirlenebilmesi amacıyla, aşağıdaki hususlar göz önüne alınarak kapasite yönetimi uygulanır.

Kapasite gereksinimleri, sistemin iş kritikliği göz önüne alınarak belirlenir.

Kapasitesi izlenecek olan varlıklara ilişkin olarak, izlenecek bileşenler ve izleme sıklıkları varlık sahibi tarafından belirlenir.

Yeterli kapasitenin sağlanabilmesi amacıyla kapasite arttırma ya da talep azaltma yöntemleri uygulanabilir.

Kapasite izleme verileri, bilgi sistemlerine ilişkin iyileştirme, geliştirme ve satın alma süreçlerinde girdi olarak kullanılır.

Sistem güvenliği ve işletimi bakımından tehdit oluşturabilecek olan kritik personele ilişkin yedeklilik planları oluşturulur.

4.6 Olay Kaydetme ve İzleme

Bilgi güvenliği ihlal olaylarının etkilerini ve kök nedenlerini belirleyebilmek amacıyla BİDB sistem ve altyapısına ilişkin olaylar, aşağıdaki hususlar göz önüne alınarak izlenir.

Kayıtlar, ilgili yasa, sözleşme ve mevzuatın gereksinimini karşılayacak sürelerde saklanır.

Kayıtlar yetkisiz erişim, değiştirme ve silinmeye karşı korunur.

Kayıt dosyalarının kapasitesi, kapasite yönetimi kapsamında izlenir.

Aşağıdaki olaylara ilişkin aktiviteler kaydedilir.

- Kullanıcı internet erişimi (5651)
- Kullanıcı yaratma, silme, güncelleme
- Kritik altyapı yapılandırması
- E-Mail Kayıtları
- Sistem odası giriş/çıkış kayıtları
- Sistem odası giriş/çıkış kamera görüntüleri
- Zararlı yazılımlardan korunma sistemleri olay kayıtları

4.7 Zararlı Yazılımlardan Korunma

Bilgi varlıklarını zararlı yazılım tehditlerinden korumak amacıyla, aşağıdaki hususlar göz önüne alınarak önlemler uygulanır.

Kullanıcılar, cihazlarının güvenlik ayarlarını değiştiremez.

Kullanıcı cihazlarının taşınabilir veri depolama ünitesi bağlantıları engellenir. İş gereğince, herhangi bir alternatif yöntem bulunamaması nedeniyle taşınabilir veri depolama ünitesi kullanmak zorunda olan kullanıcılara, BGYS Komisyonu Başkanı'nın teknik ve Bilgi İşlem Daire Başkanı'nün idari onayı ile erişim sağlanabilir.

İnternet kaynaklı zararlı yazılım tehditlerinden korunmak amacıyla, kurumsal internet bağlantısında Sophos ve Roksit ile içerik, URL ve DNS filtreleme gibi koruma önlemleri alınır.

E-Mail kaynaklı zararlı yazılım tehditlerinden korunmak amacıyla, e-mail giriş ve çıkışlarında GMAIL sisteminin koruma önlemleri uygulanır.

Kullanıcı cihazları ve sistemler, merkezi olarak yönetilen Trend Micro yazılımı ile korunur.

Antivirüs yazılımı, istemcileri düzenli tarayacak şekilde ayarlanır.

Kullanıcıların antivirüs servisini ya da uygulamasını durdurma, duraklatma ya da ayarlarını değiştirme yetkisi bulunamaz.

Kullanıcı bilgisayarlarına bilerek ya da bilmeyerek zararlı yazılım kurulumunun engellenmesi amacıyla local administrator yetkileri alınır.

Herhangi bir sistemde zararlı yazılımla karşılaşıldığında, ilk aksiyon zararlı yazılımın yayılmasını engellemektir. Zararlı yazılımın etkisinin belirlenmesinden sonra, sistemdeki verilerin bütünlüğünün zarar görmeyeceği şekilde temizleme işlemleri yürütülür. Temizlemenin mümkün olmadığı zararlı yazılım saldırılarında yedekten dönme işlemi uygulanır.

Kullanıcıların zararlı yazılımlara karşı bilgi seviyelerinin arttırılması amacıyla düzenli olarak farkındalık çalışmaları yürütülür.

4.8 Teknik Açıklıkların Yönetimi

Tehdit kaynaklarının, kuruluşa ait bilgi varlıklarının olası teknik açıklıklarından yararlanmasını engellemek amacıyla, aşağıdaki hususlar göz önüne alınarak önlemler uygulanır.

Bilgi sistemlerinde, aygıtların, işletim sistemlerinin, platformların ve uygulamaların üretici tarafından desteklenen ve kararlı olan son sürümleri kullanılır.

Bilgi varlıkları envanteri, kuruluşta kullanılan tüm uygulamalar, kurulu oldukları cihazlar, üretici firma ve sürüm bilgisini de içerecek şekilde tutulur.

İstemci uygulamalarında, teknik açıdan onaylanmış ve dokümante edilmiş kısıtlı sayıda sürüm kullanılır.

Kullanıcılar, istemcilerde yazılım kurma hakkına sahip değildir.

Teknik açıklıklar hakkında destekleyici bilgilerin edinilebilmesi amacıyla, Ulakteknik, Çözümpark, InnoveraBT, Datascience ve BTK siteleri izlenir.

Bilgi sistemlerine ve uygulamalara ilişkin teknik açıklıklar, Nessus ve Alienvault uygulamaları kullanılır. Alienvault uygulaması sürekli olarak devrededir, Nessus ise haftalık sıklıkta çalıştırılır.

Teknik açıklıkların kapatılmasında kullanılacak olan yamalar ve güncelleştirmeler ürünün üretici firmasından ya da güvenilir kaynaklardan elde edilir.

Bilgi sistemlerine ilişkin, yılda en az bir kez sızma testi gerçekleştirilir.

4.9 Yedekleme

Elektronik ortamdaki veriler ve sistem imajları, olası kayıplardan korunmak amacıyla, aşağıdaki hususlar göz önüne alınarak Veeam Backup ile yedeklenir.

Verilerin hangi sıklıkta yedekleneceğine ve geri dönüş testlerinin yapılacağına, yedeklenen verilerin ne kadar süreyle saklanacağına varlık sahibi karar verir.

Yedeklenen veriler, fiziksel/çevresel koşulların verilerin erişilebilirliğini ve bütünlüğünü bozmayacağı ortamlarda barındırılır.

4.10 Denetim

Denetim faaliyetleri, canlı sistemler üzerindeki etkilerin en aza indirilmesi amacıyla, aşağıdaki hususlar göz önüne alınarak gerçekleştirilir.

Sistemler ve verilere erişim için Bilgi İşlem Daire Başkanı'nın onayı alınır.

Teknik denetimin kapsamı belirlenir ve bu kapsama uyulduğu kontrol edilir.

Yürütülecek denetimlerde veriye yalnızca okunur erişim sağlanabilir. Yalnızca okunur dışındaki erişim, verinin yalıtılmış kopyası üzerinden sağlanır. Denetimin bitiminde söz konusu kopyalar silinir ya da denetimin zorunlu koştuğu şekilde güvenli biçimde saklanır.

Sistemin erişilebilirliğini etkileme potansiyeli olan denetim çalışmaları mesai saatleri dışında yürütülür.

Gerçekleştirilen tüm denetim faaliyetlerinin kayıtları tutulur.

4.11 İş Sürekliliği

Kurum'a ait kritik iş süreçlerinin sürekliliğinin sağlanması ve kesinti durumunda en kısa zamanda ayağa kaldırılmasına ilişkin esasların hususları belirlemek amacıyla, aşağıdaki hususlar göz önüne alınarak iş sürekliliği yönetimi gerçekleştirilir

İş sürekliliği yönetimi, kritik iş süreçlerini destekleyen bilgi varlıklarının sürekliliğini sağlamayı, alınan önlemlere rağmen herhangi bir nedenle kesintiye uğraması durumunda ise en kısa zamanda normal çalışma durumuna döndürülmesini amaçlar.

Kritik bilgi tesis ve sistemleri, iş sürekliliği gereksinimlerini karşılamak amacıyla, yedekli ve yük paylaşımlı mimarilerle ve yeterli fazlalıkla işletilir.

İş sürekliliği yönetiminde felaketten dönüş planlaması yapılırken 3 değer önem taşır.

- Geri Dönüş Süresi: Kesinti sonrasında, hizmetlerin en çok ne kadar sürede yeniden çalışır hale getirileceği hedefini tanımlayan değerdir.
- Geri Dönüş Anı: Kesinti sonrasında, hizmetlerin kesinti anından en çok ne kadar geriye dönebileceği hedefini tanımlayan değerdir.
- Kabul Edilebilecek En Uzun Kesinti Süresi: İş sürecinin en çok ne kadar süreyle durabileceğini tanımlayan değerdir.

İş Sürekliliği ve Felaketten Dönüş Planı, Geri Dönüş Süresi, Geri Dönüş Anı ve Kabul Edilebilecek En Uzun Kesinti Süresi değerleri temel alınarak oluşturulur.

Hazırlanan felaketten dönüş senaryoları ve planları yılda bir kez test edilir.

Yaşanacak bir felaket sonrasında, risk değerlendirme faaliyetleri yinelenir.

Felaket ya da test sonrasında, felaketten dönüş için uygulanan planın etkinliği gözden geçirilerek, gerek görülürse planlar güncellenir.

İş sürekliliği planları hazırlanırken, felaket durumunda bilgi varlıklarının erişilebilirlik, gizlilik ve bütünlüğünün sürdürülmesine ilişkin önlemler göz önüne alınır.