1. AMAÇ

Bu prosedürün amacı, Bursa Uludağ Üniversitesi bünyesindeki Bilgi İşlem Daire Başkanlığı kapsamındaki işletim prosedürlerinin güvenlik çerçevesinde yönetim esaslarını belirlemektir.

2. KAPSAM

Bu prosedür, Bursa Uludağ Üniversitesi bünyesindeki Bilgi İşlem Daire Başkanlığı için belirtilen ve uyulması gereken hususlar kurum çalışanları veya üçüncü taraflarca kullanılan tüm bilgi sistemleri için geçerlidir.

3. TANIMLAR VE KISALTMALAR

Özel bir tanım bulunmamaktadır.

4. SORUMLULUK

Görevlerini yerine getirirken tüm kullanıcılar, sistem ve network yöneticileri, uygulamalar ve sistemler bu politikaya tabidir. Bu politikadan muafiyetlere ancak Bilgi güvenliği yöneticisinin önceden ve yazılı olarak izin verildiğinde izin verilecektir. Dokümanlar ihtiyaç halinde revize edildiği gibi, yılda bir kez periyodik olarak kontrol edilir.

5. UYGULAMA

5.1 Yazılı İşletim Prosedürleri

Bilgi sistemlerinin işletiminden ve kullanımından sorumlu personellerin, işletim faaliyetlerini nasıl sürdürmesi gerektiğine dair prosedürler yazılı hale getirilerek ilgili kullanıcıların erişimine sunulur.

İşletim prosedürleri ve sistem faaliyetleri için prosedürlerin yazılı hali resmi olarak kabul edilir ve yetkili yönetim tarafından değişiklikler yapılabilir. Teknik olarak mümkün olan durumlarda bilgi sistemleri aynı prosedürler, araçlar ve yardımcı programlar kullanılarak sürekli olarak yönetilir.

5.2 Değişiklik Yönetimi

Bilgi güvenliğini etkileyen, kurum iş süreçleri, bilgi işleme tesisleri ve sistemlerdeki değişiklikler kontrol edilir. Değişiklik kontrol yönetiminde aşağıdaki prensipler göz önünde bulundurulur.

- Önemli değişikliklerin tanımlanması ve kaydedilmesi,
- Değişikliklerin planlanması ve test edilmesi,
- Değişikliklerin bilgi güvenliği ve iş sürekliliği etkileri de dâhil potansiyel etkilerinin değerlendirilmesi,
- Önerilen değişiklikler için resmi onay,
- Bilgi güvenliği gereksinimlerinin karşılandığının doğrulanması,
- Kritik durumlarda geri dönüş senaryoları değerlendirilmelidir.

Değişiklikler yapıldığında ilgili tüm bilgileri içeren denetim kayıtları tutulur.

Ek : FR 3.3.2_12 Yeni sunucu ve mevcut sunucu değişiklik talep formu.
Ek : FR 3.3.1_01 Yeni yazılım ve mevcut yazılım değişiklik talep formu.

5.3 Kapasite Yönetimi

Kapasite gereksinimleri söz konusu sistemin iş kritikliği dikkate alınarak belirlenir. Sistemi ayarlama ve izleme, gerekli hallerde, sistemlerin kullanılabilirliğini ve verimliliğini artırmak için uygulanır. Tarama ve izleme kontrolleri zamanında sorunları tespit etmek için önemlidir. Gelecekteki kapasite gereksinimlerinin kestirimleri, yeni iş ve sistem

gereksinimlerini ve kuruluşun bilgi işleme yeteneklerinde mevcut ve öngörülen eğilimlerini dikkate anılarak değerlendirilir.

Uzun tedarik sürelerine ve yüksek maliyetlere sahip sunucu ve sistem kaynakları için özel ilgi gerekir. Bu nedenle bu kritiklikteki sistem kaynakları mutlaka izlenir. İş Uygulamaları ve Yönetim Bilgi sistemlerine ait sistem kaynaklarının kullanım eğilimleri sistem yöneticilerince izlenerek kayıt altına alınır.

Sistem ve network yönetiminden sorumlu personeller, sistem güvenliği veya hizmetleri için bir tehdit sunan kilit personelin üzerindeki darboğazları ve bağımlılığı belirlemek ve önlemek için bu bilgileri kullanır ve uygun aksiyonları gerçekleştirir. Yeterli kapasitenin sağlanması, kapasite arttırılarak ya da talep azaltılarak elde edilebilir. Kapasite talep yönetim örnekleri aşağıdaki hususları içerir:

- Kullanılmayan verinin silinmesi (disk alanı),
- Uygulamaların, sistemlerin, veri tabanlarının ya da ortamların hizmetten çıkarılması,
- Toplu proseslerin ve zamanlamaların optimizesi,
- Uygulama mantığının ya da veri tabanı sorgularının optimize edilmesi,
- Eğer iş kritik değilse kaynak tüketen hizmetler için reddetme ya da bant genişliği sınırlaması

(Örneğin; Video akışları)

5.4 Geliştirme, Test ve İşletim Ortamlarının Birbirinden Ayrılması

Geliştirme, test ve işletim ortamları, yetkisiz erişim veya işletim ortamlarında değişiklik risklerinin azaltılması için birbirinden ayrılmıştır. Geliştirme, test ve işletim ortamları aynı sunucu/bilgisayar üzerinde barındırılmaz. Mümkünse farklı etki alanları ve ağlarda konumlandırılır.

Yapılacak güncelleme veya yeni uygulama kurulumları ilk önce test sunucusunda gerçekleştirilip daha sonra canlı sistemlere kurulumlar yapılmalıdır. Yapılan her geliştirme ve yeni kurulum işlemleri değişiklik yönetimi dikkate alınarak gerçekleştirilmeli ve değişiklik kayıt formuna işlenerek kayıt altına alınmalıdır.

Kötücül Yazılımlardan Korunma; zararlı yazılıma karşı koruma; zararlı yazılım kod tespitine ve yazılım onarımına, güvenlik bilincine ve uygun sistem erişim ve değişim yönetimi kontrollerine dayanır. Zararlı yazılımlardan korunmaya ilişkin aşağıdaki prensipler dikkate alınır:

- Zararlı içerik barındıran web sitelerine erişim firewall üzerinden Url ve içerik filtreleme ile engellenir.
- Özel kritiklik seviyesinde olan sistemler gerekli görüldüğü takdirde dış dünyadan yalıtılır.
- Devreye alınacak anti virüs uygulamalarının, mümkünse sistemlerde düzenli gözden geçirme ve dosyalarda yetkisiz değişikliklerin izlenmesini sağlayacak özellikte olmasına dikkat edilir.
- Kullanıcılara teslim edilen bilgisayarlar Anti Virüs uygulaması kurulmadan teslim edilmez.
- İşletim Sistemleri haftada en az bir kez olmak üzere otomatik anti virüs uygulaması ile taranır.
- İşletim sistemlerindeki Anti Virüs uygulamaları son kullanıcıların yetkisiz devre dışı bırakmasına karşı şifre korumalıdır.
- Tüm personel, Bilgi Güvenliği Farkındalık Eğitimleri ile zararlı yazılımlara karşı bilinçlendirilir.
- Zararlı yazılım bulaşma riski değerlendirilerek, gerekli yedekleme, kurtarma ve İş sürekliliği planları hazırlanır.
- Periyodik olarak test edilir.
- Güncel zararlı yazılımlardan haberdar olmak için özel ilgi grupları ile iletişim halinde kalınır.
- Firewall, router vb. ağ cihazlarının Firmware güncelleştirmeleri düzenli takip edilerek, güncel versiyonun kullanılması sağlanır.
- İşletim Sistemlerinin Güncelleştirme ve Yama yönetimi için uygun kontroller sağlanır.
- Mail sistemleri için gerekli anti-spam kontrolleri uygulanır.
- Mail yoluyla gelebilecek phishing saldırılarına karşı mail altyapısının SPF, PTR ve Reverse DNS kontrolleri uygulaması sağlanır.

5.5 Yedekleme

Bilgi ve sistemler, süreç sahipleri ve birim yöneticilerinin yedekleme gereksinimleri dikkate alınarak yedeklenir. Yedeklemenin frekansı, türü ve ortamı ile birlikte yedeklenecek veri süreç sahipleri ile istişare edilerek belirlenir ve bu doğrultuda yedekleme planı oluşturulur.

Yedekleme planları, bir felaket veya ortam hatasından sonra gerekli tüm bilgi ve yazılımın telafi edilebilir olmasından emin olunacak şekilde oluşturulur.

Yedekleme planı tasarlanırken aşağıdaki prensipler dikkate alınır:

- Yedeklerin türü (örneğin; tam veya diferansiyel yedekleme) ve sıklığının kuruluşun iş gereksinimlerini, ilgili bilgilerin güvenlik gereksinimlerini ve kuruluşun sürekli çalışması için bilginin kritikliğini yansıtır.
- Yedeklemeler, mümkünse merkezde bir felaketten dolayı görülecek hasardan kaçınmak için yeterli bir mesafede olan uzak bir yerde muhafaza edilecek şekilde planlanır.
- Yedekleme bilgileri, fiziksel ve çevresel etkilere karşı korunur.
- Yedekleme ortamı, acil durumlarda kullanmak gerektiğinde kullanılabilir durumda olduğundan emin olmak için düzenle aralıklar ile test edilir.
- Yedekten geri dönüş testleri test ortamında yapılır, orijinal ortamlarda yedekleme ya da geri yükleme sürecinin başarısız olması durumunda onarılamaz veri kaybına ya da hasarına neden olabileceğinden orijinal ortamında yapılmaz.
- Gizliliğin önemli olduğu (yedeklenen verinin hassas veri olması durumunda) durumlarda, yedeklemenin şifreleme yoluyla korunması gerekir.

EK: FR 3.3.2_09 Yedek Alma Takip Formu

5.6 Kaydetme ve İzleme

5.6.1 Olay Kaydetme

Kullanıcı faaliyetleri, istisnai durumlar, hatalar ve bilgi güvenliği olaylarını kaydeden olay kayıtları ilgili sistemlerden toplanarak saklanır ve gerektiğinde gözden geçirilir. Olay Kayıtları, hassas veri ve kişisel kimlik bilgileri içerebilir. Bu gibi loglara yönelik uygun koruma yöntemleri belirlenir.

Loglarda mümkün olduğunca aşağıdaki içerikler yer alır:

- Kullanıcı kimlikleri,
- Sistem faaliyetleri,
- Oturum açma ve oturum kapatma gibi anahtar olayların tarihleri, saatleri ve detayları,
- Mümkünse aygıt kimliği ya da yeri ve sistem tanımlayıcısı,
- Başarılı ve reddedilmiş, sistem erişim girişimlerinin kayıtları,
- Erişilen dosyalar ve erişim türü,
- Ağ adresi ve protokolleri,
- Anti-virüs sistemleri ve saldırı tespit sistemleri gibi koruma sistemlerinin etkinleştirilmesi ve devre dışı bırakılması,
- Uygulamalarda kullanıcılar tarafından yürütülen işlemlerin kayıtları.

5.6.2 Kayıt Bilgisinin Korunması

Log kayıt ortamlarına erişim yalnızca yetkili personelce sağlanır ve erişim yetkileri periyodik olarak gözden geçirilir.

5.6.3 Yönetici ve Operatör Kayıtları

5.6.1 Maddesindeki log kayıt kuralları çerçevesinde kayıtları tutulmaktadır.

5.7 Saat Senkronizasyonu

Etki alanında yer almayan sistemlere de NTP adresi girilerek saat senkronizasyonu sağlanır.

5.8 İşletimsel Yazılım Kontrolü

İhtiyaç duyulan yazılım yüklemeleri Bilgi Teknolojileri personelince gerçekleştirilir. İşletim sistemlerinde yazılım kurulumuna ilişkin kontrollerde aşağıdaki prensipler göz önünde bulundurulur:

- İşletimdeki sistemlerde (Canlı Sistemlerde) sadece çalıştırılabilir onaylı kod bulundurulur, geliştirme kodu ya da derleyiciler bulundurulmaz.
- Uygulama ve işletimsel sistem yazılımları sadece kapsamlı ve başarılı bir şekilde test edildikten sonra uygulanır.
- Testler, kullanılabilirliği, güvenliği, diğer sistemlere etkiyi ve kullanıcı dostluğunu kapsar ve ayrı sistemler üzerinde yapılır.
- Yazılımsal değişiklikleri uygulamadan önce bir geri alma stratejisi belirlenir.
- Gerektiğinde uygulama yazılımının önceki sürümleri bir acil durum önlemi olarak saklanır.
- Yazılımının eski sürümleri tüm gerekli bilgi, parametreler, prosedürler, yapılandırma detayları ve destekleyen yazılım ile birlikte veriler arşivde tutulabildiği sürece saklanır.

6. İLGİLİ DOKÜMANLAR

TS ISO / IEC 27001 Bilgi Güvenliği Yönetim Sistemi
TS ISO / IEC 27002 Bilgi Teknolojisi-Güvenlik Teknikleri Bilgi Güvenliği Yönetimi için Uygulama Kuralları

FR 3.3.2_12 Yeni Sunucu ve Mevcut Sunucu Değişiklik Talep Formu
FR 3.3.1_01 Yeni Yazılım ve Mevcut yazılımda Değişiklik Talep Formu
FR 3.3.2_09 Yedek Alma Takip Formu
FR 3.3.1_02 İş Bitirme Formu