1. AMAÇ

Bu doküman, ISO 27001:2022 uyumlu olarak kurulan ve işletilen Bilgi Güvenliği Yönetim Sistemi'nin teknik güvenlik işletiminin tanımlanması amacıyla hazırlanmıştır.

2. KAPSAM

Bu doküman, ISO 27001:2022 BGYS kapsamı dâhilinde olan tüm BİDB iş birimlerini kapsamaktadır.

3. SORUMLULUK

BİDB bu dokümanının tam ve doğru olarak uygulanmasından sorumludur.

3.1 Gözden Geçirme

Bu doküman yılda bir kez periyodik olarak veya gerekli görüldüğü hallerde Bilgi Güvenliği Yöneticisi tarafından gözden geçirilerek güncellenir.

4. TANIMLAR VE KISALTMALAR

İYTE: İzmir Yüksek Teknoloji Enstitüsü

BİDB: Bilgi İşlem Daire Başkanlığı

WYYB: Web Yönetim ve Yazılım Birimi

Müşteri: Akademik/İdari personel ve tüm öğrenciler

5. REFERANSLAR

ISO/IEC 27001:2022 Ek-A Maddeleri

6. UYGULAMA

6.1 Bilgi Sistemleri Geliştirme ve Bakımı

6.1.1 Bilgi Güvenliği İhtiyaçlarının Analiz Edilmesi ve Belirtimi

Geliştirme türü fark etmeksizin aşağıdaki güvenlik ihtiyaçları göz önünde bulundurulur;

- Kimlik doğrulamaya ilişkin ihtiyaçların analizi,
- Uygulamaya ilişkin roller ve sorumlulukların analizi,
- Roller ve sorumluluklara ilişkin tüm yetkilerin analizi,
- Uygulamalar üzerinde hangi seviyede kayıt (log) alınacağının analizi,
- Uygulamalar/varlıkların gizlilik, bütünlük ve erişilebilirlik açısından analizi.

Roller ve sorumlulukların analizi,

- BİDB WYYB içerisinde ilgili yazılımı geliştiren ekipten en az bir kişi sorumlu olarak atanır.
- BİDB WYYB içerisindeki ilgili yazılım sorumlusu değiştiğinde, BİDB birimi EBYS üzerinden ilgili bilgilendirmeyi müşteriye yazı ile yapar.
- Görevlerin ayrılığı prensibine uygun rol ve sorumluluk dağılımı beklenir.

Roller ve sorumluluklara ilişkin tüm yetkilerin analizi,

- Bilgi Güvenliği Yöneticisi tarafından firewall üzerindeki sunucu yönetimi erişim listesi Web Yönetim ve Yazılım Birim Yöneticisine 6 ayda bir gönderilir. Sunucu yönetimi erişim listesi

WYYB Yöneticisi tarafından gözden geçirilip güncel liste Bilgi Güvenliği Yöneticisine gönderilerek kayıt altına alınır.

- WYYB Yöneticisi tarafından uygulamalar üzerindeki erişim yetki listesi 6 ayda bir gözden geçirilir ve WYYB Yöneticisi tarafından kayıt altına alınır.

Uygulamalar üzerinde hangi seviyede kayıt(log) alınacağının analizi,

- Başarılı ve başarısız erişim logları
- Ekle, değiştir ve sil işlemlerine ilişkin loglar

6.1.2 Halka Açık Uygulama Servislerinin Güvenliği

Halka açık sistemlerin güvenliği için aşağıdaki konular göz önünde bulundurulur;

- Gerekli tüm alanlar ve bileşenler için kimlik doğrulama mekanizmalarının ihtiyaç duyulan seviyede uygulanır.
- Halka açık kritik uygulamalardan kimlik doğrulama adımı içeren tüm bileşenler üzerinde trafik şifreli (SSL) olarak iletilir ve tüm iletişim için şifreli (SSL) kanallar kullanılır.
- Veritabanına doğrudan erişim verilmez.
- Halka açık sistemler üzerinde, IP adresi, erişim bilgisi, yapılan istekler loglanır. Sistemler ek log yönetimi ihtiyacı varlık sahibi veya ilgili varlığın sistem yöneticisi tarafından analiz edilir.

6.1.3 Uygulama Servislerinin İletişim Güvenliği (Web Servisleri)

Uygulama servislerinin iletişiminde, uygulamanın hassaslığına göre aşağıdaki konu başlıkları dikkate alınır;

- Kullanıcı kimlik doğrulama bilgilerinin doğru ve geçerli olduğu doğrulanır.
- İletimin/iletişimin güvenilir olduğu doğrulanır ve İletim kanallarının şifreli(SSL) olması sağlanır (kritik bileşenler üzerinde).
- Veritabanı bileşenlerinin doğrudan internete açılmaması sağlanır.
- Kritik uygulamalar üzerinde IP bazlı erişim kısıtlamasının gerekliliği sorgulanır.

6.1.4 Yazılım Geliştirme Ortamı Esasları

- Yazılım geliştirme ortamı olarak Visual Studio, php, Python, ruby kullanılır. Geliştirme ortamlarına erişimler yetkiler dahilinde gerçekleştirilir. Yetkisi olan kullanıcılar kendilerine ait kullanıcı adı ve şifrelerle erişim sağlarlar.
- Geliştirilen yazılımların kaynak kod versiyonları “TFS” ve “Git” üzerinde saklanır.
- SQL Server, MySQL, MariaDB ve PostgreSQL kullanılan veritabanlarıdır.
- Yazılım geliştirme sürecinde güvenli geliştirme ortamına ilişkin, insan, süreç ve teknoloji odak alınarak riskler belirlenir ve önlemler alınır. Bu bağlamda yeni sistem geliştirmeleri yapılırken aşağıdaki konu başlıkları dikkate alınır;
    - Sistem tarafından işlenen, iletilen saklanan verilerin hassaslığı,
    - Yasal ve düzenleyici gereksinimler,
    - Hali hazırda uygulanan güvenlik önlemlerinin durumu,
    - Sistem geliştiriminde ne ölçüde dış kaynak kullanılacağı,
    - Geliştirme ortamına erişim kontrolü,

- Geliştirme ortamındaki değişiklerin izlenmesi
- Yedeklerin güvenli alanlarda saklanması.

- Sistem değişiklikleri ve işletim platformu değişiklikleri; değişiklik ve konfigürasyon yönetimi esaslarına uygun olarak yönetilir.
- İşletim platformu (işletim sistemi, veritabanı vb.) değişikliklerinden sonra sistem güvenlik ve sistem kabul testleri uygulandıktan sonra kullanıma alınır.
- Paket programlarda mümkün olduğunca değişiklik yapılmaz. İstenen değişikliklerin üretici tarafından standart güncellemeler olarak yapılabileceği olasılığı değerlendirilir.
- Değişiklik yapılması gereken durumlarda, orijinal yazılıma dokunulmaz, değişiklikler net şekilde işaretlenmiş bir kopya üzerinden yapılır.

6.1.5 Sistem Güvenlik Testi

Yeni geliştirilen veya güncellenen sistemler/uygulamalar üzerinde testler gerçekleştirilir. Bu testler sistemlerin beklenen şekilde çalıştığının doğrulanması ve güvenlik gereksinimlerinin ne ölçüde sağlandığının anlaşılması için gerçekleştirilir. Geliştirme BİDB bünyesinde gerçekleştiriliyorsa, bu testler iki aşamalı olarak gerçekleştirilir, ilk aşamada geliştirici uygulamayı test eder ikinci aşamada ise yazılım test ekibi testleri gerçekleştirilir. Proje ihtiyaçlarına göre son kullanıcı testleri de gerçekleştirilir. Sistemlerin kritikliğine göre BİDB içinde veya dış kaynak kullanılarak geliştirilen sistemler, bağımsız bir kuruluş tarafından güvenlik testine tabi tutulur.

6.1.6 Sistem Kabul Testi

BİDB bünyesinde sistem kabul testleri için PoC (Proof of Concept) çalışmaları gerçekleştirilir. Bu çalışma sırasında, birlikte çalışabilirlik, işlevsellik ve bilgi güvenliği gereksinim testleri kapsama alınır.

6.1.7 Test Verileri ve Koruma Esasları

Canlı sistemde kullanılan, kullanıcı kimlik bilgileri ya da kişisel bilgilerin test amaçlı kullanımından mümkün olduğunca kaçınılır. Kişisel bilgilerin test amaçlı kullanımı gerekli ise, değişime ve silinmeye karşı korunur.

Operasyonel verilerin test sırasında kullanımda aşağıdaki konu başlıkları göz önünde bulundurulur;

- Canlı sistemde uygulanan erişim kontrol esasları, test ortamında da uygulanır.
- Canlı sistem verilerinin, test ortamına aktarılması için ayrı bir yetkilendirme/kullanıcı hesabı uygulanır.

6.1.8 Yazılım Geliştirme Esasları

BİDB Bünyesinde 2 platformda yazılım geliştirme yapılmaktadır;

- dotNET
- Özgür Yazılım

6.1.9 Yazılım Geliştirme Süreci

6.1.9.1 İstek

a) Birimlerden EBYS ile yazılım talepleri gelir.

b) BİDB Daire Başkanı tarafından kabul süreci başlatılır.

6.1.9.2 Kabul Süreci

a) BİDB Daire Başkanı tarafından personelin iş yüküne göre yazılım ekibi kurar, ön bilgilendirme yaparak görev verir.
b) BİDB Daire Başkanı, ilgili birimle talep edilen yazılım gereksinimi hakkında görüşmek üzere toplantı ayarlar.
c) Yazılım ekibi, talep edilen yazılımın yapılabilirliği ile ilgili kabul raporunu BİDB Daire Başkanına iletir.
d) BİDB Daire Başkanı, kabul raporu sonucuna göre ilgili birimi EBYS üzerinden bilgilendirir.

6.1.9.3 İstek Analizi

a) Müşteri ihtiyaçlarının belirlenmesi
b) Kısıtlamaların belirlenmesi
c) Geliştirilecek olan yazılımın yaşam döngüsünün belirlenmesi
    - Planlama,
    - Analiz,
    - Tasarım,
    - Üretim,
    - Test,
    - Canlı Sisteme Geçiş,
    - Bakım

6.1.9.4 Gereksinim Dokümanı

Sistem tasarımına kaynak olabilmesi için teknik sistem gereksinimlerinin toplanması, müşteri ihtiyaçlarına göre gereksinimlerin belirlenmesi ve sisteme nasıl yansıtılacağının belgelendirilmesidir.

6.1.10 Geliştirme, Test ve Operasyonel Ortamların Ayrımı

Operasyonel ortamdaki yetkisiz erişim ve değiştirmeye ilişkin riskleri azaltmak adına aşağıdaki konu başlıkları gözönünde bulundurulur;

- Geliştirme ortamından canlı ortama geçişler kontrollü yapılır.
- Hassas sistemler için geliştirme ortamı ve canlı ortam donanımları ayrılır. (Operasyonel olarak ayrım yapılamadığı durumlarda test ve canlı ortam aynı donanım üzerinde koşabilir.)
- Operasyonel sistemlerde yapılan değişiklikler canlıya alınmadan önce test edilir.
- Test işlemleri canlı ortamda gerçekleştirilmez. Test işlemlerinin canlı ortamda gerçekleştirilmesi zorunlu (yasa, mevzuat, sözleşme v.b) ise uygulama ve sistemlerin kullanılmadığı veya daha az kullanıldığı zaman dilimlerinde gerçekleştirilir.
- Geliştiriciler, canlı sistemde ve geliştirme ortamında farklı kullanıcı profili kullanırlar.

6.1.11 Görevler Ayrılığı

Yazılım geliştirme kapsamında;

BİDB bünyesinde görevler ayrılığını belirlemek adına geliştirme ve test ekiplerinin ayrılması gerekli olmakla beraber, personel sayısı yeterli olmadığı için yazılım geliştiren kişiler karşılıklı (çapraz) olarak test

ekibi içinde de görev almaktadır. Örneğin X kişisinin geliştirdiği A programını, A programında görev almayan Y kişisi test eder.

Süreç	İlgili Kişi(ler)
Yazılım Geliştirme	Ahmet AKŞİT Bülent YİĞİTALP Subutay Alper ALBAYRAK
Test Senaryosu Geliştirme ve Test Etme	Ahmet AKŞİT Bülent YİĞİTALP Subutay Alper ALBAYRAK
Canlı Sisteme Aktarma	Ahmet AKŞİT Bülent YİĞİTALP Subutay Alper ALBAYRAK

6.2 Bilgi Sistemleri Temini

İYTE bünyesinde dışarıdan sağlanan yazılım temin süreci ile ilgili esaslar aşağıdaki gibi belirlenmiştir. Dışardan sağlanan yazılım temin süreci, üçüncü taraf bilgi güvenliği esaslarına uygun olacak şekilde işletilir. Ek olarak, aşağıdaki konular dikkate alınır;

- Lisans anlaşmaları, kodlara kimin sahip olacağı, fikri mülkiyet haklarına ilişkin çerçevenin belirlenmesi,
- Güvenlik kabul gereksinimlerinin belirlenmesi,
- Güvenlik testlerinin yapıldığına dair kayıt sunma yöntemlerinin belirlenmesi,
- Kaynak koda sahip olunamaması durumunda escrow anlaşmalarının yapılması,
- Dışardan sağlanan yazılım temin anlaşmalarında gizlilik maddelerinin olması.

7. İLGİLİ KAYITLAR