GİRİŞ

1 AMAÇ

Bu politikanın amacı, hukuka, yasal, düzenleyici, ya da sözleşmeye tabi yükümlülüklere, iç ve dış tarafların her türlü Bilgi Güvenliği Yönetim Sistemi gereksinimlerine ilişkin, Bilgi İşlem Daire Başkanı'nın bilgi güvenliği yaklaşımını ve hedeflerini tanımlamak, tüm çalışanlara ve ilgili taraflara bu hedefleri duyurmaktır.
Bilgi Güvenliği Politikası kurumsal bilgi güvenliği ilkelerini ana hatlarıyla belirler. Bilgi Güvenliği Politikası, Bilgi İşlem Daire Başkanlığı'nda bilginin ve işlenme yöntemlerinin güvenli olarak gerçekleştirilmesi amacıyla düzenlemeler yapar.
Bu politika Bilgi Güvenliği Yönetim Sistemi (BGYS) kapsamında bulunan Bilgi İşlem Daire Başkanlığı'nda tüm çalışanları ve bilgi varlıklarını kapsamaktadır.

2 KAPSAM

Bu politika, [ISO/IEC 27001:2022] Bilgi Güvenliği Yönetim Sistemi (BGYS) kapsamında bulunan Bilgi İşlem Daire Başkanlığı'nda tüm çalışanları ve bilgi varlıklarını kapsamaktadır.

3 SORUMLULUK

İYTE Bilgi İşlem Daire Başkanı, Bilgi Güvenliği Politikasının Bilgi İşlem Daire Başkanlığı'nda tüm çalışanlara ve ilgili üçüncü taraflara duyurulmasını sağlar.

3.1 Gözden Geçirme

Bu politika periyodik olarak senede bir defa veya gerekli görülen hallerde Bilgi Güvenliği Yöneticisi tarafından gözden geçirilir.

4 TANIMLAR VE KISALTMALAR

Bilgi Güvenliği Yönetim Sistemi (BGYS): Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır.
Bilgi Varlığı: Kuruluşun sahip olduğu, işlerini aksatmadan yürütebilmesi için gerekli olan dolayısıyla korumakla yükümlü olduğu varlıklardır.
İYTE: İzmir Yüksek Teknoloji Enstitüsü
BİDB: Bilgi İşlem Daire Başkanlığı
Müşteri: Akademik/İdari personel ve tüm öğrenciler

5 REFERANSLAR

[ISO/IEC 27001:2022] Madde 5.2 : Politika

6 UYGULAMA

6.1 Bilgi İşlem Daire Başkanı Taahhüdü

İzmir Yüksek Teknoloji Enstitüsü Bilgi İşlem Daire Başkanı bilgi güvenliğinin gerçekleştirilmesi, işletimi, izlenmesi, gözden geçirilmesi, bakımı ve iyileştirilmesi için gerekenin yapılacağını taahhüt eder.

BİDB bilgi güvenliği yönetimi ile ilgili olarak aşağıdaki ilkeleri benimsemektedir;

- Müşterilerine ve paydaşlarına sunduğu ürün ve hizmetlere ilişkin faaliyetlerinin güvenliğinin sağlanmasına önem vermektedir.
- Tüm iş süreçlerinin birbiri ile entegre, uyumlu ve dengeli olması hedeflenmektedir. Entegre ve dinamik iş stratejisi bilgi varlıklarının güvenliğini ve sürekliliğini gerekli kılmaktadır.
- Müşterileri ve paydaşlarına değer sağlayan ürün ve hizmetlerinin gizlilik, bütünlük ve erişilebilirliğini tehdit edebilecek risklere karşı tedbir almayı ilke edinir.
- Bu politika ve organizasyonun amacı ile uyumlu bilgi güvenliği hedefleri belirlenir ve düzenli aralıklarla uyumluluk ölçülerek, sürekli iyileştirme fırsatları değerlendirilir.

6.2 Bilgi Güvenliği Politikası

Bilgi güvenliği, bilgi varlıklarının gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması ile mümkündür.
Bilginin;

- Gizlilik gerekliliği, bilginin sadece yetkili kişiler tarafından erişilebilir olmasını,
- Bütünlük gerekliliği, bilgi varlıklarının tam ve doğruluğunun sağlanmasını, yetkisiz değişimlerden korunmasını,
- Erişilebilirlik gerekliliği, bilgi varlıklarının ihtiyaç duyulduğu anda yetkili kullanıcılar tarafından kullanılabilir olmasını ifade eder.

BİDB bilgi güvenliğini sağlamak amacıyla kendi kurumsal işleyişini düzenleyici prensipler oluşturur. Bilgi Güvenliği Politikası'nın belirlenmesi, güvenlik rollerinin tanımlanması ve ilgili tüm güncellemelerin yapılması Bilgi İşlem Daire Başkanı'nın desteği ve tüm BİDB alt birimlerinin koordinasyonuyla gerçekleştirilir. BİDB gerekli durumlarda iç ve dış uzmanların görüşüne başvurabilir.
BİDB'de bilgi varlıkları uygun şekilde sınıflandırılır. Varlıkların değerlemesi yapılır ve uygun seviyede kontrol geliştirmek için varlıkların değeri hesaplanır.

6.3 Bilgi Güvenliği Amaçları

BİDB yukarıda belirtilen ilkelerden taviz vermeden bilgi güvenliği çalışmalarını aşağıda belirtilen amaçlarla gerçekleştirmeyi hedefler;

- Bilgi Güvenliği Yönetim Sistemi (BGYS), uluslararası olarak kabul edilmiş olan [ISO/IEC 27001: 2022] Bilgi Güvenliği Yönetim Sistemi standardı şartları doğrultusunda planlanır, gerçekleştirilir ve geliştirilir,
- İlgili kanun ve yönetmeliklere uyumlu hale gelinmesi için gereken çalışmalar yapılır,
- BGYS'nin sürekli iyileştirilmesi için gerekli iç denetim, yönetimin gözden geçirmesi, düzeltici faaliyetler ile risklerin ve fırsatların belirlenmesi için gerekli aksiyonlar yönetim ve yönetimin bilgi güvenliği sorumluluğu verdiği ekipler tarafından sağlanır,
- Bilgi güvenliği ile ilgili tüm rol ve sorumluluklar belirlenir ve yönetim tarafından yetkilendirmeler yapılır,
- Bilgi güvenliği yönetim sistemi çerçevesinde gerekli çalışmaların gerçekleştirilmesi için kaynaklar yönetim tarafından sağlanır,

- Paydaşları ile birlikte kuruluşun rekabet avantajını olumsuz yönde etkileyebilecek maddi ve manevi kayıplar engellenir,
- Bilgi Güvenliği Yönetim Sistemi kapsamı bilgi varlıkları belirlenerek, müşteriler, tedarikçiler ve iş ortakları gibi ilgili tarafların bilgi güvenliği beklentileri değerlendirilerek, varsa yasal ve sözleşmeler yükümlülükler analiz edilerek yönetim tarafından iş stratejileri doğrultusunda belirlenir,
- Bilgi varlıklarının sınıflandırılması ve bu varlıkların gizlilik, bütünlük ve erişilebilirlik değerlendirmesinin yapılabilmesi için varlık envanteri oluşturulur,
- Bilgi güvenliği risklerini yönetmek için risklerini değerlendirme, risk analizi ve risk işleme çalışmaları gerçekleştirilerek, gerekli tedbirler geliştirilir ve olası riskleri önlemek için çalışmalar gerçekleştirilir,
- Bu politika ve organizasyonun amacı ile uyumlu bilgi güvenliği hedefleri belirlenir ve düzenli aralıklarla uyumluluk ölçülerek, sürekli iyileştirme fırsatları değerlendirilir,
- Halka açık sistemlerin sürekli erişilebilirliği sağlanır,
- Çalışan özlük bilgilerinin mahremiyeti sağlanır,
- Müşterilere ait tüm bilgilerin mahremiyetinin sağlanması,
- Veri bütünlüğü sağlanır,
- Erişim kayıtlarını tutarak suç niteliğinde olabilecek erişimlerin delilleri yasal otoritelere sağlanır,
- Tedarikçi nezdinde bilgi güvenliği sağlanır,
- Operasyonel Kazanılmış Bilgilerin sürekli geliştirilmesi ve korunması sağlanır,
- Son kullanıcı bilgi güvenliği farkındalığını ve bu farkındalığın sürekli arttırılması sağlanır,
- Bilgi güvenliğini etkin biçimde yöneterek bilgi güvenliği kaynaklı yaşanabilecek zararlar asgariye indirilir,
- Bilgi güvenliği ihlal olayı yaşama ihtimalini düşürmek için gerekli çalışmalar yapılır, yaşanması durumunda koordineli şekilde yanıt verilir,
- Kritik iş süreçlerinde yaşanabilecek kesintilerin önüne geçilmesi için gerekli düzenlemeler yapılır, geçilemediği durumda hedeflenen kurtarma süresi içerisinde tekrar çalışabilir hale gelmesi sağlanır,
- Bilgi Güvenliği Yönetim Sistemi kapsamında müşterilerimizin bilgi varlıklarının gizliliği, bütünlüğü ve erişebilirliği sağlanır.
- Bilgi Güvenliği Yönetim Sistemi'nin sürekli iyileştirilmesi sağlanır,
- Bilgi İşlem Daire Başkanlığı'nda istihdam öncesinde, sırasında ve sonrasında insan kaynakları güvenliğini sağlama açısından kuralların belirlendiği süreçler oluşturulur.
- Güvenli çalışma alanları, arşiv odaları, sistem odaları gibi kurum içi çalışma bölgelerinde ve kurum çevresinde güvenliğin sağlanması için gerekli önlemlerin alınması sağlanır.
- Tedarikçi ilişkilerinin güvenli bir şekilde yürütülmesi amacıyla; tedarik hizmetlerinin gözden geçirilmesi, meydana gelen değişikliklerin yönetilmesi için politikalar oluşturulur, özellikle bilgi teknolojileri tedarikçileri ile yapılan/yapılacak olan ve bilgi güvenliği risklerinin ifade edildiği anlaşmalarda güvenlik gereksinimleri belirlenir.

6.4 Bilgi Güvenliği Hedefleri

BGYS amaçları kapsamında belirlenen ölçülebilir hedefler, Bilgi Güvenliği Performans Değerlendirme Formu aracılığı ile belirlenir, Performans Değerlendirme ve Sürekli İyileştirme Prosedürü'nde anlatıldığı gibi değerlendirilir ve izlenir.

7 İLGİLİ KAYITLAR

- Performans Değerlendirme ve Sürekli İyileştirme Prosedürü
- BGYS Hedef Formu
- İş Sürekliliği Planı