1.0 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

1.1 Amaç

Bu politikanın amacı, hukuka, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklere ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemek için, üst yönetiminin yaklaşımını ve hedeflerini tanımlamak, tüm çalışanlara ve ilgili taraflara bu hedefleri bildirmektir.

1.2 Kapsam

TRAKYA ÜNİVERSİTESİ BİLGİ İŞLEM DAİRE BAŞKANLIĞI YETKİ VE GÖREV ALANINDA BULUNAN BİLİŞİM SİSTEMLERİNİN, NETWORK VE SİSTEM ALT YAPILARININ PLANLANMASI, KURULUMLARI, YÖNETİLMESİ VE GEREKLİ DONANIM VE YAZILIMLARIN SATIN ALINMASI, KURULU SİSTEMLERİN BİLGİLERİN GÜVENLİĞİNİN SAĞLANMASI, İLETİŞİM VE İNTERNET ALT YAPISI YENİLİKLERİNİN UYGULANMASI ÜNİVERSİTE VE BİLİŞİM PERSONELLERİNE GEREKLİ EĞİTİMLERİN VERİLMESİ, AKADEMİK ÇALIŞMALARA VE EĞİTİM ÇALIŞMALARINA EN YÜKSEK DÜZEYDE KATKININ SAĞLANMASI

1.2.1 İç Kapsam

İdare, kuruluşa ilişkin yapı, roller ve yükümlülükler;

Trakya Üniversitesi bünyesinde bulunan Bilgi İşlem Dairesi Başkanlığını kapsar.

Genel Yönetim Organizasyon Şemasında belirtilmiş roller ve görev tanımlarındaki sorumluluklar.

Yerine getirilecek politikalar, hedefler ve stratejiler;

- BGYS Politikaları,
- Yönetimce belirlenmiş yıllık BGYS hedefleri,
- Kaynaklar ve bilgi birikimi cinsinden anlaşılan yetenekler (örneğin, anapara, zaman, kişiler, süreçler, sistemler ve teknolojiler),
- Bilgi Güvenliği Yönetim Sisteminin kurulması, işletilmesi ve sürdürülmesi için Bilgi İşlem Daire Başkanlığı tarafından atanan Yönetim Temsilcileri ve BGYS ekibi,
- İç paydaşlarla ilişkiler ve onların algılamaları ve değerleri, kuruluşun kültürü, kuruluş tarafından uyarlanan standartlar, kılavuzlar ve modeller, sözleşmeye ilişkin ilişkilerin; biçim ve genişliğini kapsamaktadır.
- İç Paydaşlar ;
  - Akademik Personel
  - İdari Personel
  - Öğrenciler

1.2.2 Dış Kapsam

- Uluslararası, ulusal, bölgesel veya yerel olmak üzere, sosyal ve kültürel, politik, yasal, mevzuata ilişkin, finansal, teknolojik, ekonomik ortam,
- Tedarikçi ve paydaşların verilerinin gizliliği,
- Kalite Odaklılık,
- Kuruluşun hedefleri üzerinde etkisi bulunan paydaşlarla ilişkiler ve onların algılamaları ve değerleri;,
- Üst Yönetim dahil tüm Trakya Üniversitesi çalışanları,
- İlgili tüm yasal mevzuat, düzenleyici, sözleşmeden doğan şartlar, standartlar,
- Trakya Üniversitesi Teşkilat ve Görevleri Hakkında 656 Sayılı KHK Çerçevesinde İlgili diğer Kamu Kurum ve Kuruluşları.
- Dış Paydaşlar ;
  - YÖK
  - Kamu İhale Kurumu
  - Kredi Yurtlar Kurumu
  - ÖSYM
  - Bilim ve Teknoloji Yüksek Kurulu
  - TÜBİTAK – ULAKBİM
  - Mezunlar

1.3 Tanımlar

BGYS: Bilgi Güvenliği Yönetim Sistemi.

Envanter: Kurum için önemli olan her türlü bilgi varlığı.

Üst Yönetim: Trakya Üniversitesi; Rektörlüğü ve Genel Sekreterliği.

Birim/Bölüm Yöneticisi: Trakya Üniversitesi; Daire Başkanı ve Şube Müdürleri.

Gizlilik: Bilginin içeriğinin görüntülenmesinin, sadece bilgiyi/veriyi görüntülemeye izin verilen kişilerin erişimi ile kısıtlanmasıdır. (Ör: Şifreli e-posta gönderimi ile e-postanın ele geçmesi halinde dahi yetkisiz kişilerin e-postaları okuması engellenebilir)

Bütünlük: Bilginin yetkisiz veya yanlışlıkla değiştirilmesinin, silinmesinin veya eklemeler çıkarmalar yapılmasının tespit edilebilmesi ve tespit edilebilirliğin garanti altına alınmasıdır. (Ör: Veri tabanında saklanan verilerin özet bilgileri ile birlikte saklanması, dijital imza)

Erişilebilirlik/Kullanılabilirlik: Varlığın ihtiyaç duyulduğu her an kullanıma hazır olmasıdır.
Diğer bir ifadeyle, sistemlerin sürekli hizmet verebilir halde bulunması ve sistemlerdeki bilginin kaybolmaması ve sürekli erişilebilir olmasıdır. (Ör: Sunucuların güç hattı dalgalanmalarından ve güç kesintilerinden etkilenmemesi için kesintisiz güç kaynağı ve şasilerinde yedekli güç kaynağı kullanımı). Bu dokümanda "Erişilebilirlik" olarak kullanılacaktır.

Bilgi Varlığı: İlgili kurum / birim ve ilgili paydaşları için kurumsal süreçlerinde bir değer ifade eden ve bu nedenle uygun şekilde korunması gereken bir varlıktır.
Bilgi varlığı; Trakya Üniversitesi'nin yürüttüğü hizmet süreçlerini sürdürebilmesi için önemli olan varlıklardır. Bu politikaya konu olan süreçler ve paydaşlar kapsamında bilgi varlıkları şunlardır:

- Yazılı/basılı, görsel, işitsel veya elektronik ortamda sunulan her türlü bilgi ve veri,
- Bilgiye erişmek ve bilgiyi değiştirmek için kullanılan her türlü yazılım ve donanım,
- Bilginin transfer edilmesini sağlayan ağlar,
- İlgili bölüm/birimlerin çalışanları,

1.4 Sorumluluklar

Sorumluluk ve yetkileri belirlenmiş görevlerin nitelik ve yeterlilikleri görev tanımlarında tanımlanmıştır. Bilgi güvenliği ile ilgili faaliyetlerin sürdürülmesinden ve geliştirilmesinden Bilgi Güvenliği Yönetim Sistemi Ekibi sorumludur. BGYS Ekibi ve Yönetim Temsilcileri Üst Yönetim tarafından atanmıştır.

1.4.1 Yönetim Sorumluluğu

Trakya Üniversitesi Üst Yönetimi, tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan Bilgi Güvenliği Sistemine uyacağını ve sistemin verimli şekilde çalışması için gerekli kaynakları (bütçe sağlamayı, uzman personel, donanım ve yazılım vb.) tahsis edeceğini, sistemin tüm çalışanlar tarafından anlaşılmasını sağlayacağını taahhüt eder.

Üst Yönetim kademesinde bulunan yöneticiler ve üst yönetimin gerekli gördüğü diğer yöneticiler BGYS' nin kurulumu, uygulanması, sürdürülebilirliği açısından alt kademelerde bulunan personele yardımcı olurlar ve yazılı ya da sözlü olarak güvenlik talimatlarına uyarlar, ihtiyaç duyulduğunda çalışmalara katılırlar.

1.4.2 Yönetim Temsilcisi Sorumluluğu

- BGYS (Bilgi Güvenliği Yönetim Sistemi)'nin planlanması, kabul edilebilir risk seviyesinin belirlenmesi, risk değerlendirme metodolojisinin belirlenmesi,
- BGYS kurulumunda destekleyici ve tamamlayıcı faaliyetler için gerekli kaynakların sağlanması, kullanıcı kabiliyetlerinin sağlanması/iyileştirilmesi ve farkındalığın oluşması, eğitimlerin yapılması, iletişimin sağlanması, dokümantasyon gereksinimlerinin sağlanması,
- BGYS uygulamalarının yürütülmesi ve yönetilmesi, değerlendirmelerin, iyileştirmelerin ve risk değerlendirmelerinin sürekliliğinin sağlanması,
- İç denetimler, hedeflerin ve yönetim gözden geçirme toplantıları ile BGYS ve kontrollerin değerlendirilmesi,
- BGYS'de mevcut yapının sürdürülmesi ve sürekli iyileştirmelerin sağlanmasından sorumludur.

1.4.3 BGYS Ekip Üyeleri Sorumluluğu

- Birim/Bölümleri ile ilgili varlık envanteri ve risk analiz çalışmalarının yapılması,
- Sorumluluğu altında bulunan bilgi varlıklarında bilgi güvenliği risklerini etkileyecek bir değişiklik olduğunda, risk değerlendirmesi yapılması için Yönetim Temsilcisini bilgilendirmesi,
- Birim/bölüm çalışanlarının politika ve prosedürlere uygun çalışmasının sağlanması,
- Birim/Bölümleri ile ilgili BGYS kapsamında farkındalığın oluşması, iletişimin sağlanması, dokümantasyon ihtiyaçlarının belirlenmesi,
- BGYS' de mevcut yapının sürdürülmesi ve sürekli iyileştirilmesinden sorumludur.

1.4.4 İç Denetçi Sorumluluğu

İç denetim planı doğrultusunda, görev verilen iç denetimlerde denetim faaliyetlerinin yapılmasından ve raporlanmasından sorumludur.

1.4.5 Birim/Bölüm Yöneticileri Sorumluluğu

Bilgi Güvenliği Politikasının uygulanması ile çalışanların esaslara uyumunun ve 3. tarafların politikadan haberdar olmalarının sağlanmasının fark ettiği bilgi sistemleri ile ilgili güvenlik ihlal olaylarının bildirilmesinden sorumludurlar.

1.4.6 Tüm Çalışanların Sorumluluğu

- Çalışmalarını bilgi güvenliği hedeflerine, politikalarına ve bilgi güvenliği yönetim sistemi dokümanlarına uygun olarak yürütmekten,

- Kendi birimi ile ilgili bilgi güvenliği hedeflerinin takibini yapar ve hedeflere ulaşılmasını sağlar.
- Sistemler veya hizmetlerde gözlenen veya şüphelenilen herhangi bir bilgi güvenliği açıklığına dikkat etmek ve raporlamaktan,
- Üçüncü taraflar ile yapılan hizmet sözleşmelerine (danışmanlık vb.) ilave olarak gizlilik sözleşmesi yapmak ve bilgi güvenliği gereksinimlerini sağlamaktan sorumludur.

1.4.7 Üçüncü Tarafların Sorumluluğu

Bilgi güvenliği politikasının bilinmesi ve uygulanması ile BGYS kapsamında belirlenen davranışlara uyulmasından sorumludur.

1.5 Bilgi Güvenliği Hedefleri

Bilgi Güvenliği Politikası, Trakya Üniversitesi çalışanlarına kurumun güvenlik gereksinimlerine uygun şekilde hareket etmesi konusunda yol göstermek, bilinç ve farkındalık seviyelerini arttırmak ve bu şekilde kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak, güvenilirliğini ve imajını korumak ve üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunlukları sağlamak amacıyla kurumun tüm işleyişini etkileyen fiziksel ve elektronik bilgi varlıklarının korunmasını hedefler. Yönetim Tarafından belirlenen hedefler belirlenmiş periyodlarda izlenir ve YGG toplantılarında gözden geçirilir.

1.6 Risk Yönetim Çerçevesi

Kurumun risk yönetim çerçevesi; Bilgi güvenliği risklerinin tanımlanmasını, değerlendirilmesini ve işlenmesini kapsar. Risk Analizi, uygulanabilirlik bildirgesi ve risk işleme planı, bilgi güvenliği risklerinin nasıl kontrol edildiğini tanımlar. Risk işleme planının yönetiminden ve gerçekleştirilmesinden BGYS Yürütme Komitesi sorumludur. Tüm bu çalışmalar, varlık envanteri ve risk değerlendirme talimatında detaylı olarak anlatılmaktadır.

1.7 Bilgi Güvenliği Genel Esasları

a) Bu politika ile çerçevesi çizilen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar, Trakya Üniversitesi çalışanları ve 3. taraflar bu politikaları bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdür.

b) Bu kural ve politikalar, aksi belirtilmedikçe, basılı veya elektronik ortamda depolanan ve işlenen tüm bilgiler ile bütün bilgi sistemlerinin kullanımı için dikkate alınması esastır.

c) Bilgi Güvenliği Yönetim Sistemi, TS ISO/IEC 27001 "Bilgi Teknolojisi Güvenlik Teknikleri (Information Technology Security Techniques) ve Bilgi Güvenliği Yönetim Sistemleri

Gereksinimler (Information Security Management Systems Requirements)" standardını temel alarak yapılandırılır ve işletilir.

d) BGYS'nin hayata geçirilmesi, işletilmesi ve iyileştirilmesi çalışmalarını, ilgili tarafların katkısıyla yürütür. BGYS dokümanlarının gerektiği zamanlarda güncellenmesi BGYS Yönetim Temsilcisi sorumluluğundadır.

e) Kurum tarafından çalışanlara veya 3. taraflara sunulan bilgi sistemleri ve altyapısı ile bu sistemler kullanılarak üretilen her türlü bilgi, belge ve ürün aksini gerektiren kanun hükümleri veya sözleşmeler bulunmadıkça kuruma aittir.

f) Çalışanlar, danışmanlık, hizmet alımı Tedarikçi ve Stajyer ile gizlilik anlaşmaları yapılır.

g) İşe alım, görev değişikliği ve işten ayrılma süreçlerinde uygulanacak bilgi güvenliği kontrolleri belirlenir ve uygulanır.

h) Çalışanların bilgi güvenliği farkındalığını artıracak ve sistemin işleyişine katkıda bulunmasını sağlayacak eğitimler düzenli olarak mevcut kurum çalışanlarına ve yeni işe başlayan çalışanlara verilir.

i) Bilgi güvenliğinin gerçek ya da şüpheli tüm ihlalleri rapor edilir; ihlallere sebep olan uygunsuzluklar tespit edilir, ana sebepleri bulunarak tekrar edilmesini engelleyici önlemler alınır.

j) Bilgi varlıklarının envanteri bilgi güvenliği yönetim ihtiyaçları doğrultusunda oluşturulur ve varlık sahiplikleri atanır.

k) Kurumsal veriler sınıflandırılır ve her sınıftaki verilerin güvenlik ihtiyaçları ve kullanım kuralları belirlenir.

l) Güvenli alanlarda saklanan varlıkların ihtiyaçlarına paralel fiziksel güvenlik kontrolleri uygulanır.

m) Kuruma ait bilgi varlıkları için kurum içinde ve dışında maruz kalabilecekleri fiziksel tehditlere karşı gerekli kontrol ve politikalar geliştirilir ve uygulanır.

n) Kapasite yönetimi, üçüncü taraflarla ilişkiler, yedekleme, sistem kabulü ve diğer güvenlik süreçlerine ilişkin prosedür ve talimatlar geliştirilir ve uygulanır.

o) Ağ cihazları, işletim sistemleri, sunucular ve uygulamalar için denetim kaydı üretme konfigürasyonları ilgili sistemlerin güvenlik ihtiyaçlarına paralel biçimde ayarlanır. Denetim kayıtlarının yetkisiz erişime karşı korunması sağlanır.

p) Erişim hakları ihtiyaç nispetinde atanır. Erişim kontrolü için mümkün olan en güvenli teknoloji ve teknikler kullanılır.

q) Sistem temini ve geliştirilmesinde güvenlik gereksinimleri belirlenir, sistem kabulü veya testlerinde güvenlik gereksinimlerinin karşılanıp karşılanmadığı kontrol edilir.

r) Kritik altyapı için süreklilik planları hazırlanır, bakımı ve tatbikatı yapılır.

s) Yasalara, iç politika ve prosedürlere, teknik güvenlik standartlarına uyum için gerekli süreçler tasarlanır, sürekli ve periyodik olarak yapılacak gözetim ve denetim faaliyetleri ile uyum güvencesi sağlanır.

1.8 Politikanın İhlali ve Yaptırımlar

Trakya Üniversitesi Bilgi Güvenliği Politikasına ve Standartlarına uyulmadığının tespit edilmesi durumunda, bu ihlalden sorumlu olan çalışanlar için İlgili Mevzuata göre, 3. Taraflar için de geçerli olan sözleşmelerde geçen ilgili maddelerinde belirlenen yaptırımlar uygulanır.

1.9 Yönetimin Gözden Geçirmesi

Yönetim gözden geçirme toplantıları BGYS Yönetim Temsilcisi Organize edilerek, Üst Yönetim ve Birim/Bölüm yöneticileri katılımı ile gerçekleştirilir. Bilgi Güvenliği Yönetim Sisteminin uygunluğunun ve etkinliğinin değerlendirildiği bu toplantılar en az yılda bir kez gerçekleştirilmektedir.

1.10 Bilgi Güvenliği Politika Dokümanı Güncellenmesi ve Gözdem Geçirilmesi

Politika dokümanının sürekliliğinin sağlanmasından ve gözden geçirilmesinden BGYS Yönetim Temsilcileri sorumludur.

Doküman, en az yılda bir kez gözden geçirilmelidir. Bunun dışında sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra da gözden geçirilmeli ve herhangi bir değişiklik gerekiyorsa üst yönetime onaylatılarak yeni versiyon olarak kayıt altına alınmalıdır. Her revizyon tüm kullanıcıların erişebileceği şekilde yayınlanmalıdır.