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

Üniversitemizin akademik eğitim, öğretim faaliyetleri ile idari faaliyetlerini ve bu faaliyetlerine ilişkin bilgi varlıklarını, bu varlıkların korunması amacıyla yürüttüğü bilgi güvenliği kapsamındaki ilgili iş süreçlerini kapsar.

İngilizce:
It includes the related working processes within the scope of information security that the university conducts to secure academic education-training activities and administrative activities together with the information entities regarding these activities and these entities at all.

1.2.1 İç Kapsam

İdare, kuruluşa ilişkin yapı, roller ve yükümlülükler;

Erzurum Teknik Üniversitesi bünyesinde bulunan Bilgi İşlem Daire 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 ETÜ Yönetimi 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 Erzurum Teknik Üniversitesi çalışanları,
- İlgili tüm yasal mevzuat, düzenleyici, sözleşmeden doğan şartlar, standartlar,
- Erzurum Teknik 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

1.2.3 İLGİLİ TARAFLARIN İHTİYAÇ VE BEKLENTİLERİNİN ANLAŞILMASI

Erzurum Teknik Üniversitesi, öğrenci ile yaptığı sözleşme/teklif üzerinde belirttiği şartları, teklifte/sözleşmesinde belirtilmeyen ancak hizmet için gerekli olan şartları, yasal ve yasal olmayan bütün şartları ve kendisi tarafından belirlenen her türlü ek şartları bir araya getirerek hizmet şartlarını oluşturmuştur. Öğrenciye sunulacak hizmetler için belirlenen tüm şartları tamamen karşılar.

Tedarikçilerle ilgili hizmetlerin detayları hizmet sözleşmeleri ile belirlenir.

İlgili Taraf (İç)	Beklentiler
Kurumun Tüzel Kişiliği	- Prestijin korunması, - Elde edilen bilgi birikiminin korunması, - Tüm tarafların güvenli çalışması.
Kurucu Vakıf	- Karlılık ve kuruluşun pazar değerinde artış, - Yasal ve sözleşmelerden doğan gereksinimlerin yerine getirilmesi, - Kurum sırlarının korunması, - Öğrenci memnuniyetinin sağlanması.

	- Sosyal bilimler alanında söz sahibi, özgün bilgi ve yaklaşımlar üreten, küresel ölçekte saygın ve etkili bir üniversite olmasını.
Kurum Personeli	- BGYS farkındalığı yaratılmış uygun çalışma koşulları, iş güvenliği, emniyet, sağlık, terfi, takdir, motivasyon, ödüllendirme, - Kişisel verilerinin korunması, - Kurumun çalışanlarla ilgili sorumluluklarını yerine getirmesi.

Tedarikçiler	- Ürün ve hizmetlerin eksiksiz zamanında temin etmesi, uzun süreli temin sözleşmesi, - Ürün servis için geri besleme, - Kendilerine emanet edilen kurumsal verilerin korunması.
Otoriteler	- Lisans, ruhsat, belge, sözleşme, yasa ve yönetmeliklere uyum sağlanması, - Bilgi güvenliğinin korunması, - Güncel yasa ve kanunlara uyum, - Değişikliklerin izlenmesi ve uygulanması.
Öğrenciler	- Kaliteli Hizmet Sunulması, - Kesintisiz hizmet, - Kuruma emanet edilen bilgilerin gizlilik, bütünlük ve erişebilirlik kriterleri doğrultusunda korunması, - Kişisel Verilerin Korunmasının Sağlanması.
Finansal Kuruluşlar	- İyi finansal performans, - İş hacminin artması, - Çalışma koşullarının BGYS'e göre belirlenmesi.
Denetçi Kuruluş /Denetmenler	- İlgili tarafların şirketin sahip olduğu standartlara göre uyumlu ve gerektiği gibi çalıştığını görmeyi.
Diğer Üniversiteler	- Birlikte yürütülen ortak projelerde iş birliğinin koruması.
Çevre,Şehircilik ve İklim Değişikliği Bakanlığı	- Sistem odalarında enerji tüketimini en aza indirecek, yüksek verimlilikte enerji kullanımını sağlayacak soğutma ve güç yönetimi sistemlerinin kullanılmasını bekler. - Enerji verimliliğini arttıracak teknolojilerin ve uygulamaların kullanılmasını bekler. - Çevre dostu, düşük enerji tüketen ve daha az ısınan donanım ve ekipmanların tercih edilmesini bekler. - Geri dönüşümü olmayan donanımların azaltılmasını bekler. - Enerji santralinde (elektrik, su, doğalgaz) daha az tüketilmesini bekler.

	- Daha fazla geri dönüştürülebilir malzeme kullanılmasını bekler. - Kağıt kullanımının azaltılması ve sıfır baskı hedefiyle dokümanların /kayıtların elektronik ortamda tutulmasını bekler. - Sistem odasının ısıtılması veya soğutulmasında yenilebilir enerji kullanılmasını bekler. - Yenilebilir enerji kullanımının arttırılmasını bekler. - Su kullanımının azaltılmasını bekler. - Klimalarda enerji sınıfı yüksek, verimli klimalar kullanılmasını bekler. - Karbon salınımının azaltılmasını bekler.

1.3 Tanımlar

BGYS: Bilgi Güvenliği Yönetim Sistemi.

Envanter: Kurum için önemli olan her türlü bilgi varlığı.

Üst Yönetim: Erzurum Teknik Üniversitesi; Rektörlüğü ve Genel Sekreterliği.

Birim/Bölüm Yöneticisi: Erzurum Teknik 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; Erzurum Teknik 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

Erzurum Teknik 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, Erzurum Teknik 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, Erzurum Teknik 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.

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

d) 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.

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

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

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

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

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

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

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

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

k) Kapasite yönetimi, üçüncü taraflarla ilişkiler, yedekleme, sistem kabulü ve diğer güvenlik süreçlerine ilişkin prosedür ve talimatlar geliştirilir ve uygulanır.
l) 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.
m) Erişim hakları ihtiyaç nispetinde atanır. Erişim kontrolü için mümkün olan en güvenli teknoloji ve teknikler kullanılır.
n) Sistem temini ve geliştirilmesinde güvenlik gereksinimleri belirlenir, sistem kabulü veya testlerinde güvenlik gereksinimlerinin karşılanıp karşılanmadığı kontrol edilir.
o) Kritik altyapı için süreklilik planları hazırlanır, bakımı ve tatbikatı yapılır.
ö) 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

Erzurum Teknik 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 Gözden 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.

2.0 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKA LİSTESİ

Erzurum Teknik Üniversitesi BGYS politikaları listesi aşağıdaki gibidir.

P01 BİLGİ SİSTEMLERİ GENEL KULLANIM POLİTİKASI

P02 PERSONEL GÜVENLİĞİ POLİTİKASI
P03 İNTERNET ERİŞİM POLİTİKASI
P04 E-POSTA POLİTİKASI
P05 ANTİ-VİRÜS POLİTİKASI
P06 ŞİFRE POLİTİKASI
P07 KABLOSUZ İLETİŞİM POLİTİKASI
P08 UZAKTAN ERİŞİM POLİTİKASI
P09 KRİZ / ACİL DURUM YÖNETİMİ POLİTİKASI
P10 FİZİKSEL GÜVENLİK POLİTİKASI
P11 SUNUCU GÜVENLİK POLİTİKASI
P12 AĞ CİHAZLARI GÜVENLİK POLİTİKASI
P13 AĞ YÖNETİMİ POLİTİKASI
P14 VERİTABANI GÜVENLİK POLİTİKASI
P15 DEĞİŞİM YÖNETİMİ POLİTİKASI
P16 GÜVENLİK AÇIKLARI TESPİT ETME POLİTİKASI
P17 SANAL ÖZEL AĞ (VPN) POLİTİKASI
P18 KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI
P19 BİLGİ SİSTEMLERİ YEDEKLEME POLİTİKASI
P20 YAZILIM GELİŞTİRME
P21 KABUL EDİLEBİLİR KULLANIM POLİTİKASI
P22 ORTAMIN ELDEN ÇIKARILMASI POLİTİKASI
P23 TEÇHİZATIN ELDEN ÇIKARILMASI POLİTİKASI
P24 TEMİZ MASA TEMİZ EKRAN POLİTİKASI
P25 KRİPTOGRAFİK KONTROLLER POLİTİKASI
P26 ZİYARETÇİ KABUL POLİTİKASI
P27 TAŞINABİLİR CİHAZ POLİTİKASI
P28 BİLGİ VE YAZILIM ALIŞVERİŞİ POLİTİKASI
P29 ÜÇÜNCÜ TARAF GÜVENLİK POLİTİKASI
P30 VARLIKLARA YÖNELİK SORUMLULUK POLİTİKASI
P31 BASILI ÇIKTI VE DAĞITIM POLİTİKASI
P32 BİLGİ SINIFLANDIRMA POLİTİKASI
P33 OLAY İHLAL BİLDİRİM VE YÖNETİM POLİTİKASI
P34 BULUT BİLİŞİM POLİTİKASI
P35 GÜVENLİ KODLAMA POLİTİKASI

2.1 Tanımlar

Ağ: (Network**)** Bilgisayarların iletişim hatları aracılığıyla veri aktarımının sağlandığı sistem, bilgisayar ağıdır.

Alfanümerik: Latin alfabesindeki harfleri (A-Z, a-z) ve Arap rakamlarını (0-9) kullanan karakter dizisini tanımlamakta kullanılan bir sıfattır.

Antivirüs Programı: Bilgisayarın zararlı programlardan korunması için hazırlanan güvenlik yazılımdır.

Bayt: (Byte) Elektronik ve bilgisayar bilimlerinde genellikle 8 bitlik dizilim boyunca 1 veya 0 değerlerini bünyesine alan ve kaydedilen bilgilerin türünden bağımsız bir bellek ölçüm birimidir.

Bit: Bilgi sistemlerinde kullanılan en küçük bilgi birimidir. Yani programlama ve haberleşmede, bir bit bilgi depolama ve haberleşme veya bağlantının en küçük ve temel ünitesidir.

BIOS: (Basic input output system) İşletim sistemi ile donanım arasındaki bütün bağımsız sürücü programlarını yönetir. Diğer bir deyişle Anakart'ın (Bilgisayar merkezi kartı) birçok özelliğini kullanmamıza olanak sağlayan yazılım, sistem ve donanımlarımız arasında bağlantı kurar.

BGYS: Bilgi Güvenliği Yönetim Sistemi

Cihaz: Bilgi işleme ve depolama amaçlı kullanılan PC (kişi tahsis edilen bilgisayar), laptop, cep telefonu, sunucu, veri depolama cihazı (storage), el terminali ve yazıcılardır.

DDOS Atağı: (Distributed Denial of Service Attack), çoklu sistemlerde hedef sistemin kaynakları ya da bant genişliği istilaya uğradığı zaman oluşur, bunlar genellikle bir veya birden fazla web sunucusudur. Bu sistemler saldırganlar tarafından çeşitli yöntemler kullanılarak bağdaştırılır.

Dizin: (Indeks) Excel, Word dosyaları gibi bilgi kaynaklarının içindeki bilgi parçacıklarına ulaşmak için konu başlık, yer adları kişi adları gibi erişim uçlarına ulaşmak için kullanılan ayrıntılı alfabetik listedir.

Domain: Domainler kayıtlı isimlerdir ve şirketler genelde kendi şirketlerinin isminde domain alırlar. Bir domainin sonunda tr, es, au gibi ülke kodları ya da domain türüne bağlı olarak com, net, org, gov, edu gibi uzantılar yer alabilir. Alan adları IP adresi denilen, bilgisayarların birbirini tanımasını sağlayan numara sisteminin daha basitleştirilmiş ve akılda kalması için kelimelerle ifade edilmiş halidir.

Erişim Kontrol Sistemi: (Access Control System) Bir bilgi işlem sistemine hangi kullanıcının,
hangi haklarla erişebileceğinin ve bu sistem üzerinde hangi işlemleri yapmaya yetkin olduğunun belirlenmesi ve yönetilmesidir.

Firmwareleri: Elektronik eşyalarda bulunan donanımların veya cihazın işlevlerini nasıl yerine getireceklerini bildiren ve genellikle tekrar yazılabilir olan ufak kodlardır. Firmware salt okunurdur, okunabilir fakat yazılamaz.

Firewall: (Güvenlik Duvarı veya Ateş Duvarı) Güvenlik duvarı yazılımı, bir kural kümesi temelinde ağa gelen giden paket trafiğini kontrol eden donanım tabanlı ağ güvenliği sistemidir.

Gateway: (Ağ Geçidi) Farklı ağ iletişim kurallarını kullanan iki bilgisayar ağı arasında veri çerçevelerinin iletimini sağlayan ağ donanımıdır.

Haber Grubu: Mail ya da web ortamında belli bir uzmanlık alanında tartışma veya fikir alışverişi yapılan platformdur.
Heksadesimal: (Hexadecimal) 16 tabanlı sayı sistemidir. Hxx bilgisayar belleğindeki 8 bitlik baytları göstermek için kullanılan bir kestirme yoldur. Bu sayı sistemine "16 tabanlı sayı sistemi" denilmesinin nedeni, 16 tane sembolden oluşmasıdır. Sembollerden 10 tanesi rakamlarla (0, 1, 2, 3, 4, 5, 6, 7, 8, 9), geri kalan 6 tanesi harflerle (A, B, C, D, E, F) temsil edilir.
IP: İnternet'te her bilgisayarın bir IP (Internet Protokol) adresi vardır. Bir IP adresi, noktalarla ayrılan dört rakam grubundan oluşur, her grupta en fazla 3 rakam olabilir; "85.102.156.141" şeklindedir. Internete bağlanan her bilgisayara sistem tarafından verilen bir ayırdedici numara, yani bir tür "adres"tir. IP numarası sayesinde bilgisayarlar internette diğer bilgisayarlarla veri alışverişi yapar. Yani bilgisayarınızın IP numarası sayesinde, herhangi bir web sitesindeki bilgiler sizin bilgisayarınıza kadar ulaşır.

IpSec: (Internet Protocol Security) protokolü, IP paketlerini kimlik doğrulamasına (authentication) ve şifrelemeye (encryption) tabi tutarak IP iletişimini güvenli hale getiren bir protokol takımıdır

IpSec VPN: IpSec VPN, merkez ofiste bulunan bir güvenlik duvarı (firewall) ya da ağ geçidi (gateway) ile internet üzerinden güvenli bir tünel oluşturarak uç noktaları merkeze bağlama mantığıyla çalışan bir bağlantı çeşididir. Mobil cihazlar ya da kişisel cihazlarla IpSec VPN kullanmak mümkün değildir.

İstemci: Yerel ağ ya da internet üzerinde, belli bir hizmeti (ya da hizmetleri) vermekle görevli olan ana bilgisayara (sunucu) bağlanan diğer bilgisayarların her birine verilen genel isimdir. İstemciler, ana bilgisayara bağlanarak sunulan hizmetten yararlanırlar.
İşletim Sistemi: Bilgisayarda çalışan, bilgisayar donanım kaynaklarını yöneten ve çeşitli uygulama yazılımları için yaygın servisleri sağlayan yazılımlar bütünüdür.

Kriptografi: İletilen bilginin istenmeyen şahıslar tarafından anlaşılmayacak bir biçime dönüştürülmesinde kullanılan tekniklerin bütünüdür. Diğer bir deyişle gizlilik, kimlik denetimi,

bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür.

Kümeleme: (Clustering) Birçok bilgisayarı birlikte tek bir bilgisayar gibi göstererek çalıştırma tekniğidir.

L2TP: Bilgisayar ağlarında kişisel sanal ağı destelemek için kullanılan tuneling protokolüdür. Kendi içinde hiçbir gizlilik ya da şifreleme içermez. Tünel yapısı ile bilgi transferi sağlayan şifreleme protokolünden yararlanır.

MAC: Bilgisayar arası iletişim belirli kurallar çerçevesinde gerçekleşir. Her bilgisayarın iletişim için kullandığı nasıl ki IP adresi varsa bu iletişim sırasında kullanılan ağ cihazlarının da tanımlanması için bir adrese gerek vardır. MAC Adress; Bir bilgisayar ağında, bir cihazın ağ donanımını tanımaya yarayan hexadecimal sayı sistemi ile ifade edilen her ağ cihazına özel olarak atanan 48 bitlik adreslere verilen isimdir.

Misafir Ağı: Şirket dışından Şirkete gelenlerin güvenli bir şekilde internete erişimini sağlayan ağdır.

Passphrase: Bir parola veya bir bilgisayar sisteminde veri erişimini kontrol etmek için kullanılan kelime ya da metin dizisidir.

Penetrasyon Testi: Bilişim Sistemlerini oluşturan ağ altyapılarını, donanım, yazılım ve uygulamalara kötü niyetli birinin saldırmasını öngören yöntemler kullanılarak yapılan saldırı ve müdahaleler ile güvenlik açıklarının tespit edilip bu açıklarla sisteme sızılmaya çalışılması ve tüm bu işlemlerin raporlanmasıdır.

Port: Bilgisayar ile çevre birimleri arasında iletişimi sağlayan fiziksel arayüzdür.

PPTP: (Point to Point Tunnel Protocol) Noktadan Noktaya Tünel Protokolü" anlamına gelmektedir. PPTP; VPN'in tünel protokollerinden birisidir.

Public Key: Bu yöntemde kullanıcıların 2 adet şifresi bulunur. Bu şifrelerden birisi herkese açık (umumi,public key) diğeri ise gizli (private, hususi) şifredir. Çalışma mantığına göre umumi olan şifre herkese rahatça dağıtılabilir ve bu şifreden hususi olan şifreye ulaşmanın matematiksel bir yolu bulunmamalıdır. Ayrıca umumi şifre ile şifrelenmiş mesajın hususi şifre ile açılmasının bir yolunun bulunması gerekir.

Private Key: İletişimin kurulabilmesi için bu yöntemde de iki anahtara gerek vardır, ancak anahtarlar temel olarak aynıdır. Her iki anahtar ile de aynı işlevler yerine getirilir.

RDP: (Remote Desktop Protocol) Türkçe uzak masaüstü protokolü anlamına gelmektedir. Kişisel bilgisayar kullanarak "Uzak Ara Bağlantısı" (RDP) protokolü ile bağlanılan, dünyanın

her noktasından, şirket verilerine kolay, hızlı, güvenli ve esnek erişim sağlaması ile tanınan bir teknolojidir.

Root: Tam yetkili kullanıcı yani yönetici demektir. Windows işletim sistemlerindeki yönetici (administrator) kavramıyla eş anlamlı bir kelimedir.

Script: Herhangi bir program dilinde yazılmış uygulama parçalarının tümünün kodlarını içeren kod bütününe script adı verilir.

SSID: (Service Set Indentifier/Hizmet seti kimliği) Bir kablosuz ağı tanımlayan addır.

SSL: (Secure Socket Layer) SSL kişisel gizlilik ve güvenilirlik sağlayan, network üzerindeki bilgi transferi sırasında bilginin bütünlüğü ve gizliliği için sunucu ile istemci arasındaki iletişimin şifrelenmiş şekilde yapılabilmesine imkan veren bu sayede gizliliğinin ve bütünlüğünün korunmasını sağlayan bir güvenlik protokolüdür.

SSL VPN: Son kullanıcı tarafında bir yazılıma ya da donanıma gerek kalmadan işletim sistemlerinin sağladığı İnternet tarayıcılarının kullanılmasıyla bir ağa güvenli bir biçimde bağlantı çeşididir. Mobil cihazlar ya da kişisel cihazlarla SSL VPN kullanmak mümkündür.

Statik IP: IP adresleri İnternet Hizmet Sağlayıcıları tarafından atanır ve bu adresler zaman içerisinde değişebilir. Statik IP adresleri ise değişmez, atandığı cihaz veya sunucu için sabit olarak kalır.

Sunucu: Bir bilgisayar ağı üzerinden kullanıcı isteklerine yanıt veren bilgisayar teknolojisidir.

Sürücü: Bilgisayarın donanım ve aygıtlarla iletişim kurmasını sağlayan bir yazılımdır.

Switch: (Ağ anahtarı) Bilgisayarların ve diğer ağ öğelerinin birbirlerine bağlanmasına olanak veren ağ donanımıdır.

Tünel: Kurumsal ağa erişmek için kullanılan uygulamaların kullandığı veri gizleme yöntemidir.

UTP kablosu: Korumasız bükümlü kablodur. Bilgisayarlar arası veri iletişiminde kullanılır.

Virüs Pattern: Antivirüs programının virüsleri tanıma amacıyla kullandığı imza dosyasıdır.

VLAN: (Virtual Local Area network) Ağ kullanıcılarının ve kaynaklarının bir switch üzerindeki portlara bağlanarak yapılan mantıksal bir gruplamadır.

VPN: Virtual Private Network'ün (Sanal Özel Ağ) kısaltması olup, ağlara güvenli bir şekilde uzaktan erişimde kullanılan bir teknolojidir. Sanal bir ağ uzantısı yarattığından uzaktan bağlanan makine konuk gibi değil, ağa fiziksel olarak bağlıymış gibi görünür.

Yönlendirici: (Router) Ağdaki bilgisayarların yönlerini bulmalarına klavuzluk eder. Bir başka deyişle ağdaki IP paketlerini bir ağdan başka bir ağa taşımaya yarayan cihazlara router denmektedir.

	HAZIRLAYAN	ONAYLAYAN
ÜNVANI	BGYS YÖNETİM TEMSİLCİSİ (DAİRE BAŞKANI)	GENEL SEKRETER
ADI SOYADI	Dr. Naci BAYRAK	Prof.Dr. Ahmet DUMLU
İMZA		