GEBZE TEKNİK ÜNİVERSİTESİ

BİLİŞİM POLİTİKALARI

İçerik

A. AMAÇ ve KAPSAM

Bilişim Politikaları, Gebze Teknik Üniversitesinin (GTÜ) ihtiyaç duyduğu bilginin üretilmesi, saklanması, korunması ve paylaşımı sürecinde bilişim sistemlerinin ve bu sistemlerin işleyişlerinin, 6698 Sayılı Kişisel Verilerin Korunması Kanunu, İSO 27001 ve sair mevzuat ile Cumhurbaşkanlığı İletişim Başkanlığı, internet servis sağlayıcısı TÜBİTAK ULAKBİM'in ilgili politikalarına uygun ve güvenli kullanılması için gerekli usul ve esasları belirlemeyi amaçlar.

Bilişim Politikaları, GTÜ bünyesindeki bütün akademik, idari personel ve öğrenciler ile kendilerine herhangi bir nedenle geçici ve/veya kısıtlı olarak bilişim kaynaklarımızı kullanma yetkisi verilen paydaş ve ziyaretçileri kapsar.

B. HUKUKİ DAYANAK

Bu belgenin hazırlanmasında, "5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" ile "Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik" ve GTÜ mevzuatları esas alınmıştır.

C. TANIMLAR

1. Bilgi İşlem Dairesi Başkanlığı (BİDB): GTÜ'nün bilgi teknoloji hizmetlerini yürüten idari birimi olup kurum organizasyon yapısında Genel Sekreterlik makamına bağlı çalışır.

2. Birincil Kullanım: GTÜ bilişim kaynaklarının; üniversitenin eğitim, öğretim, araştırma, uygulama ile idari ve yönetim faaliyetleriyle ilgili kullanımıdır.

3. Diğer Kullanıcılar: GTÜ bilişim kaynaklarını, kısıtlı veya geçici olarak kişilerdir. Bu kullanıcıların kullanım hakları ve kullanış biçimleri Rektörlük onayı doğrultusunda belirlenir.

4. İkincil Kullanım: Birincil kullanım dışındaki her türlü kullanımdır. İkincil kullanıcı, birincil kullanıcıyı etkilememesi için sınırlandırılabilir.

5. GTÜ Bilişim Kaynakları: Mülkiyet ve kullanım hakkı GTÜ'ye ait olan, kiralanan, lisanslanan veya GTÜ tarafından kullanım hakkına sahip olunan bilgisayar, bilgisayar ağı, yazılım ve donanım servislerinin tümüdür.

6. GTÜ Kullanıcıları: GTÜ bilişim kaynaklarını, eğitim-öğretim ve araştırma amaçlı hizmet faaliyetleri çerçevesinde kullanan tüm akademik ve idari personel ile tüm lisans ve lisansüstü öğrencileridir.

7. GTÜ-NET: GTÜ dâhilinde bölüm, birim, bina ve kampüs düzeyinde bilişim kaynaklarını bir ağ yapısı ile birbirine bağlayan ve internet erişimini sağlayan yerel ağa verilen isimdir.

8. GTÜ-WEB Siteleri: GTÜ web sayfası (gtu.edu.tr) ve GTÜ bilişim kaynaklarını kullanan fakülteler, enstitüler, bölümler, araştırma merkezleri, laboratuvarlar, idari birimler, sosyal faaliyet kulüplerinin etkinlik ve seminer web sayfalarının tümüdür.

9. Yasaklanmış Kullanım: GTÜ bilişim kaynaklarının hiçbir şekilde kullandırılmaması durumudur. Sistem ve ağ güvenliğinin ihlal edilmesi veya GTÜ bilişim kaynaklarını olumsuz etkileyen kullanımın tespit edilmesi durumda BİDB tarafından kullanıcının yasaklı hâle getirilmesidir.

D. GENEL İLKELER VE KULLANIM ESASLARI

BİDB, GTÜ bilişim kaynaklarının kullanılmasıyla ilgili gerekli kuralların ve ilkelerin oluşturulmasında, yenilenmesinde ve uygulanmasında yetkili ve sorumludur. Diğer tüm politika ve yönetmeliklerin bu kurallar ve ilkeler ile tutarlı olmasından, kurumun tüm personelinin ve tüm kullanıcıların bu kuralları ve ilkeleri bilmesini ve anlamasını sağlamaktan GTÜ Rektörlüğü sorumludur. Bu politikada tanımlanan tüm kullanıcılar; kullanım ilkelerini, ilgili politika ve prosedürlerdeki kuralları bilmekten ve bu kurallara uymaktan sorumludurlar.

1. Türkiye Cumhuriyeti'nin ilgili yasaları ve internet servis sağlayıcısı TÜBİTAK ULAKBİM'in ilgili politikaları, GTÜ kullanıcılarının ihtiyaç duyduğu eğitim-öğretim ve araştırma amaçlı hizmet faaliyetleri çerçevesinde bilginin üretilmesi, saklanması, korunması ve paylaşımı sürecinde GTÜ bilişim kaynaklarını kullanması için gerekli usul ve esasları belirler.
2. GTÜ bilişim kaynakları; Üniversite yönetmeliklerine, Türkiye Cumhuriyeti yasalarına ve bunlara bağlı olan yönetmeliklere aykırı faaliyetlerde bulunmak amacıyla kullanılamaz.
3. GTÜ bilişim kaynakları, temel kullanım kapsamındaki ihtiyaçlar için hizmete sunulmaktadır. Bu kaynakların israfından kaçınılmalıdır.
4. GTÜ bilişim kaynaklarında kullanılan altyapıyı, donanımı ve yazılımı zarara uğratıcı, tahrip edici, zedeleyici ve sağlıklı çalışmasını engelleyici girişimlerde bulunulmaması ve kaynakların verimli kullanılması esastır.
5. GTÜ bilişim kaynaklarında bulunan her türlü bilgi (yazılım, donanım, ağ kaynağı), kullanım kurallarına ve koşullarına (kaynak gösterme, telif hakkı, izin, lisans koşulları vb.) uyularak kullanılır.
6. BİDB çalışanları Bilişim Politikalarına göre hareket ederler. Bu politikalara uymayan talepler yerine getirilmez.
7. GTÜ kullanıcıları, temel kullanım kapsamında kendilerine tahsis edilen ve mülkiyeti kendilerine ait olan kaynakların güvenliğini sağlamaktan, güvenlik eksikliğinden kaynaklanacak zararlardan ve bilgisayarda yer alan bilgileri kritik olma düzeyine göre yedeklemekten sorumludur. BİDB tarafından tavsiye edilen lisanslı güvenlik yazılımlarını yüklemek, işletim sistemlerinin güncelliğini takip etmek kullanıcının sorumluluğundadır.
8. GTÜ kullanıcıları; kullanıcı yetkisi, kodu, şifresi ve GTÜ adresini kullanarak bu kaynaklar üzerinde gerçekleştirdikleri çalışmalar ve etkinlikler ile bu kaynaklar üzerinde bulundurdukları veya oluşturdukları bilgi, belge, yazılım gibi her türlü kaynağın içeriğinden, kullandıkları kaynakların kullanım kurallarına uyulmasından şahsen sorumludur.
9. GTÜ kullanıcıları, bu politikada açıklanmamış olsa bile yasal kurallar içindeki tüm kısıtlama ve yaptırımlardan, ahlaki kurallar içindeki tüm kişisel haklar ve fiillerden, internet etik kuralları çerçevesinde kabul gören tüm evrensel kurallara ve Türkiye Cumhuriyeti'nin ilgili yasalarına uymak zorundadır.
10. GTÜ bilişim kaynakları, GTÜ yönetiminin yetkilendirdiği makamlarca belirlenmiş kurallar ve yönergeler çerçevesinde, yetkinin veriliş amacını aşmayacak şekilde ve yapılacak her iş için uygun yetkilendirme ile kullandırılır, yetki almadan değiştirilemez, ortadan kaldırılamaz.
11. GTÜ bilişim kaynakları, kullanım hakkını doğrudan/dolaylı olarak devretmek ya da kiralamak amacıyla ticari nitelik taşıyan gelir teminine yönelik kullanılamaz.
12. GTÜ bilişim kaynaklarının; GTÜ içi bilgi kaynaklarını (duyuru, haber, doküman vb.) yetkisiz ve/veya izinsiz olarak 3. kişilere/kuruluşlara dağıtmak amacıyla GTÜ'ye ve 3. kişilere/kuruluşlara ait bilgilere ve kaynaklara izinsiz ve/veya yetkisiz erişim sağlamak ve diğer kullanıcıların kaynak kullanım hakkını engelleyici faaliyetlerde bulunmak için kullanılması yasaktır.
13. GTÜ bilişim kaynakları, genel ahlak ilkelerine aykırı materyal üretmek, barındırmak, iletmek, gerçek dışı, rahatsızlık verici, gereksiz korku yaratacak, kişilerin ve kurumların fikri mülkiyet haklarını ihlal edici, başkalarının veri ve bilgilerini tahrip edici, kişisel bilgilere tecavüz edici, iftira ve karalama mahiyetinde materyalin üretimi, rastgele ve alıcının istemi dışında mesaj (SPAM iletiler) göndermek ve ülkenin birlik ve beraberliğine bölünmez bütünlüğüne aykırı siyasi, dini, etnik propaganda amacıyla kullanılamaz.
14. BİDB'nin onayı olmadan GTÜ bilişim kaynaklarıyla ilgili hiçbir donanım veya yazılım (bilgisayar, sunucu, kablolu-kablosuz ağ cihazları gibi cihazlar veya fiber, cat6, gibi kablolar) montajlanamaz, kurulamaz, kullanılamaz; mevcut kaynakların yerleri ya da ayarlarıyla ilgili hiçbir değişiklik yapılamaz.

15. Kişilerin kurum içine getirdikleri kendi şahıslarına ait cihazlar, GTÜ bilişim kaynaklarının işleyişini olumsuz yönde etkiliyorsa BİDB gerektiğinde müdahale eder, yönetimini devralır, kurum içinde çalışmasını engeller.

16. BİDB, bilgisayar ağında oluşabilecek güvenlik açıklarını asgari düzeye indirebilmek için kullanıcılara güvenlik yazılımları (antivirüs, antispam ve kişisel güvenlik yazılımı) ve işletim sistemi güncellemelerini yeniliklerini izleyerek kullanıcıları bilgilendirir.

17. BİDB, gerek görülmesi hâlinde bir kullanıcının hesabını iptal etme veya geçici bir süreliğine dondurma, sunduğu hizmetin şeklini değiştirme veya son verme hakkına sahiptir. Değişiklik sonrasında oluşabilecek sorun ve kayıplardan GTÜ sorumlu tutulamaz.

18. GTÜ kullanıcıları, bilişim kaynakları kullanımı ile ilgili olarak sorunları belirlemek, çözmek veya esaslara aykırı davranışları tespit etmek amacıyla yetkili makamlarca kendilerinden talep edilen bilgileri vermekle yükümlüdür.

19. GTÜ, bilişim kaynaklarını ve bu kaynaklarla gerçekleştirilen aktiviteleri izleme, kaydetme ve periyodik olarak denetleme hakkını saklı tutar.

20. Bu kurallar yayınlandığı tarihten itibaren geçerlidir. Gerekli görüldüğü durumlarda GTÜ yetkili makamlarınca metin üzerinde değişiklik yapılabilir. GTÜ bilişim politikası ve yönetmeliklerinde tanımlanmayan durumlar BİDB tarafından değerlendirilir.

E. YETKİ VE SORUMLULUKLAR

1. GTÜ'de tüm bilişim kaynaklarının kurulumu ve işletmesine ait yetki ve sorumluluk BİDB'ye aittir.
2. BİDB; akademik, idari, eğitim ve araştırma amaçları doğrultusunda bölüm ve birimlerin bilişim kaynaklarına ulaşabilmelerini sağlamak üzere oluşturulan altyapıyı kurmak, işletmek ve güncellemekle sorumludur.
3. BİDB, bilişim sistemlerini teknik düzeyde planlama ve uygulama sorumlusu ve yetkilisidir.
4. GTÜ akademik ve idari personelinin bilgisayarlarına BİDB'nin yüklediği programların lisans sorumluluğu (GTÜ'nün satın aldığı lisanslı programlar hariç) BİDB'ye aittir.
5. GTÜ kullanıcıları, bilgisayarındaki işletim sisteminin ve işletim sistemi üzerinde çalışan yazılımların güvenlik tehditlerine karşı korunabilmesi için yazılımları en son yamaları (patch) ile güncel tutmakla ve BİDB tarafından belirlenen esaslara göre verilen kullanıcı adı ve şifresini kullanmakla sorumludur. Kullanılan şifreler politikalara uygun olarak belirlenmelidir.
6. GTÜ kullanıcıları, bilgisayarlarında mutlaka antivirüs programının yüklü ve programın güncellemelerinin tam olmasından sorumludur. GTÜ kullanıcısı, GTÜ'nün kullandığı lisanslı antivirüs yazılımını BİDB'den temin edebilir.
7. GTÜ kullanıcıları, GTÜ bilişim kaynakları kullanımı için kendilerine tahsis edilen kullanıcı kodu ve şifresini korumakla ve politikalara uygun şifre belirlemekle sorumludur. Kullanıcı her ne sebeple olursa olsun kullanıcı adı ve şifresini üçüncü kişilerle paylaşmamalıdır.
8. GTÜ kullanıcıları, kişisel verilerinin yedeğini almaktan sorumludur.
9. GTÜ bilişim kaynaklarını kullanıma sunma hakkı sadece BİDB'ye aittir. Aksi halde ortak kullanıma açık olan kaynakların çoğaltılması, paylaşılması ve yayınlanması ile oluşabilecek siber suçlardan kaynağı paylaşan kişi sorumludur.
10. BİDB, Üniversite bilişim kaynakları kullanımı hakkında genel kuralları belirlemek, bu kuralları gelişen teknolojinin öngördüğü biçimde sürekli olarak değerlendirmek ve gerekli değişiklikleri hayata geçirmekten sorumludur. Bu tür değişiklikler yapıldığında genel duyuru mekanizmaları ile kullanıcıları bilgilendirir.
11. "Yasal Sorumluluk Reddi (Disclaimer)" metinleri, genel ilkelere aykırı kullanımların kabul edilebilir olduğunu göstermez ve GTÜ Bilişim Politikalarını ve yönetmeliklerini geçersiz kılamaz.

F. UYGULAMA VE YAPTIRIMLAR

GTÜ bilişim kaynaklarına, bu kaynakların işleyişlerine ve genel ilkelere uygun olmayan kullanım durumunda; gerçekleştirilen eylemin yoğunluğuna, kaynaklara veya kişi/kurumlara verilen zararın boyutuna, tekrarına göre aşağıdaki işlemlerin bir ya da birden fazlası sırayla ya da sırasız GTÜ Rektörlüğü adına BİDB tarafından uygulanır:

1. Kullanıcı sözlü ya da yazılı olarak uyarılır.
2. Kullanıcı "yasaklanmış kullanım" durumuna getirilir.
3. Kullanıcıya tahsis edilmiş GTÜ bilişim kaynakları kısa veya uzun süre kapatılabilir.
4. GTÜ akademik veya idari soruşturma veya disiplin mekanizmaları harekete geçirilebilir.
5. Adli yargı mekanizmaları harekete geçirilebilir.
6. Kullanım ve kullanıcı tanımlarının yetersiz kaldığı ya da "Gebze Teknik Üniversitesi Bilişim Politikaları" belgesi dâhilinde tanımlı olmayan durumlarda BİDB geçici tedbirler alıp GTÜ Rektörlüğünü bilgilendirir, durum ilgili birimlerce değerlendirilir.

G. KULLANICI PAROLA ESASLARI

Amaç: Bu politikanın amacı güçlü şifre oluşturma, bu şifreyi koruma ve şifre değişim aralıkları için bir standart oluşturmaktır.

Kapsam: Bu politika GTÜ bilişim kaynaklarını, bilişim altyapısını ve bunları kullanmakta olan tüm kullanıcıları, birimleri ve bağlı kuruluşları, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım sağlayıcılarını kapsamaktadır.

Parolalar bilgisayar güvenliğinin en önemli unsurlarıdır. GTÜ bilişim kaynaklarına veya kullanıcıların kişisel cihazlarına erişim için kullandıkları parolalar güvenlik açısından aşağıdaki belirtilen politikaları sağlamalıdır. Kötü seçilmiş bir şifre bütün kurumsal ağı etkileyebilecek sonuçlar doğurabilir. Bunun gibi bir durumla karşılaşmamak için kurumsal ağa dâhil olan bütün kullanıcılar, kendisini ve kurumunu korumak için aşağıdaki önlemleri almakla sorumludur:

1. Parola en az 8, en fazla 14 karakter uzunluğunda olmalıdır.
2. Parola en az 1 (bir) büyük harf, 1(bir) küçük harf, 1(bir) rakam ve 1(bir) özel karakter (***! @ # $ % ^ & * ( ) _ + \| ~ - = \ ` { } [ ] : " ; ' < > ? , . /***) içermelidir.
3. Parola için kolay tahmin edilebilir kişisel bilgiler kullanılmamalıdır. Parola kişiye özel olup başka kullanıcılarla paylaşılmamalıdır.
4. Parolalar yılda en az 2 (iki) defa (6 ayda bir) değiştirilmelidir. Değiştirilen parola mutlaka son kullanılan 3 (üç) şifreden farklı olmalıdır.
5. Her cihaz ve uygulama için ayrı parola belirlenmeli, aynı parola kullanılmamalıdır.
6. Parolaların korunması kullanıcının sorumluluğundadır.

H. BİLGİ GÜVENLİĞİ POLİTİKALARI

Amaç: Bilgi güvenliği politikalarında GTÜ'deki eğitim-öğretim faaliyetlerine ilişkin tüm bilgi varlıklarımızın gizliliği, bütünlüğü ve gerektiğinde yetkili kişilerce erişilebilirliğini sağlamak amaçlanır.

Kapsam: Bu politika GTÜ bilişim kaynaklarını, bilişim altyapısını ve bunları kullanmakta olan tüm birimleri ve bağlı kuruluşları, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamaktadır. Bilgi güvenliği politikası kapsamında bilgi varlıkları (veri dosyaları sözleşmeler vb.), yazılım varlıkları (uygulama yazılımları, sistem yazılımları, hizmet yazılımları vb.), fiziksel bilişim varlıkları (ağ cihazları, sunucular, depolama araçları, vb.), hizmet ve insan kaynakları varlıkları bulunmaktadır.

Hedef: Bilgi güvenliği yönetimi kapsamına alınan tüm süreçlerde ve varlıklarda gizlilik, bütünlük ve erişilebilirlik prensiplerine uyacak önlemler almak amacıyla GTÜ bilişim hizmetlerinin gerçekleştirilmesinde

kullanılan tüm fiziksel ve elektronik bilgi varlıklarının bilgi güvenliğini sağlamayı hedefler. Bu hedefler doğrultusunda her bir varlık için risk seviyesini, kabul edilebilir risk seviyesinin altında tutmak hedeflenmektedir.

1. Bilgi Güvenliği Politikası tüm faaliyetlerimizin ISO 27001:2013 standardına uygun yürütülmesini garanti altına alır.
2. Bilgi Güvenliği Politikası kurumun güvenilirliğini ve itibarını korumayı sağlar.
3. Bilgi Güvenliği Politikası kurumun ve paydaşlarının bilgi varlıklarına güvenli bir şekilde erişimini sağlar.
4. Bilgi Güvenliği Politikası kurumun ve paydaşlarının bilgi varlıkları üzerinde oluşabilecek riskleri değerlendirmeyi ve yönetmeyi sağlar.
5. Bilgi güvenliğinin ihlali durumunda gerekli görülen yaptırımları uygular.
6. Tabi olduğu ulusal ve uluslararası yasal ve ilgili mevzuat gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülüklerini karşılamaktan, iç ve dış paydaşlara yönelik kurumsal sorumluluklarından kaynaklanan bilgi güvenliği gereksinimlerini sağlar.
7. İş/Hizmet sürekliliğine karşı bilgi güvenliği tehditlerinin etkisini azaltır ve işin sürekliliği ile sürdürülebilirliğini sağlar.
8. Çeşitli kontrollerle bilgi güvenliği seviyesini korumayı ve iyileştirmeyi taahhüt eder.
9. GTÜ kullanıcıları bilgi güvenliği politikalarına, talimat ve prosedürlerine uymakla yükümlüdür.
10. GTÜ kullanıcılarını içeriden veya dışarıdan gelebilecek tehditlere karşı korumak, üretilen veya kullanılan bilgilerin gizliliğini güvence altına alarak GTÜ'nün imajını korumakla yükümlüdür.
11. Üçüncü taraflarla yapılan sözleşmelerde güvenlik prosedürleri belirlenir.
12. Bilgi güvenliği prosedürlerini yerine getirerek personelin bilgi güvenliği farkındalıklarını artırır.
13. Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlar.
14. GTÜ kullanıcıları, kritiklik düzeylerine göre işlediği bilgiyi yedekler.
15. GTÜ kullanıcıları, bilgi güvenliği ihlal olaylarını bilgi güvenliği yetkilisine bildirmeli, raporlamalı ve bu ihlalleri engelleyecek önlemleri almalıdır.
16. GTÜ bilişim kaynakları, T.C. yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacıyla kullanılamaz.
17. Hizmet alanlara, verenlere ya da üçüncü taraflara ait olmasına bakılmaksızın, üretilen ve/veya kullanılan bilgilerin gizliliği, bütünlüğü ve erişilebilirliği her durumda güvence altına alınır.
18. Bilgi güvenliği politikaları ve GTÜ Bilgi Güvenliği Yönetim Sistemi Standartları (TS ISO/IEC 27001) Bilgi İşlem Dairesi Başkanlığı tarafından yürütülür.
19. GTÜ kullanıcıları bilgi güvenliği kapsamında aşağıda belirtilen kurallara uymakla yükümlüdür:

19.1. GTÜ tarafından lisansları alınan güvenlik yazılımlarını sistemlerden kaldıramaz veya devre dışı bırakamaz.
19.2. İstemciden istemciye dosya paylaşım programlarını bilgisayarlara yüklemeleri ve kullanmaları yasaktır.
19.3. İşle ilgili olmayan veya telif hakları ile korunan dosyaları indirmeleri, depolamaları, çoğaltmaları ve paylaşıma açmaları yasaktır.
19.4. Lisansı temin edilmemiş yazılımlar kullanamaz.
19.5. Zararlı yazılımları sistemlere yükleyemez veya yüklemeye çalışamaz.
19.6. Sistemlerde açık servisleri ve güvenlik açıklarını tespit eden ağ trafiğini dinleyen programları yüklemeleri ve çalıştırmaları yasaktır. Tespit edilmesi halinde cezai işlemler başlatılır.

19.7. Üniversiteye ait bilgisayar ve çevre birimlerini, yan donanımlarını (mobil ürünler hariç) izinsiz olarak kullanım dışı bırakmaları, bunların yerlerini değiştirmeleri, kurum dışına çıkartmaları yasaktır.
19.8. BİDB'nin bilgisi dışında, kendilerine veya firmalara ait sistem ve donanımları yazılı izin veya sözleşme olmadan bilişim ve bilgi sistemlerine bağlayamaz.
19.9. Kullanımına yetkili olunmayan sunucu hizmetlerini çalıştıramaz ve sunucu sistemler üzerinde kişisel bilgisayar uygulamalarını kullanamaz.
19.10. GTÜ'ye ait, halka açık olanlar dışındaki bilgileri kopyalamaları; internet üzerinde, haber gruplarında, posta listelerinde, forumlarda ve sosyal medya üzerinden paylaşmaları yasaktır.
19.11. BİDB'den izin almadan çevirmeli ağ modemi, GPRS/Edge modemler, bluetooth ve kızılötesi iletişim cihazlarını sistemlere bağlayamaz.
19.12. Gizlilik dereceli bilgileri içeren yazılı veya elektronik belgelere yetkisiz şekilde erişmeye çalışmaları, erişmeleri, değiştirmeleri, bu belgeleri belirlenen alıcısı dışındaki kişi ve kurumlara teslim etmeleri, yetkisiz kişilerle paylaşmaları yasaktır.
19.13. Yazıcılara gönderilen gizlilik dereceli belgeleri, kontrol altında bulundurmadan cihaz üzerinde bırakamaz.

20. GTÜ'ye ait veriler GTÜ'nün özel sistemleri veya GTÜ kontrolündeki yerli sistemler hariç bulut depolama sistemlerinde saklanmayacaktır.
21. GTÜ'ye ait veya kurumsal mahremiyet içeren veri, doküman ve belgeler kurumsal olarak yetkilendirilmemiş veya kişisel olarak kullanılan cihazlarda bulundurulmayacaktır.
22. GTÜ'ye ait verilerin işlendiği yerlerde yayma güvenliği ve benzeri güvenlik önlemleri veri yetkilisinin sorumluluğundadır.
23. Veri paylaşımı ve haberleşmede yerli kriptolama sistemleri kullanılacak ve yerli uygulamalar tercih edilecektir.

İ. İNTERNET HİZMETLERİ POLİTİKALARI

İnternet Hizmetleri Politikası, GTÜ'nün hizmet sağlayıcısı olan TÜBİTAK ULAKBİM' in sunduğu Ulusal Akademik Ağ (ULAKNET) kullanım politikalarını ve GTÜ Bilişim Politikalarını kapsar. Bu politika kapsamında ağ kullanımı, ağ cihaz kullanımı, kablosuz ağların kullanımını içermektedir.

1. GTÜ Genel İnternet Kullanım Politikaları

1.1. GTÜ-NET; Üniversite yönetmeliklerine, TÜBİTAK ULAKBİM Politikasına, ilgili yasalara ve bunlara bağlı olan yönetmeliklere göre kullanılır.
1.2. GTÜ-NET ile kullanıcıların eğitim, öğretim, bilimsel ve teknolojik araştırma-geliştirme, bilginin yayılması ve paylaşılması amaçlanmaktadır.
1.3. GTÜ-NET kullanıcıları, bilgisayar ağ erişimi ve bilgisayar erişimi için BİDB politika ve kurallarına uymalıdır. BİDB tüm ağ erişimleri için kullanıcı doğrulaması isteyebilir.
1.4. GTÜ-NET kullanıcıları, kullanım hakkını doğrudan ya da dolaylı olarak devredemez ya da kiralamak yoluyla ticari nitelik taşıyan ve gelir teminine yönelik kullanamaz.
1.5. GTÜ-NET kullanıcıları, servis veren (web hosting servisi, e-posta servisi vb.) sunucu nitelikli bilgisayar kullanamaz.
1.6. GTÜ-NET kullanıcıları, diğer kullanıcıların kaynak kullanım hakkını engelleyici faaliyetlerde bulunamaz ve kaynaklara zarar verici/kaynakların güvenliğini tehdit edici biçimde kullanamaz.
1.7. GTÜ-NET kullanıcıları, genel ahlak ilkelerine aykırı materyal üretmek, barındırmak, iletmek, siyasi propaganda yapmak, rastgele ve alıcının istemi dışında mesaj (spam iletiler) göndermek amacıyla kullanamaz.

1.8. GTÜ-NET kullanıcılarının, diğer kullanıcılara ait verileri bozması ya da verilere zarar vermesi, diğer kullanıcıların gizlilik hakkını ihlal etmesi, kasten ya da zayıf güvenlik nedeni ile bir bilgisayarın herhangi bir bilgisayar virüsü, solucanı, trojanı, casus programı ya da istenmeyen programları bulaştırması veya yüklemesi yasaktır.
1.9. GTÜ-NET kullanılarak P2P dosya paylaşım (peer-to-peer) yazılımları kullanılamaz. Söz konusu yazılımlar bilimsel amaç için kullanılacaksa BİDB'den kısıtlı ve geçici kullanım izni talep edilir.
1.10. Kullanıcıların port taraması, güvenlik taraması, ağ izlemesi ve kullanıcının kendisi için olmayan veriyi almaya çalışması, GTÜ'nün kritik bilgisinin ortaya çıkmasını veya kurum servislerinin ulaşılamaz hâle gelmesine sebep olacak tüm aktiviteleri yasaktır.

2. Ağ Kurulumu ve Altyapı Hizmetlerinin Yürütülmesi:

2.1. Ağ altyapısı periyodik olarak incelenerek ihtiyaçların belirlenip yeni cihazların sisteme eklenmesi BİDB tarafından yürütülür.
2.2. Ağ altyapısının ihtiyaçları, mevcut altyapıya uyumlu ve GTÜ Bilişim Politikalarını karşılayabilecek doğrultuda belirlenir ve projelendirilir.
2.3. GTÜ internet ağ altyapısına uygunluğu, istenilen özellikleri karşılayıp karşılamadığı belirlenen ve uygun olan cihazların kurulumu yapılır.
2.4. İş talepleri resmî yazı ile BİDB'ye yapılır. Bunların dışında yapılan iş talepleri dikkate alınmaz. İş talepleri birim/bölüm amiri tarafından yapılmak zorundadır.
2.5. İş talepleri, önem ve geliş sırasına göre BİDB çalışanları tarafından karşılanır. Kullanıcıya talebinin ne zaman gerçekleştirilebileceği hakkında bilgi verilir. İş talebinde bulunan kişinin de işin yapılacağı zaman, yerinde olması gerekir.

3. Kablosuz İnternet Kullanımı

3.1. GTÜ kablosuz ağı, BİDB güvenlik politikaları doğrultusunda kullanılmalıdır.
3.2. GTÜ kablosuz ağına GTÜ mail hesap bilgileri ile giriş yapılır. Kurum dışı kullanıcılar, kendi üniversite hesapları ile EDUROAM kablosuz ağına bağlanarak internete erişebilirler.
3.3. GTÜ kablosuz misafir ağına bağlanacak kullanıcılar, kendilerine referans olacak GTÜ kullanıcısının onayı ile sisteme belirli bir süre bağlanabilirler. Bağlantı için misafir SSID seçilir, karşısına çıkan forma onayı verecek kullanıcı bilgileri ile misafir kullanıcı kimlik bilgileri girişi yapılır ve onayı verecek kullanıcı mail hesabına gelen onay linkini tıklar.
3.4. GTÜ kablosuz ağ altyapısı; akademik, idari, eğitim ve araştırma amaçlarına hizmet etmek üzere yapılmıştır. Kablosuz ağ üzerindeki kişisel kullanımlar diğer kullanıcıların ağ erişim gereksinimlerini (akademik, idari, eğitim, araştırma) yerine getirmelerine engel olmamalıdır.
3.5. Kablosuz ağ kaynakları kullanılarak kütlesel e-posta gönderilmesi (mass mailing, mail bombing, spam) ve üçüncü şahısların göndermesine olanak sağlanması yasaktır.
3.6. GTÜ kablosuz ağ kaynaklarının üniversite dışından kullanılmasına sebep olabilecek ya da üniversite dışındaki kişi ya da bilgisayarların kendilerini üniversite içindeymiş gibi tanıtarak internet altyapısını kullanması yasaktır.
3.7. Ağ güvenliğini tehdit edici faaliyetlerde bulunmak yasaktır. Tehdit tespit edilmesi durumunda internet erişimi süresiz kesilir.
3.8. Kablosuz ağ hizmetinden faydalanan her kullanıcı, üniversite tarafından kendisine tahsis edilen kaynakların kullanımından, güvenliğinden ve bu kaynakların bilinçli ya da bilinçsiz olarak üçüncü kişilere kullandırılması durumunda ortaya çıkabilecek yasaklanmış faaliyetlerden birinci derecede sorumludur.
3.9. Kurallara uymadığı tespit edilen öğrenci ve personele bildirilmeden gerekli tedbirler alınabilir.

3.10. Bu kurallar yayınlandığı tarihten itibaren geçerlidir. Gerekli görüldüğü durumlarda metin üzerinde değişiklik yapılabilir.

J. E-POSTA KULLANIM POLİTİKALARI

Bilgi İşlem Dairesi Başkanlığı, GTÜ'de görev yapan kadrolu akademik ve idari personele, akademik-idari birimlere, öğrenci topluluklarına, ulusal-uluslararası sempozyum, kongre vb. etkinliklere, öğrencilere, sözleşmeli personele ve kadrosuz akademik personele e-posta hizmeti verir.

1. Genel Kurallar Tanımlamalar:

1.1. Birim, bölüm ve akademik, idari personel ile öğrenci toplulukları ve GTÜ tarafından organize edilen veya katılımda bulunulan ulusal/uluslararası etkinlik ve organizasyonlara verilen kullanıcı hesabı bu politika kuralları çerçevesinde verilmektedir. Kullanıcı hesabı ve geçici şifreler sistem tarafından otomatik olarak oluşturulmaktadır.

1.2. Kullanıcı hesapları en fazla 15 karakter olmalıdır. Kullanıcı hesabı başvurularında, ulusal örf ve âdetlere, kültürel değerlere, genel ahlak kurallarına uyum aranır. Kullanıcı hesabının tamamı ya da bir kısmı hakaret, küfür, çirkin tanımlama vb. ifadeler içeremez. Bu tür sözcük ve/veya ifadelerin İngilizce ya da diğer yabancı dillerdeki karşılıkları da bu kapsam dâhilindedir. Bu tanıma uyan kullanıcı hesabı tahsisi yapılmaz, yapılmış olanlar geri alınır.

1.3. GTÜ, BİDB tarafından belirtilmiş politikalara uymayan veya sunulan hizmetleri kötüye kullandığı tespit edilen kişilerin kullanıcı hesapları 'pasif' duruma getirilerek kullanımları engellenir veya hesapları silinir. GTÜ BİDB, kullanıcı hesaplarını güvenlik gerekçesi ile pasif duruma getirme hakkına sahiptir.

1.4. GTÜ e-posta hizmeti Office365 platformu üzerinden hizmet vermektedir. Office365, Microsoft tarafından sağlanan e-posta ve takviminize her yerden erişebileceğiniz, office dokümanlarınızı (word, excel, powerpoint vb.) web üzerinden düzenleyebileceğiniz, anlık mesajlaşma ve görüntülü ve/veya sesli konferans yapabileceğiniz, dosyalarınızı paylaşabileceğiniz bir bulut platformudur.

1.5. GTÜ e-posta hizmeti Microsoft ile yapılan anlaşma ile 50 (elli) GB kotalı olarak kullanıma sunulmuştur. Belirlenen kota ihtiyaç halinde GTÜ tarafından değiştirilebilir.

1.6. GTÜ e-posta grupları tanımlanmış olup bu gruplara duyuru ve bilgilendirme mailleri gönderilmektedir. Bu tarz bilgilendirme ve duyuru mailleri alınmadığında BİDB'ye bildirilir.

1.7. GTÜ e-posta gruplarına e-posta gönderme yetkisi sadece Genel Sekreterliktedir. Genel Sekreterliğin onayı doğrultusunda yetki verilen kullanıcılar haricinde mail gönderilmesi engellenir.

1.8. GTÜ veya başka mail adreslerine yardımcı programlar vasıtasıyla toplu mail gönderimi engellenmiş ve kurum içerisinden bu tarz maillerin gönderimi yasaklanmıştır.

1.9. GTÜ e-posta hizmeti, GTÜ kablosuz ağa erişmede kimlik doğrulama olarak kullanılır.

1.10. GTÜ e-posta hizmeti ile Microsoft tarafından sunulan OneDrive web alanında 1 (bir) TB'lik depolama alanı kullanılabilir. Bu kapasite GTÜ tarafından değiştirilebilir.

2. Personel, Akademik-İdari Birim, Sempozyum, Kongre, Etkinlik ve Öğrenci Toplulukları e-posta Hesapları:

2.1. GTÜ'de yeni işe başlayan personelin özlük bilgilerinin Personel Dairesi Başkanlığı tarafından sisteme kaydından sonra personelin BİDB sistem yönetimi servisine kimlik belgesi (nüfus cüzdanı, ehliyet veya pasaport) ile şahsen başvurması hâlinde bir adet kullanıcı hesabı ve geçici şifresi verilir. Kullanıcılar, kullanıcı hesaplarını, üniversitedeki kullanıcı hesabı ile hizmet aldığı birimlere bildirmek ile yükümlüdür.

2.2. Akademik-idari birim, sempozyum, kongre ve etkinlik amacıyla T.C. vatandaşı olmayan misafirler tarafından kullanılacak e-posta hesapları; bir üst makam onayıyla BİDB'ye üst yazı

iletildikten sonra sistem yönetimi tarafından açılır ve ilgili kullanıcıya bildirilir. T.C. Vatandaşı olan misafirler için wifi ağından misafir yayın kullandırılır.
2.3. Açılacak e-posta hesapları ad.soyad@gtu.edu.tr şeklinde olmalıdır. Kullanıcı isterse ismin ilk harfi, soyisim gibi alternatifler de kullanabilir.
2.4. E-posta hesabı almak veya şifre yenilenmesi için BİDB'ye şahsen başvurulmalıdır.
2.5. GTÜ personelinin telefon, e-posta gibi yöntemlerle hesap açtırmaya veya unutulan şifreyi yeniletmeye yönelik talepleri güvenlik gerekçesi ile kabul edilmemektedir.
2.6. "Öğrenci Kulübü" veya "Öğrenci Toplulukları" hesaplarının her yıl güncellenmesi gerekir. Güncellenme işlemi yapılmayan hesaplar 1 yıl bekletildikten sonra silinir. Sağlık Kültür ve Spor Dairesi Başkanlığı ya da ilgili Öğrenci Toplulukları Komisyonu e-posta hesabından sorumlu olacak kullanıcılar Bilgi İşlem Daire Başkanlığına resmi yazı ile bildirilir.
2.7. Ayrılan veya emekli olan personel için kapatma işlemi yapılmayacaktır. Ancak GTÜ'de görevi sona ermiş kullanıcı tarafından yapılan yazılı talep üzerine, BİDB tarafından hesabı silinir.

3. Öğrenci E-posta Hesapları:
3.1. E-posta hesapları ad.soyadyıl@gtu.edu.tr şeklinde açılır. Aynı ad-soyad için ad.soyadyıl şeklinde hesap açılmaktadır. Bu durum yüksek lisans ve doktora öğrencileri için ismin ilk karakteri, soyisim (Ali Veli için ali.veli(yıl) / aveli(yıl) / a.veli(yıl)) gibi farklı kombinasyon uygulanmaktadır.
3.2. Yeni kayıt yaptıran lisans ve lisansüstü öğrenciler GTÜ APOLLO sistemi üzerinden e-posta adresi alabilirler.
3.3. Lisans ve Lisansüstü öğrencileri e-posta şifrelerini GTÜ APOLLO sistemi üzerinden alabilirler.
3.4. Öğrencilerin telefon, e-posta gibi yöntemlerle hesap açtırmaya veya unutulan şifreyi yeniletmeye yönelik talepleri güvenlik gerekçesi sebebiyle kabul edilmez.
3.5. Mezuniyetinden dolayı GTÜ ile ilişiği kesilenlerin kullanıcı e-posta hesapları açık kalabilir.
3.6. İlişik kesme işlemi mezuniyet dışındaki hâllerden kaynaklıysa ilgili birim tarafından Bilgi İşlem Dairesi Başkanlığına resmi yazı ile bildirilir ve e-posta hesabı kapatılır.
3.7. Özel öğrenciler için e-posta hesapları geçici süreli olarak açılır. Özel öğrenciler e-posta hesabı açmak ya da şifre işlemleri için GTÜ APOLLO sistemini kullanabilirler.

4. Sözleşmeli Personel, Kadrosuz Akademik Personel E-posta Hesapları:
4.1. Sözleşmeli/Misafir tüm personel için ilgili birim/bölüm amiri tarafından görev süresini belirten resmi yazı ile BİDB'ye başvurularak e-posta hesabı açılır. Açılan hesap görev süresi bitiminde otomatik olarak kapatılır.
4.2. Sözleşmeli/Misafir tüm personel, e-posta hesabı şifre işlemleri için BİDB Sistem Yönetimine şahsen kimlikleri ile başvurur.
4.3 Kurumsal e-posta hesapları şahsi amaçlarla (özel iletişim, kişisel sosyal medya hesapları vb.) kullanılmayacaktır.
4.4 Kurumsal olmayan şahsi hesaplar üzerinden Kurumsal iletişim yapılmayacaktır.

K. SUNUCU GÜVENLİĞİ VE YEDEKLEME POLİTİKASI

Amaç: GTÜ'nün bilgi sistemleri için kullandığı sunucuları ve yedekleme hizmetlerini oluşabilecek hatalar karşısında sistemlerin kesinti sürelerini ve olası veri kayıplarını en az düzeye indirmek için sunucu güvenliği ve yedekleme politikaları tanımlanmıştır.

Kapsam: Tüm bilgi sistemleri sunucuları, sunuculardaki kurum verileri, bu sistemlerin işletilmesinden sorumlu personel ve bu sistemlerin yürütülmesinden sorumlu BİDB, sunucu güvenliği ve yedekleme politikası kapsamında yer almaktadır.

1. Sunucular üzerinde yetkili erişimlerin denetimleri yapılır.
2. Sunucular üzerine güncel antivirüs programları kurulmalı ve güncel veri tabanına sahip olmalıdır.
3. Sunucu üzerinde sadece hizmet verdiği portlar açılır ve diğer bağlantılar firewall kullanılarak erişime kapatılır.
4. Sunucuya erişim sağlayacak kullanıcılar için belli IP bloklarına izin verilir, hiçbir şekilde genel bir erişim verilmez.
5. Bilgi sistemlerinde oluşabilecek hatalar karşısında; sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigürasyon, sistem bilgilerinin ve kurum verilerinin yedeği uygun ve düzenli olarak alınır.
6. Yedeği alınacak veri ve uygulamalar için sınıflandırma yapılır. Her bir sınıf için kabul edilir, veri kaybı süresi yönetim tarafından belirlenir.
7. Yedekleme politikasına uygun yedekleme planı oluşturulur.
8. Yedekleme işlemine ait kayıtlar tutulur ve periyodik olarak yönetime rapor sunulur.
9. Başarısız olan yedekleme işlemi varsa başarısız olma sebebi giderilir ve eksik yedekleme işlemi tamamlanır.
10. Yedekleme ortamları etiketlenir. Hangi medyada hangi yedeğin tutulduğu, yedekleme tarih ve saatleri kayıt altına alınır.
11. Yedekleme medyalarının kopyaları, ana sistem odasına zarar verebilecek felaketlerden etkilenmeyecek uzaklıkta ve güvenli bir ortamda depolanır.
12. Yedeklenmiş verilerin düzenli aralıklarla geri döndürme testi yapılır.
13. Yedekleme alt yapısı, yedekleme ve geri döndürme işlemleri için sorumlu kişilerce talimatlar oluşturulur.

L. DONANIM DESTEK SERVİSİ HİZMET POLİTİKASI

Bilgi İşlem Dairesi Başkanlığı Teknik Servis Birimi tarafından GTÜ'ye ait bilişim donanımlarının kurulum destek ve servis işlemlerini aşağıda belirtilen kurum bilişim politikaları çerçevesinde yürütür. Bu politikalar çerçevesinde belirtilmeyen işleri yapma yükümlülüğü yoktur. Politikada belirtilmeyen farklı işlemler söz konusu olduğunda öncelikle işi yaptırmak isteyen birimin onayı daha sonra BİDB onayı alınmalıdır.

1. BİDB tarafından oluşturulan Teknik Servis Hizmetleri, takip programı (Donanım ve Arıza Kayıt Sistemi) üzerinden gelen taleplere hizmet verir. Bu sisteme giriş için GTÜ Anibal bilgi sistemi veya GTÜ'deki kullanıcı bilgileri ile giriş yapılır. Kullanıcı ilk kez giriş yapacaksa bim@gtu.edu.tr e-posta adresiyle iletişime geçer.
2. Akademik ve idari personelin kullandığı demirbaş numarası olan cihazlara, yazılım ve garanti kapsamında olmayan cihazlara donanım desteği verilir.
3. Garanti kapsamı içinde olan cihaz için cihazı öncelikle satın alınan firmaya yönlendirmeniz gerekmektedir. Cihazınızla ilgili herhangi bir sorunla karşılaştığınızda BİDB teknik servis takip programına kayıt açmanız gerekmektedir.
4. Talebinizi sisteme girdikten sonra talebin işleme alındığına dair size bir bilgilendirme e-postası gönderilir. İşlem sonlandığında ise talebinizin tamamlandığını belirten bir e-posta gönderilir.
5. Yazılım ve donanım taleplerinizde; talep sıranıza göre size telefonla ulaşılacak, sorunun durumuna göre BİDB'de veya yerinde sorun giderilmeye çalışılacaktır.
6. İş talebinde belirtilen telefon veya e-posta ile ulaşılamayan kullanıcıların talep istekleri 7 gün sonra kapatılır.
7. Cihazın BİDB'ye gönderilmesi ve teslim alınması kullanıcıya aittir.
8. Cihazın teknik destek personeline gönderilmeden yapılması gerekenler:

8.1. Bilgisayarınız içindeki bilgileriniz yedeklenmelidir.

8.2. Cihazınızın üzerine iş talep numarası ve ilgili destek personelini belirten bir not yazılmalıdır.
8.3. Bilgisayar veya yazıcı kurulum CD'leri cihazla birlikte yollanmalıdır.
8.4. Cihazın mesai çalışma saatleri içinde BİDB'ye getirilmesine dikkat edilmelidir.
8.5. Bilgi İşlem Daire Başkanlığı Teknik Servis Birimine teslim edilen bilgisayarın dosya sisteminde değişiklik yapılması gereken durumlarda; Bilgi İşlem Daire Başkanlığı, kullanıcı bilgilerinin yedeğinin alınmasına ilişkin kullanıcıya bilgi vermekle yükümlüdür. Kullanıcı, yedekleme işlemini gerçekleştirmediği durumlarda veri kaybından sorumludur.
8.6. BİDB, cihazın arızalı parçasının değişimini tespit ettikten sonra ilgili bölüm/birim tarafından sağlanan yedek parçanın takılmasından sorumludur. BİDB, yeni donanım ilavesi, cihazı "yükseltme" (upgrade) amaçlı olarak yedek parça desteği vermez.
8.7. Onarımı mümkün olmayan veya onarımından ekonomik olarak fayda sağlanamayacak cihazlar için, Bilgi İşlem Daire Başkanlığı Teknik Servisi Birimi tarafından hazırlanan rapor yazılı olarak kullanıcıya verilir.
8.8. Cihazın arıza tespitinden sonra yedek parça (disk, bellek, kartuş vb.) beklemesi durumunda; cihazın geri alınıp yedek parça temin edildiğinde tekrar yeni iş talebi ile BİDB'ye ulaştırılması gerekmektedir.

9. Bilgisayar ve çevre birim değişiklikleri, ilgili bölüm/birim tarafından yapılır. BİDB tarafından yazıcı, projeksiyon, monitör, tablet ve benzeri cihazlara tamir ve bakım desteği sağlanmamaktadır. İnternet bağlantıları talep doğrultusunda Ağ Birimimiz tarafından sağlanmaktadır.
10. Kullanıcıların kişisel bilgisayarlarına destek verilmemektedir.
11. Yazılımı Yükleme:

11.1. BİDB Teknik Destek Birimi tarafından üniversitemiz bünyesindeki demirbaş numaralı bilgisayarlara, dönem içinde temin edilen lisanslı yazılımlar yüklenmektedir.
11.2. Akademik ve idari personelimiz lisanslı yazılımlara kampüs genelinde lisanslı yazılımlar sunucusu üzerinden, kullanıcı adı ve şifre doğrulaması yaparak erişim hakkına sahiptir.
11.3. BİDB'nin sorumluluğu altındaki lisanslı yazılımların kurulumları yapılmaktadır.
11.4. BİDB Teknik Destek Birimi, kullanıcı bilgisayarında güvenliği tehdit edici yazılımlar tespit ettiğinde programları kaldırma hakkına sahiptir.
11.5. Kurum lisanslı yazılımları CD ve lisans anahtarları son kullanıcıya verilmez. Kurulum işlemleri teknik servis personeli tarafından gerçekleştirilir.

12. Kullanıcı Sorumlulukları:
12.1. Akademik ve idari personelin bilgisayarına yüklediği programların lisans sorumluluğu (üniversitemizin yasal olarak satın aldığı lisanslı programlar hariç) ilgili personele aittir.
12.2. Kullanıcı, bilgisayarındaki işletim sisteminin ve işletim sistemi üzerinde çalışan yazılımların güvenlik tehditlerine karşı korunabilmesi için en son güncellemeleri yapmakla yükümlüdür. Kullanıcı, bilgisayarında mutlaka BİDB tarafından lisanslı olarak temin edilen antivirüs programının yüklü olmasına dikkat etmelidir. Antivirüs yazılımı yüklü olmayan bilgisayarların tespit edilmesi halinde, programı yüklemeyen kullanıcının internet erişimi kesilir.
12.3. Kullanıcı bilgisayarında BİDB tarafından temin edilen antivirüs yazılımı mutlaka kurulu olmalıdır. Lisanslı yazılımlar dışında şüphe uyandırıcı yazılımlarla karşılaşıldığında BİDB Teknik servis Takip Programı üzerinden kayıt açılması gerekmektedir.
12.4. Kullanıcı bilgisayarına, kullanıcı adı ve şifresi ile girmesi bilgilerinin korunması açısından önem taşımaktadır. Kullanıcı şifrelerini rakam, harf veya özel karakterlerden oluşturması gerekmektedir.
12.5. Güvenli olmayan sitelere girilmesi kullanıcı güvenliği açısından sakıncalıdır.

12.6. Kullanıcı kendi bilgisayarındaki bilgilerin yedeğini almaktan sorumludur.

12.7. Bilgisayar kasaları, yazıcılar yere konmamalı; masa üzerine veya bilgisayar masalarının özel yerleri içinde kullanılmalıdır.

12.8. Cihazlar, direkt güneş ışığına maruz bırakılmamalı, kalorifer üzerine konmamalıdır. Toz ve nemden korunmalıdır.

12.9. Cihazların temizliği haftada bir nemli bir bezle yapılmalıdır.

12.10. Cihazların bağlanacakları elektrik prizlerinin topraklı priz olmasına dikkat edilmelidir. Varsa kesintisiz güç kaynağı (UPS) hattı kullanılmalıdır.

12.11. Cihazın bağlı olduğu elektrik ve internet hattı kablolarının ezilmemesi için kanal içinden geçmesi sağlanmalıdır.

M. WEB HİZMETLERİ POLİTİKALARI

Amaç: Bu politika ile GTÜ'nün web sayfasının, GTÜ vizyon, misyon ve hedefleri doğrultusunda tanıtım, bilgilendirme ve portal hizmetlerini belirli standartlarda sağlaması amaçlanır. Bu doğrultuda kullanıcıların aşağıdaki politikalara uyması beklenir:

1. GTÜ web sayfası kurumsal renk ve tasarımı Rektörlük tarafından belirlenir.
2. Web tasarımı tüm sitede belirli düzen ve şablonları korumalıdır.
3. Web içerik yönetimi, her bir bölüm veya birim için yetkilendirilmiş personel tarafından gerçekleştirilir.
4. BİDB içerik girişi için görevlendirilmiş personele eğitim ve destek sağlar.
5. Web içeriklerinden birim amirleri sorumludur.
6. GTÜ web ana sayfa içeriğinden Basın ve Halkla İlişkiler Birimi sorumlu olup içerik için Rektörlük onayı alınmalıdır.
7. Web içeriği, giriş personelinin yapamadığı altyapı ve ekstra sayfa içerikleri için BİDB Web ve Yazılım Birimi destek verir.
8. GTÜ içerisinde yapılan etkinliklere ait web sayfaları için resmî yazı ile BİDB başvuru yapılır. BİDB gerekli altyapıyı, kurulumu yapıp içerik yönetimini etkinlik yöneticisine devreder.
9. GTÜ alan adları talepleri için resmî yazı ile BİDB'ye başvuru yapılır. Uygun görülmesi halinde alt alan adları tanımlanır. Kişisel sayfalar ve içerikler için alan adı tanımlaması yapılmaz.

N. YAZILIM GELİŞTİRME POLİTİKALARI

Amaç: Yazılım Geliştirme üzerindeki denetimler (analiz, tasarım, kodlama, test ve bakım), GTÜ'nün günlük operasyonlarını yürütmek için kullandıkları yazılımların oluşturulması esnasında kullanılan denetim mekanizmalarıdır. Programların geliştirilmesi esnasında uygulanması gereken bu denetimler, yazılımların denetimli bir şekilde geliştirilmesini sağlamayı hedeflemektedir. Bu şekilde güvenlik ölçütlerinin hem yazılımın geliştirilmesi aşamasında hem de geliştirilen yazılım uygulamaya alındıktan sonra gözetilmesi sağlanır. Bu politika yazılım geliştirme hakkındaki ölçütleri ortaya koymaktadır.

Kapsam: Bu politika GTÜ BİD Başkanlığı yazılım geliştirme alanındaki faaliyetlerini kapsamaktadır.

Politika: Yazılım geliştirme üzerindeki denetimler şu temel ölçütlere uygun şekilde oluşturulmalıdır.

1. Sistem yazılımında mevcut olan denetimler, kullanılacak yeni bir yazılım veya mevcut sistem yazılımına yapılacak olan güncellemeler ile etkisiz hale getirilmemelidir.
2. BİDB sadece uygun yazılım projelerinin başlatıldığından ve proje alt yapısının uygun olduğundan emin olmalıdır.
3. GTÜ'nün yazılım gereksinimleri, uygun bir şekilde tanımlanmalıdır.
4. Sistem geliştirmede, ihtiyaç analizi fizibilite çalışması, tasarım, geliştirme, test ve onaylama safhalarını içeren bir yöntem kullanılmalıdır.

5. BİDB tarafından geliştirilmiş yazılımlar ve seçilen paket sistemler ihtiyaçları karşılamalıdır.
6. GTÜ içerisinde kişisel olarak geliştirilmiş yazılımların kullanılması kısıtlanmalıdır.
7. Hazırlanan yazılımlar mevcut metotlar dâhilinde, işin ve iç denetim gerekliliklerini yerine getirdiklerinden emin olunması açısından test edilir, yapılan testler ve test sonuçları belgelenerek onaylanır.
8. Yeni alınmış veya revize edilmiş bütün yazılımlar test edilmeli ve onaylanmalıdır.
9. Eski otomasyon sistemlerdeki veriler tamamen, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılmalıdır.
10. Uygulama ortamına aktarılma kararı uygun bilgilere dayalı olarak BİDB tarafından verilir.
11. Yeni yazılımların dağıtımı ve uygulanması BİDB tarafından denetim altında tutulur.
12. Yazılımlar sınıflandırılır/ etiketlenir ve envanterleri çıkarılarak bir yazılım kütüğünde muhafaza edilmelidir.

O. YÜRÜRLÜKTEN KALDIRILAN MEVZUAT

Bu yönergenin yürürlüğe girdiği tarihten itibaren GTÜ Senatosunun 14.02.2019 tarih ve 2019/03 oturum sayılı kararı ile kabul edilen Gebze Teknik Üniversitesi Bilişim Politikaları Yönergesi yürürlükten kalkar.

Ö. YÜRÜRLÜK

Bu senato onay tarihinden itibaren yürürlüğe girer.

P. YÜRÜTME

Bu yönerge hükümlerini GTÜ Rektörü yürütür.

Yönergenin Kabul Edildiği Senato Kararının	
Tarih	**Sayısı**
07.04.2023	2023/09