1. AMAÇ:

Bilgi Güvenliği Yönetim Sistemi (BGYS) Politikalarının amacı; Bartın Üniversitesi çalışanlarının, sistemlerinin, bilgi ve varlıklarının; gizlilik, bütünlük ve erişilebilirlik bakımından yapılması, uyulması gereken iş kurallarını hedeflemek ve bu hedefler kapsamında iş sürekliliğini sağlamaktır.

Kurumun amacı herhangi kimse üzerinde kısıtlayıcı politikalar üretmek değil aksine açıklık, güven ve bütünlüğe yönelik kültürü yerleştirmektir. Kurum bilerek / bilmeyerek yapılan, yasadışı veya zararlı eylemlere karşı çalışanın ve kurumun haklarını koruma altına almaktadır. Bilgi teknolojileri ile alakalı sistemler kurumun sahip olduğu değerlerdir. Güçlü bir bilgi güvenliği bütün çalışanların dâhil olduğu takım çalışmasıyla gerçekleştirilir. Bilgi güvenliğinin sağlanabilmesi için bütün personelin bilgi güvenliği politikalarını iyi bilmesi ve uygulamanın sorumluluğunu taşıyabilmesi gerekmektedir.

2. KAPSAM:

Bilgi Güvenliği Yönetim Sistemi dâhilinde yapılan işlemler.

3. YAPTIRIM:

Bu politikalara uygun olarak hareket etmeyen çalışanlar hakkında iş kanunlarının ilgili hükümleri veya iş kanunları, 657 sayılı Devlet Memurları Kanunu, 2547 sayılı Yükseköğretim Kanunu, 2914 Sayılı Yüksek Öğrenim Personel Kanunu, Yükseköğretim Kurumları Disiplin Yönetmeliği, Yükseköğretim Kurumları Öğrenci Disiplin Yönetmeliklerinin ilgili hükümleri uygulanacak olup yine bu konularda hüküm bulunmayan hallerde ilgili mevzuat hükümleri uygulanacaktır. Öğrenciler için Yükseköğretim Kurumları Öğrenci Disiplin Yönetmeliği'nin ilgili hükümleri uygulanacak olup yine bu konularda hüküm bulunmayan hallerde de ilgili mevzuat hükümleri uygulanacaktır. Tedarikçi ve ziyaretçiler için ise ilgili mevzuat hükümleri uygulanarak yasal süreç başlatılacaktır.

4. SORUMLULAR:

BGYS politikalarının, gözden geçirilmesi ve güncellenmesinden Rektörlük Makamı Onayı ile oluşturulan Bilgi Güvenliği Ekibi sorumludur. Üniversite Senatosu tarafından Bilgi Güvenliği Politikası onaylanır ve duyurulması sağlanır. Bu politikalardan bütün çalışanlar, öğrenciler, tedarikçiler ve ziyaretçiler sorumludur.

5. İLGİLİ DOKÜMANLAR:

6. UYGULAMA:

6.1 POLİTİKA LİSTESİ

P01 İnternet Erişim Politikası

P02 E-Posta Politikası

P03 Anti-Virüs Politikası

P04 Şifre Politikası

P05 Fiziksel Güvenlik Politikası

P06 Sunucu Güvenlik Politikası

P07 Ağ Yönetimi Politikası

P08 Uzak Bağlantı Politikası

P09 3. Taraf Güvenlik Politikası

P10 Kabul Edilebilir Kullanım Politikası

P11 Temiz Masa Temiz Ekran Politikası

P12 Mobil Cihaz Politikası

P13 Veri Tabanı Güvenlik Politikası

P14 Yazılım Temini ve Geliştirme Politikası

P15 Değişim Yönetimi Politikası

P16 Olay Yönetim Politikası

P17 Kripto Grafik Kontroller Politikası

P18 Kamera Politikası

P19 Yedekleme Politikası

P20 Web Tahsisi Politikası

6.2 BİLGİ GÜVENLİĞİ UYGULAMA POLİTİKALARI

P01 İNTERNET ERİŞİM POLİTİKASI

1. Amaç

Kurum içinde güvenli internet erişimi için sahip olması gereken standartların uygulanmasını amaçlamaktadır. İnternetin uygun olmayan kullanımı; kurumun yasal yükümlülükleri, kapasite kullanımı ve kurumsal imajı açısından istenmeyen sonuçlara neden olabilir. Bu tür olumsuzlukların gerçekleşmemesi için etik ve yasalar çerçevesinde internet kullanım kurallarını belirlemektir.

2. Kapsam

Bu politika kurum internetini kullanan çalışanları, öğrencileri, tedarikçileri ve ziyaretçileri kapsamaktadır.

3. Politika

- Kurum ağlarına bağlı bütün bilgisayarlar içerik denetimi yapan bir uygulama üzerinden internete çıkacaktır. Üniversite bünyesinde Eğitim, Öğretim, idari, akademik amaçlara ve yasalara uygun olmayan tüm siteler yasaklıdır. Ancak yetkilendirilmiş sistem yöneticileri ve kişiler internete çıkarken bütün servisleri kullanma hakkına sahiptir.

- 5651 sayılı kanun (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun) gereği kurum internet erişim kayıtları en az 24 ay arşivlenmektedir.

- Bilgisayarlar üzerinden yasalara aykırı internet sitelerine girmek ve dosya (film, müzik, program vb.) indirmek yasaktır.

- Vpn dışındaki diğer tüm Tunnel platformları, proxy ve dns değişiklikleri yapılarak internete bağlanılması yasaktır.

- Başkalarının fikri haklarını ihlal edici mahiyette (copyright) materyalin (yazı, makale, kitap, film, müzik eserleri vb.) dağıtımı yasaktır.

- Sistem ve ağ güvenliğinin ihlal edilmesi yasaktır, cezai ve hukuki mesuliyetle sonuçlanabilir. Kurum bu tür ihlallerin söz konusu olduğu durumları inceler ve eğer bir suç oluştuğundan şüphe duyulursa iş kanunları, 657 sayılı Devlet Memurları Kanunu, 2547 sayılı Yükseköğretim Kanunu, 2914 Sayılı Yüksek Öğrenim Personel Kanunu, Yükseköğretim Kurumları Disiplin Yönetmeliği, Yükseköğretim Kurumları Öğrenci Disiplin Yönetmeliklerinin ilgili hükümlerini uygulayabilir veya yasa uygulayıcısı ile işbirliği yapabilir.

- İnternet üzerinden kullanım amaçlarına uygunsuz, müstehcen, rahatsız edici materyaller ile kuruma ve kurumun çalışanlarına, bunların aile fertlerine veya Türkiye Cumhuriyeti Devletine, ulusuna, yasama, yürütme ve yargı organlarına, askeri ve emniyet teşkilatına, vatandaşlarına yönelik iftira, karalama mahiyetinde mesajlar yayınlamak ve paylaşmak yasaktır.

- Kullanıcıların internet üzerinden görevleri ile ilgisi bulunmayan, internet trafiğini kısıtlayabilecek, zarar verebilecek, etik olmayan veya yasalara uygun olmayan çevrimiçi olarak yayın yapan televizyon, radyo, film, oyun vb. içerikli yayınların kullanılması yasaktır.

- Kullanıcıların internet üzerinden görevleri ile ilgisi bulunmayan, Üniversitenin kurumsal imajını zedeleyici ve yasalarla da yasaklı bulunan site ve forum vb. gibi sayfalara e-posta adresleri üye olması yasaktır.

- Kullanıcıların kurum hesaplarına ait kullanıcı adı ve şifreleri internet üzerinden paylaşması yasaktır.

- Kullanıcıların kurum internet ağı üzerinden yaptığı kişisel işlemlerde (banka, alışveriş, e-posta vb.) oluşacak olumsuzluklardan kurum sorumlu değildir, bu tür sebepler ile kurum veya kişisel hesabının bir başkasının eline geçmesine sebep olunması ve bu durumda gerçekleştirilebilecek muhtemel suçlardan kişi mesuldür.

- İnternette gezinirken reklam veya bilgi çalmak amaçlı (tebrikler, ödül kazandınız, ödülünüzü almak için tıklayın vb.) aldatıcı resim ve yazılara karşı dikkatli olunmalı ve tıklanmamalıdır.

P02 E-POSTA POLİTİKASI

1. Amaç

Kurumsal e-postaların standartlara uygun, kesintisiz kullanım ve güvenliğinin sağlanması amaçlanmaktadır.

2. Kapsam

Bu politika kurum e-postasını kullanan çalışanları, öğrencileri, tedarikçileri kapsamaktadır.

3. Politika

- Kullanıcıların kurum e-postalarından gönderdikleri, aldıkları veya sakladıkları e-postalar Bartın Üniversitesi'nin bilgi varlığıdır. Bu nedenle Bilgi İşlem Daire Başkanlığı kurumsal e-postaları adli mercilerin istemesi ya da mahkeme kararı olması durumlarında haber vermeksizin denetleyebilir ve yasa uygulayıcıları ile paylaşabilir.
- Bartın Üniversitesi, kurum ile ilişiği kesilmesi durumunda kullanıcıların kurumsal e-postalarına erişimini engeller ve kullanıcılar ile e-posta yedeklerini paylaşma zorunluluğu yoktur.
- İlişiği kesilen kullanıcıların e-posta hesapları devre dışı bırakılır, e-postalarına erişimleri engellenir. Mahkeme kararı ile ilgili hesaplara erişim talebi yapılması durumunda, e-postalar ilgili kişi/kurum ile paylaşılabilir.
- Bartın Üniversitesi ile ilgili Gizli/Kritik verileri içeren bilgiler elektronik posta, internet dosya paylaşım siteleri, paylaşım yazılımları ile tutulamaz ve gönderilemez.
- Bartın Üniversitesi'nin e-posta gruplarına, kişisel kullanım amaçlı e-posta gönderilmesi yasaktır.
- Kurumsal e-posta, yasadışı, taciz, su istimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik, spam, sahte, zincir e-posta ve bu e-postalara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postaların gönderilmesi için kesinlikle kullanılamaz. Bu tür özelliklere sahip bir e-posta alındığında hemen Bilgi İşlem Daire Başkanlığı'na veya Bilgi Güvenliği Ekibi'ne haber verilmesi ve yetkili kişiler müdahale edene kadar e-postanın silinmemesi, cevaplanmaması, iletilmemesi ve içeriğine tıklanmaması gerekmektedir.
- E-posta gönderen çalışan, e-posta içeriğini dikkate alarak, sadece ilgili kişilere göndermelidir. E-posta gönderilmeden önce "kime" ve "bilgi" bölümlerine eklenen kişi listesi kontrol edilmelidir.
- Kullanıcılar, e-posta ile istenen mail içeriğinde kullanıcı adı ve şifre paylaşmamalıdır. Kullanıcı adı ve şifre talep edilen e-postalar alındığında hemen Bilgi İşlem Daire Başkanlığı'na veya Bilgi Güvenliği

Ekibi'ne haber verilmeli ve yetkili kişiler müdahale edene kadar e-posta silinmemeli, cevaplanmamalı, iletilmemeli ve içeriğine tıklanmamalıdır.

- Kullanıcıların; kurumsal e-posta ile uygun olmayan içeriklere sahip e-posta (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyeti ihlal eden ve hakaret içeren vb.) göndermeleri yasaktır.

- Kurum akademik, idari ve sözleşmeli personeline e-posta hesabı açılması için personelin, http://bim.bartın.edu.tr adresindeki formlar kısmında PERSONEL ELEKTRONİK POSTA İSTEK/ŞİFRE DEĞİŞİKLİĞİ FORMU doldurması ve üst yazı ile imzalı bir şekilde Bilgi İşlem Daire Başkanlığı'na ulaştırması gerekmektedir.

- Üniversitede faaliyet gösteren fakülte, enstitü, yüksekokul, meslek yüksekokulu; bölüm, başkanlık, müdürlük, koordinatörlük, müşavirlik, anabilim dalı, sempozyum vs. gibi bütün kurumsal noktalara e-posta adresi tanımlanabilmesi için Bilgi İşlem Daire Başkanlığı'na mail yoluyla iletilmelidir.

- Kurumsal e-postalar için görevlendirmesi yapılan personelin birimi ile ilgisi kalmadığı durumda yeni görevlendirilen personelin yazısı UBYS tarafından kontrol edilerek işlem yapılmaktadır.

- Kullanıcı, gizli mail içeriğini ilgisi bulunmayan kişilere göstermeyeceğini, hizmet hakkının sadece kendisine ait olduğunu, bu hakkın kullanımına ilişkin özel ve gizli şifresini ve kullanıcı adını ve/veya kodunu başkasına kullandırmayacağını ve devretmeyeceğini, başkası tarafından öğrenilme şüphesi dahi olsa derhal değiştireceğini, aksi takdirde yapılan bütün işlemlerin sorumluluğunun kendine ait olacağını, kendisi kullanmadığı iddiası ile sorumluluktan kurtulamayacağını kabul eder.

- Bartın Üniversitesi personelinin, kurum kimliği altında sürdürülen bütün faaliyetler için kuruma ait elektronik posta adresine sahip olması ve ilgili yazışmalar için "@Bartın.edu.tr" uzantılı e-posta hesabını kullanması gerekir.

- Kullanıcı, hesabında ve/veya sitesinde ticari reklamlara ve üyelik ile sağlanan yerli/yabancı destekleyici (sponsor) reklamlarına, bağlantılarına yer veremez. Ticari reklamlar ve haber duyuruları gibi istenmeyen mesajlar gönderemez.

- Kullanıcı şifresi sadece kullanıcı tarafından bilinir. Kullanıcı ilk kullanımdan itibaren parolasını değiştirmek zorundadır. Şifrenin seçimi ve korunması tamamıyla kullanıcının sorumluluğundadır. Şifre unutulduğu takdirde http://bim.bartin.edu.tr adresindeki formlar kısmında Akademik ve İdari PERSONEL ELEKTRONİK POSTA İSTEK/ŞİFRE DEĞİŞİKLİĞİ FORMU doldurması ve üst yazı ile imzalı bir şekilde Bilgi İşlem Daire Başkanlığı'na ulaştırması gerekmektedir.

- Kullanıcı hesabı;
  - T.C. yasalarının belirlediği yasadışı kullanımlarda,
  - Bartın Üniversitesi tarafından belirlenen kullanım politikalarına uyulmadığı durumlarda,

- Kullanıcı hesapları için belirlenen sınırların aşıldığı durumlarda,
- Bartın Üniversitesi bilişim kaynaklarının akademik amaçlı çalışmaları engelleyici biçimde akademik amaçlı olmayan, ticari ve yasadışı amaçlı kullanıldığı durumlarda,
- Kişilere ait kullanıcı hesaplarının farklı kişiler tarafından kullanımının tespit edildiği durumlarda,
- Sunucu sistemler üzerinde tanımlı diğer kullanıcıların şifrelerini bulmaya çalışmak, dosyalarına müdahale etmek, değiştirmek vb. girişimlerin tespit edildiği durumlarda,
- Sistem doğruluğunun, bütünlüğünün, güvenliğinin ve servis devamlılığının engellendiği durumlarda,

Kullanıcıya haber verilmeksizin Bilgi İşlem Daire Başkanlığı tarafından geçici olarak kapatılabilir. Kullanıcı hesabının kalıcı olarak kapatılacağı durumlarda kullanıcılar önceden bilgilendirilir.

P03 ANTİ-VİRÜS POLİTİKASI

1. Amaç

Bilgisayar ve sunucuların zararlı yazılımlardan korunması amaçlanmaktadır.

2. Kapsam

Bu politika bütün bilgisayarları ve sunucuları kapsamaktadır.

3. Politika

- Kurumun bütün bilgisayarları ve sunucuları Anti-virüs yazılımına sahip olacaktır.
- Hiç bir kullanıcı herhangi bir sebepten dolayı Anti-virüs programını sistemden kaldıramaz veya durduramaz.
- Anti-virüs yazılımı düzenli aralıklar ile otomatik olarak güncellenecektir.
- Anti-virüs yazılımı anlık olarak bilgisayar ve sunucularda virüs taraması yapacaktır.
- Virüs bulaşan makineler tam olarak temizleninceye kadar ağa bağlanmayacaktır. Bilgisayarlarda virüs olduğu uyarısı alındığında veya şüpheli durumlarda hemen Bilgi İşlem Daire Başkanlığı'na veya Bilgi Güvenliği Ekibine haber verilmeli ve yetkili kişiler müdahale edene kadar bilgisayarın kullanılmaması gerekmektedir.
- İnternet üzerinden bilinmeyen ve şüpheli kaynaklardan indirilen dosyaların içerisinde virüs olabilir, bu tür kaynaklardan dosya indirilmesi yasaktır.
- Bilgisayarlarda kullanılacak CD, DVD, USB gibi depolama aygıtlarını ve internet üzerinden indirilen dosyaları virüs taraması yapmadan kullanmak yasaktır.
- Bilgi İşlem Daire Başkanlığı'nın hazırlamış olduğu bilgisayarlar güncellemeleri yapılmış anti virüs yazılımı yüklenmiş şekilde kurum ağına dâhil edilir.

P04 ŞİFRE POLİTİKASI

1. Amaç

Bilgi Güvenliğinin arttırılması için güçlü bir şifreleme oluşturulması ve şifrelerin güvenliğinin sağlanması amaçlanmaktadır.

2. Kapsam

Bilgisayar, sunucu, uygulama ve epostaları kullanan bütün kullanıcı hesaplarını kapsamaktadır.

3. Politika

- Bilgisayar kullanıcı hesaplarının şifreleri en az 10 karakter ve karmaşık şekilde büyük harf, küçük harf, rakam ve özel karakter (\ * ? - = / _ + % & vb.) kullanılması zorunludur.
- Şifreleme bilgisayar güvenliği için önemli bir özelliktir. Kolay tahmin edilen (Aa123456, Ab123456, Qaz12345, Asd12345, memleket, çocuk, çalışanın kendi ismi, doğum tarihi, ardışık rakam ve harfler, İstanbul, Bartın vb.) şifreler kullanılması yasaktır.
- Kurum içerisinde kullanılan bilgisayar, uygulama ve eposta hesap şifrelerinin yılda bir değiştirilmesi zorunludur.
- Kurum içerisinde kullanılan sunucu hesap şifrelerinin yılda en az 1 kez değiştirilmesi zorunludur.
- Bilgisayarlar ve sunucularda işlem yapılmadığı sürece otomatik olarak 5 dakika sonrasında şifreli ekran koruması devreye girecektir.
- Bilgi İşlem Daire Başkanlığı tarafından oluşturulan yeni şifrelerin ilk kullanımdan itibaren değiştirilmesi zorunludur.
- Kurumsal uygulamalarda üst üste 5 kez hatalı şifre girildiğinde kullanıcı hesabı kilitlenecektir, bu gibi durumlarda Bilgi İşlem Daire Başkanlığı ile iletişime geçilmesi gerekmektedir.
- Kurumsal hesaplara ait şifrelerin herhangi bir kimseyle (iş arkadaşları, aile bireyleri vb.) paylaşılması yasaktır.
- Kurumsal hesaplara ait şifreleri kâğıt veya elektronik ortamlara (e-posta, word, excel, forum siteleri vb.) yazılması ve paylaşılması yasaktır.
- Sistem yöneticileri kendi kullanıcı adı ve şifreleri ile sunuculara bağlanmalıdır, yerel yönetici (local admin) hesaplarının kullanılması yasaktır.
- Kullanıcı hesaplarına ait şifreler Bilgi İşlem Daire Başkanlığı tarafından kayıt altında tutulmamaktadır. Kullanıcıların bilgisayarlarında oturum açma işlemleri, şifre değişiklikleri ve Bilgi

İşlem Daire Başkanlığı tarafından yapılan şifre değişiklik kayıtları (değiştirme ve oturum açma zamanı, bilgisayar ip adresi ve adı) sistemler üzerinde 24 ay süreyle saklanmaktadır.

- Kurum içinde kullanılan diğer uygulamaların (Yönetim programları, Firewall, Mail Gateway, UBYS vb.) şifreleri de Şifre Politikasına uygun olarak tanımlanacaktır.
- Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de Şifre Politikasına uygun olarak hazırlanacaktır.

P05 FİZİKSEL GÜVENLİK POLİTİKASI

1. Amaç

Kurumun bilgi varlıkları, ekipmanları ve alt yapı cihazlarının fiziksel güvenliği ve yetkisiz erişimlerinin önlenmesi amaçlanmaktadır.

2. Kapsam

Kurumun bilgi varlıkları, ekipmanları ve alt yapı cihazlarını kullananları kapsamaktadır.

3. Politika

- Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binada ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanacak ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilecektir.
- Bartın Üniversitesi'ne girişler ve koridorlar güvenlik açısından kamera ile kayıt altına alınarak izlenmektedir. Kamera kayıtları en az 30 gün saklanmaktadır.
- Açık ofislerde ve odalarda bulunan gizli bilgi varlıklarının olduğu dolaplar ve çekmeceler kilitli ve kontrol altında tutulacaktır.
- Kurumun bilgi varlıkları, bilgisayar ve çevre birimleri (harici diskler, yazıcı, monitör, projeksiyon vb.), alt yapı cihazlarını hasar / hırsızlık gibi oluşabilecek risklere karşı önlem almak ve güvenliği açısından uyarı yazıları yazmak kişi ve birimin kendi sorumluluğundadır.
- Kritik bilgi varlıkları ve altyapı cihazları kilitli odalarda ve kabinetlerde muhafaza edilecektir.
- Erişim yetkisi verilerek girilen alanların erişim yetkileri düzenli aralıklar ile kontrol edilecektir.

P06 SUNUCU GÜVENLİK POLİTİKASI

1. Amaç

Kurumun sahip olduğu sunucuların temel güvenlik kurallarını oluşturmayı amaçlamaktadır.

2. Kapsam

Bu politika kurumun sahip olduğu bütün sunucuları kapsamaktadır.

3. Politika

- Kurum bünyesindeki bütün sunucuların yönetiminden sadece yetkilendirilmiş sistem yöneticileri sorumludur.
- Bütün sunuculara Bilgi İşlem Daire Başkanlığı'nın yetkilendirdiği kişiler dışında erişim yapılması yasaktır.
- Kullanılmayan sunucular güvenlik, performans ve elektrik tasarrufu açısından kapalı tutulacaktır.
- Sunucuların, işletim sistemi, uygulamalar, veri tabanları ve ağ ekipmanlarının erişim logları ilgili cihazlarda en az 24 ay saklanacaktır.
- Sunucuların kaynakları (cpu, ram, disk, ağ trafiği vb.) düzenli olarak kontrol edilecektir.
- Sunucuların yönetimi için her kullanıcı kendi hesabı ile bağlantı yapacaktır. Sunuculara dışarıdan yapılan bağlantılar Uzak Bağlantı Politikasının belirlediği kurallara göre gerçekleştirilecektir.
- Sunucular fiziksel olarak güvenlik önlemi alınmış sistem odalarında bulundurulacaktır.
- Sistem odaları sıcaklık, nem değerleri ve su basmasına karşı denetlenecektir.
- Sistem odası sıcaklık derecesi tavsiye edilen (22-25 ^{0}C) seviyede tutulacak şekilde soğutulacaktır.
- Sistem odalarına giriş ve çıkışlar erişim kontrolü olacak ve kayıt altına alınacaktır.
- Sistem odalarındaki ekipmanların bakımları düzenli olarak yapılacak ve bakım kayıtları tutulacaktır.
- Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunacaktır, yangın ve benzer felaketlere karşı koruma altına alınacaktır.
- Sunucularda anti-virüs programı yüklü olacak ve anlık olarak tarama yapacaktır.

P07 AĞ YÖNETİMİ POLİTİKASI

1. Amaç

Kurumun bilgi teknolojileri ağında yer alan bilgilerin, ağ alt yapısının ve ekipmanlarının güvenliğini ve sürekliliğini sağlamayı amaçlamaktadır.

2. Kapsam

Kurum bünyesindeki ağ altyapısı, donanım ve kullanıcıları kapsamaktadır.

3. Politika

- Üniversitenin ağ alt yapısındaki, donanımı ve yazılımı zarara uğratan, tahrip edici, zedeleyici ve sağlıklı çalışmasını engelleyici hiçbir girişimde bulunulmaması; kaynakların verimli kullanılması en temel ilkedir.
- Üniversitenin ağ hizmetleri Türkiye Cumhuriyeti yasalarına ve Üniversite yönetmelikleri başta olmak üzere yasalara bağlı olan yönetmeliklere aykırı faaliyetlerde bulunmak amacıyla kullanılamaz.
- Üniversitenin ağ hizmetleri akademik ve idari işlemlerin görülmesi amacıyla verilmektedir. Diğer kullanımlar, ancak bu kullanım gereksinimleri karşılandıktan sonra arta kalan zaman ve kapasite boyutlarında gerçekleştirilebilir.
- Üniversitenin ağ alt yapısı ve bilgisayar ağı üzerinde yer aldığı Ulusal Akademik Ağ (ULAKNET) ve diğer ulusal ve uluslararası ağların kullanım politikalarına, bilişim kaynaklarını kullanan bütün birimlerin ve bütün kullanıcıların uyma ve bu bağlamda gerekli önlemleri alma zorunluluğu vardır.
- Ağ ekipmanları Bilgi İşlem Daire Başkanlığının yetkilendirdiği kişiler tarafından erişilebilecek ve yönetilebilecektir. Kurum ağına ve ağ ekipmanlarına yetkisiz erişim yasaktır.
- Kurum ağı, sadece kurum bilgisayarları, ağ ekipmanları ve mobil cihazlar bağlanacak şekilde yönetilmektedir. Kuruma ait olmayan bilgisayar veya mobil cihazlar kablosuz olarak (BU_Misafir) ayrı bir ağ üzerinden bağlanacaktır.
- Misafirler için özel misafir ağı, kurum ağından bağımsız özel kablosuz internet hattı oluşturulmuştur. Misafirler bu ağı kullanırken İnternet Erişimi Politikasına uygun hareket edecektir.
- Misafirler için Misafir Kullanıcı İnternet İstek Formu doldurulup Bilgi İşlem Daire Başkanlığı'na teslim edilecektir.
- Bilgi teknolojileri ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için yedek ağ ekipmanları bulundurulacaktır.
- Ağ cihazlarının konfigürasyonları düzenli olarak ağ takip programı üzerinden yedeklenecektir.

- Uzaktan bağlantı için kullanılacak portların güvenliği sağlanacaktır.
- Ağ cihazları yılda en az 1 defa açıklık (sızma) tarama testlerinden geçirilerek zafiyetler tespit edilecek ve gerekli tedbirler alınarak güvenli hale getirilecektir.
- Kurumun bilgi teknolojileri ağı detaylı olarak takip (monitoring) ve analiz edilecektir.
- Kabin yerleri, birimlerdeki ağ alt yapısı kurulurken, internet erişiminin en verimli şekilde kullanılması, ağ alt yapısı masraflarını ve kablo mesafelerine bağlı olarak veri kayıplarının en aza indirgenmesi dikkate alınarak belirlenir. Üniversite internet kullanıcıları kabin ve kabin odalarıyla ilgili aşağıdaki kurallara uymak zorundadır.
- Bilgi İşlem Daire Başkanlığı çalışanlarının haricinde hiçbir kullanıcı kabin içerisine müdahalede bulunamaz.
- Kabinleri besleyen elektrik prizlerine, sigortalara ve kesintisiz güç kaynağına müdahalede bulunamaz.
- Kabinlerin üzerine eşya, yakınına sıvı maddeler konulması ve kabinin güvenliğini bozacak her türlü durum için ortaya çıkabilecek sorunlardan ilgili birim, fakülte, enstitü, yüksekokul veya meslek yüksekokulu sekreterliği sorumludur.
- Kabin yerleri, birimlerdeki ağ alt yapısı kurulurken, internet erişiminin en verimli şekilde kullanılması, ağ alt yapısı masraflarını ve kablo mesafelerine bağlı olarak veri kayıplarının en aza indirgenmesi dikkate alınarak belirlenir.
- Üniversitenin ağ hizmetleri kaynaklarının herhangi bir amaçla kullanım hakkı, Bilgi İşlem Daire Başkanlığı ve Rektörlük Makamı tarafından onay verilmeden üçüncü özel veya tüzel kişilere verilemez.
- Bilgi İşlem Daire Başkanlığının bilgisi dışında ağ kurmak, aktif-pasif cihazları ağa eklemek veya kablosuz yayın yapmak kesinlikle yasaktır.
- Üniversitede kablosuz ağ kullanıcıları, ağ üzerinde kendilerine verilen kullanıcı yetkisini ve kullanıcı kodunu, şifresini kullanarak bu kaynaklar üzerinde gerçekleştirdikleri çalışmalar ve etkinlikler ile bu kaynaklar üzerinde bulundurdukları veya oluşturdukları bilgi, belge, yazılım gibi her türlü kaynağın içeriğinden ve kullandıkları kaynakların kullanım kurallarına uyulmasından şahsen sorumludur.
- Bilgi İşlem Daire Başkanlığının sağladığı güvenlik çözümleri haricinde kullanılan kişisel güvenlik çözümlerinin kullanılmasıyla birlikte oluşacak sorunlardan kişi kendisi sorumludur.
- Veri kablosu, sonlandırma ve aktarma işlemlerinde kullanılan bütün bileşenlerin (patch panel, veri prizi, patch ve drop kablolar vs.) uluslararası kablolama standartlarına uygun olarak kullanılması zorunludur.

- Kampüs içinde ve binalar arasında dolaşan fiber optik (F/O) hattının zarar görmemesi için gerekli önlemleri almak ve bu fiber ağının geçtiği yerlerde yapılan inşaat, kazı ve diğer faaliyetleri denetlemek ve oluşabilecek sorunların tamir onarımını yapmak Bilgi İşlem Daire Başkanlığının sorumluluğunda değildir.
- Cihazların ve bu cihaza bağlı ekipmanların fiziki sorumlulukları, cihazın bulunduğu yerin (bina, kat laboratuvar vs.) birim amiri ve birim amirinin belirlemiş olduğu oda ve kabin sorumlusuna aittir.

P08 UZAK BAĞLANTI POLİTİKASI

1. Amaç

Kurumun bilgi teknolojileri sistemlerine dışarıdan yapılacak olan uzak bağlantıların güvenliğinin sağlanması amaçlanmaktadır.

2. Kapsam

Bu politika bilgi teknolojileri sistemlerine dışarıdan bağlantı yapacak bütün kurum çalışanlarını ve paydaşlarını kapsamaktadır.

3. Politika

- Uzaktan bağlantı sadece SSL VPN ile yapılmaktadır.
- Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya paydaşlar yerel ağdaki kullanıcılar ile eşit sorumluluklara sahip olacaktır.
- VPN kullanım hakkı verilen kişiler listelenecek ve en az yılda 1 kez düzenli olarak kontrol edilecektir.
- VPN kullanım hakkı verilen kişilerin kullanıcı hesap bilgilerini başkalarıyla paylaşması yasaktır.
- Kurum bilgisayarları haricinde VPN bağlantısı yapılacak cihazlarda anti-virüs yazılımları kurulu ve güncel olmak zorundadır.
- Kurum gerekli gördüğü durumlarda herhangi bir uyarıda bulunmadan VPN bağlantı erişimlerini kesme hakkına sahiptir.

P09 3. TARAF GÜVENLİK POLİTİKASI

1. Amaç

Kurumun bilgi teknolojilerine ve bilgi varlıklarına üçüncü taraflar tarafından ulaşılması durumunda güvenliğinin sağlanması amaçlanmaktadır.

2. Kapsam

Bu politika bütün Üniversite birimleri/çalışanları ve paydaşları (tedarikçiler, müşteriler, ziyaretçiler, bakım firmaları vb.) kapsamaktadır.

3. Politika

- Kurum paydaşları ile bilgi teknolojileri sistemlerimize veya bilgi varlıklarına müdahale, test, bakım onarım vb. amaç ile geldiklerinde Gizlilik Sözleşmesi yapılacaktır ve bulundukları sürece kurum politikalarına uygun hareket etmekle yükümlüdürler.
- Kurum paydaşları ile kuruma ait özel bilgilerin paylaşıldığı proje veya iş anlaşmaları durumunda Gizlilik Sözleşmesi yapılacaktır.
- Kurum paydaşları bilgi teknolojileri sistemlerimize veya bilgi varlıklarımız üzerinde yapacakları çalışmaları Bartın Üniversitesi Bilgi İşlem Daire Başkanlığına bildirmek zorundadır.
- Kurum paydaşları bilgi teknolojileri sistemlerimize veya bilgi varlıklarına, kendilerine verilen yetki kapsamında erişim sağlayacaktır.
- Kurum paydaşları bilgi teknolojileri sistemlerimize veya bilgi varlıklarına erişim yetkileri, çalışma alanlarını kapsayacak şekilde kısıtlı yetki verilecektir. İşlem logları saklı tutulacak ve çalışma bittikten sonra verilen yetkiler hemen geri alınacaktır.
- Kurum paydaşlarına bilgi teknolojileri sistemlerimize eriştikleri süre boyunca Bartın Üniversitesi Bilgi İşlem Daire Başkanlığı'nın belirlediği yetkili personel tarafından refakat edilecektir.
- Kurum paydaşlarına bilgi teknolojileri sistemlerimize veya bilgi varlıklarına erişim izni verilecek bilgisayarlar/mobil cihazlar için UZAK BAĞLANTI POLİTİKASI uygulanacaktır. Kurum gerekli gördüğü durumlarda herhangi bir uyarıda bulunmadan VPN bağlantı erişimlerini kesme hakkına sahiptir.

P10 KABUL EDİLEBİLİR KULLANIM POLİTİKASI

1. Amaç

Bilgi teknolojileri sistemlerine ve bilgi varlıklarına Gizlilik, Bütünlük ve Erişilebilirlik sınıfları açısından yapılması ve uyulması gereken iş kurallarını çalışanlara bildirmeyi amaçlamaktadır.

2. Kapsam

Bu politika bütün Üniversite birimleri/çalışanları ve paydaşları (tedarikçiler, vatandaşlar, ziyaretçiler vb.) kapsamaktadır.

3. Politika

- Kurum bilgisayarının veya cihazlarının, çalışandan alınması durumunda; çalışanın cihazlar üzerindeki kişisel verileri için erişim yetkisi istemesi halinde Üst Yönetim bilgisayar veya cihazlara erişim izni vermeme hakkına sahiptir.
- Bilgi İşlem Daire Başkanlığı'nın Gizli olarak belirlediği bütün bilgilerin gizliliğine uyulması zorunludur. Bu bilgilerin izinsiz olarak kopyalanması, çoğaltılması, paylaşılması ve iletilmesi yasaktır.
- Bütün çalışanlar, kendilerine tahsis edilmiş bilgisayar / cihazların erişim bilgilerini ve güvenliğini korumakla sorumludur ve paylaşması yasaktır.
- Çalışanların, bilgisayarından anti-virüs koruma yazılımını devre dışı bırakması yasaktır.
- Çalışanların kuruma ait bilgisayar ve cihazlarda kaynağı belli olmayan ve üretici firması tarafından kopya edilmesi yasaklanmış bir yazılımı kullanması veya kopyalaması yasaktır.
- Kuruma ait bilgisayarlara ve cihazlara lisanssız program yüklenmesi yasaktır.
- Kullanıcıların kurumun kendilerine tahsis etmiş olduğu bilgisayar, cihaz ve kurum dosya sunucusu üzerinde kuruma ait bilgi, belge , programlar ve kurumun amacı dışında dosya bulundurması veya paylaşması yasaktır.
- Kullanıcıların kurumun kendilerine tahsis etmiş olduğu bilgisayar veya cihazlar üzerinde iş amacı haricindeki programları (oyun, eğlence vb.) kullanması yasaktır.
- Kritik dokümanlara erişim yetkisi bulunan kullanıcı, doküman içeriğindeki bilginin uygun bir şekilde korunmasından sorumludur.
- Herhangi bir kişi kendine ait olmayan kritik doküman bulur ise bu durumu Bilgi İşlem Daire Başkanlığı'na ve Bilgi Güvenliği Kurul Temsilcisine bildirecektir.
- Çalışanlar, "Gizli" belgeleri kilitli dolaplarda muhafaza edecektir.

- Sunucu ve bilgisayarların saatleri kullanıcılar tarafından değiştirilemez. Saatler sistem tarafından otomatik olarak yönetilmektedir.

- Çalışan, taşınabilir cihazları (laptop, tablet, cep telefonu, harici disk vb) güvenlik açıklarına karşı daha dikkatle korumak zorundadır. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmalıdır. Cihazların çalınması veya kaybolması durumunda en kısa zamanda Bilgi İşlem Daire Başkanlığı ve Bilgi Güvenliği Ekibine haber verilmesi gerekmektedir.

- Çalışanların kurumun tahsis ettiği bilgisayar ve cihazları kendisi dışında herhangi bir kimseye (iş arkadaşları, aile bireyleri vb.) kullandırması ve paylaşması yasaktır.

- Kullanıcıların program yükleme ve PC'lerindeki diğer iş talepleri; UBYS üzerinden gerçekleştirilecek ve Bilgi İşlem Daire Başkanlığı tarafından yönetilecektir.

P11 TEMİZ MASA TEMİZ EKRAN POLİTİKASI

1. Amaç

Çalışanların mesai saatleri içi veya dışında görevleri gereği kullandığı bilgilerin (yazılı doküman, belgeler, formlar, bilgisayarlar vb.) yetkisiz erişim veya uygunsuz kullanımı sonucunda oluşabilecek riskleri ortadan kaldırmayı amaçlamaktadır.

2. Kapsam

Bu politika kurumun bütün çalışanlarını kapsamaktadır.

3. Politika

- Çalışma masasından ayrıldığında basılı doküman ya da taşınabilir depolama aygıtları üzerinde tutulan bilgiler güvenlikli ortamlarda (çelik kasa, kilitli dolap ve çekmeceler vb.) saklanacaktır.
- Her türlü faks, fotokopi, yazıcı vb. cihazlar üzerinde yetkisiz erişimlere karşı belge, doküman vb. bırakılmayacak ve sürekli kontrol edilecektir.
- Bilginin kullanıldığı sistemler (sunucular, kamera DVR cihazları, bilgisayar, cep telefonları vb.) şifresiz kullanılmayacak ve korumasız bir şekilde bırakılmayacaktır.
- Bilgi teknolojileri sistemlerinde kullanılan kullanıcı adı ve şifreler bilgisayar veya masa üzerinde yazılı olarak bulundurulmayacaktır.
- İhtiyaç duyulmadığına karar verilen dokümanlar ve içinde bilgi bulundurulabilecek elektronik cihazlar uygun metotlarla (kağıt öğütücü, disk/disket kıyıcı, yakma vb.) imha edilecektir.
- Gizli olarak tanımlanan (sözleşme, fatura, kişisel veri içeren, şartnameler, veri dokümanları vb.) dokümanlar ve kopyaları, müsvedde olarak kullanılmayacak ve kağıt öğütücü ile imha edilecektir.
- Çalışanların kullandığı kurum bilgisayarları 10 dakika boyunca herhangi bir işlem yapılmadığında otomatik olarak kilitlenecektir. Ayrıca bu işlem **Windows + L** tuşuna basılarak anlık olarak yapılabilecektir.
- Kullanıcılar bilgisayarlarının masaüstlerindeki dosyalarını, düzenli olması için klasörler içerisinde muhafaza edeceklerdir.

P12 MOBİL CİHAZ POLİTİKASI

1. Amaç

Kuruma ait bilgi içeren mobil cihazların güvenli kullanım ve yönetimini amaçlamaktadır.

2. Kapsam

Kuruma ait bilgi içeren bütün mobil ve taşınabilir cihazları kapsar.

3. Politika

- Kuruma ait mobil cihazlar (cep telefonu, dizüstü bilgisayar, usb bellek, harddisk, tablet vb.) ilgili kişiye zimmetlenerek teslim edilmelidir.
- Her çalışan kendisine zimmetlenen cihazın güvenliğinden ve amacına uygun kullanımından sorumludur.
- Kuruma ait bilgi içeren mobil cihazlara yetkisiz müdahaleyi önlemek için kullanıcı tarafından şifre tanımlanması zorunludur.
- Kuruluş telefon hatları ve mobil cihazlar üzerinden kullanım amaçlarına uygunsuz, müstehcen, rahatsız edici materyaller ve başkalarına iftira, karalama mahiyetinde iletişim kurmak, mesajlar yayınlamak ve paylaşmak yasaktır.
- Kurumun tahsis ettiği mobil cihazların kendisi dışında herhangi bir kimseye (iş arkadaşları, aile bireyleri vb.) kullandırılması ve paylaşılması yasaktır.
- Mobil cihazlarda ne tür bilgiler saklandığının farkında olunmalı ve kuruma ait bilgiler mümkün olduğunca mobil cihazlar üzerinde bulundurulmamalıdır.

P13 VERİTABANI GÜVENLİK POLİTİKASI

1. Amaç

Kurumun veri tabanı sistemlerinin güvenli kullanım ve yönetimini amaçlamaktadır.

2. Kapsam

Bütün veri tabanı sistemlerini kapsar.

3. Politika

- Veri tabanında kritik verilere her türlü erişim işlemlerinin (okuma, değiştirme, silme, ekleme) log kayıtları tutulacaktır. Log kayıtlarına, Bilgi İşlem Daire Başkanlığı'nın yetkilendirdiği kişiler dışında erişim yapılması yasaktır.
- Veri tabanı bulunan sunuculara, Bilgi İşlem Daire Başkanlığı'nın yetkilendirdiği kişiler dışında erişim yapılması yasaktır.
- Veri tabanı sunucularına bağlanma yetkisine sahip kullanıcılar sadece kendi kullanıcı adı ve şifresi ile bağlantı yapacaktır.
- Sunucularda bulunan veri tabanlarının kritiklik seviyelerine göre yedekleri alınacaktır.
- Veri tabanı sunucuları fiziksel olarak güvenlik önlemi alınmış sistem odalarında bulundurulacaktır.
- Veri tabanlarında yapılacak bakım onarım ve güncelleme çalışmalarından önce ilgili birimlere duyuru yapılacaktır.
- Veri tabanı bulunan medyalar (harici disk, usb bellek vb.) kurum dışına çıkarılmayacaktır.
- Veri tabanlarına kurum dışından erişimler Uzak Bağlantı Politikası'na uygun şekilde yapılacaktır.
- Veri tabanı sunucularının kaynakları (cpu, ram, disk, ağ trafiği vb.) düzenli olarak kontrol edilecektir.
- Veri tabanlarına kurum dışından erişim sağlayan firmalar ile Bilgi İşlem Daire Başkanlığı arasında Gizlilik Sözleşmesi imzalanacaktır.

P14 YAZILIM TEMİNİ ve GELİŞTİRME POLİTİKASI

1. Amaç

Kurumun yazılım temini ve geliştirme ihtiyacının güvenli yönetilmesini amaçlamaktadır.

2. Kapsam

Bütün yazılım temini ve geliştirmelerini kapsar.

3. Politika

- Bilgi İşlem Daire Başkanlığı, kaynak yönetimini sağlamak, mevcut altyapıya ve kullanım amacına uygun yazılım projeleri gerçekleştirmek ile yükümlüdür.
- Kurum genelinde kullanılacak yazılımların (geliştirilen veya satın alınan) kanunlarla belirli olan şartları sağlaması zorunludur. Bu konuda Bilgi İşlem Daire Başkanlığı sadece kendi onayladığı yazılımların sorumluluğunu kabul etmektedir. Birimlerin Bilgi İşlem Daire Başkanlığı'nın onayını almadan yaptıkları yazılım alımlarında yada kullanımlarında ise sorumluluk birimlere aittir.
- Kurum genelinde kullanılacak olan yazılımlarda Bilgi İşlem Daire Başkanlığı tarafından onaylanmış yazılımların (geliştirilen veya satın alınan) kullanılması öncelik arz etmektedir.
- Yeni alınmış veya revize edilmiş bütün yazılımlar Bilgi İşlem Daire Başkanlığı tarafından test edilecek ve onaylanacaktır.
- Kuruma ait yazılımlar Varlık Envanteri Listesine eklenecek ve takip edilecektir.

P15 DEĞİŞİM YÖNETİMİ POLİTİKASI

1. Amaç

Kurumun bilgi teknolojileri sisteminde yapılması gereken yazılımsal ve donanımsal değişikliklerde süreklilik ve güvenliği sağlamayı amaçlamaktadır.

2. Kapsam

Bu politika kurumun bütün çalışanlarını kapsamaktadır.

3. Politika

- Yazılımsal ve donanımsal değişiklik talepleri UBYS Servis Destek Modülü üzerinden takip edilecektir.
- Yazılımsal ve donanımsal değişiklikler yapılmadan önce, bu değişiklikten etkilenecek bütün sistem ve uygulamalar belirlenerek ilgili kişilere bilgi verilecektir.
- Yazılımsal ve donanımsal değişikler gerçekleştirilmeden önce değişikliğin yapılacağı sistemlerin yedekleri alınacaktır.
- Sistemlerde yapılacak değişikliklerde ilgili üretici tarafından onaylanmış güncellemeler kullanılacaktır.
- Yazılımsal ve donanımsal değişiklikler sisteme alınmadan önce Bilgi İşlem Daire Başkanlığı veya ilgili alt birim tarafından onaylanacaktır.

P16 OLAY YÖNETİM POLİTİKASI

1. Amaç

Bilgi güvenliği olaylarının kayıt altına alınması ve yönetilmesini amaçlamaktadır.

2. Sorumlular

Bu politikanın uygulanmasından bütün personel sorumludur.

3. Politika

- Bilginin gizlilik, bütünlük ve erişilebilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumları düzenli olarak kayıt altına alınacaktır. Yaşanan olaylar Bilgi Güvenliği Olay Yönetimi Politikasına göre yönetilecektir.
- Yaşanan Bilgi Güvenliği olayları Bilgi İşlem Daire Başkanlığı Bilgi Güvenliği Ekibi'ne (SOME) (bilgiguvenliği@bartin.edu.tr) e-posta veya telefon (Dahili: 5459-5304) ile bildirilecektir.
- Bilgi Güvenliği olayının kaynağı Bilgi Güvenliği Ekibi tarafından araştırılacak ve olayın önemlilik seviyesine göre müdahale edilecektir.
- Bilgi güvenliği olayı kayıtları (log, fotoğraf, video vb) Bilgi Güvenliği Ekibi tarafından saklanacaktır.
- Yaşanan Bilgi Güvenliği olayları cezai ve hukuki mesuliyetle sonuçlanabilir. Kurum bu tür ihlallerin söz konusu olduğu durumları inceler ve eğer bir suç oluştuğundan şüphe duyulursa disiplin yönetmeliğini uygulayabilir veya yasa uygulayıcısı ile işbirliği yapabilir.
- Bilgi Güvenliği olayları analiz edilerek tekrarlanmaması için gerekli önlemler alınacaktır.

P17 KRİPTOGRAFİK KONTROLLER POLİTİKASI

1. Amaç

Bilgi varlıklarının saklandığı sistemlerin ve bilgi varlıklarının transferinin gizliliğini veya bütünlüğünün şifreleme yöntemleri ile korunması amaçlanmaktadır.

2. Kapsam

Bu politikanın uygulanmasından bütün personel sorumludur.

3. Politika

- Gizli olarak ifade edilen bilgi varlıklarının paylaşımında güçlü şifreleme algoritması kullanılacaktır. Bu bilgi varlıklarının paylaşımı sırasında Winrar programı ile sıkıştırılarak şifrelenecektir.
- Mobil cihazlardaki verilerin korunmasında şifre kullanılmalıdır.
- E-posta hesabı kurulu akıllı telefonlarda telefon kilidi kullanılması zorunludur.
- Tanımlanan şifreler belirli aralıklarla değiştirilmelidir.
- Hesap şifreleri kolay tahmin edilmeyen karmaşık şifreler olmalıdır.
- Misafirlerin internet kullanımı için misafir ağına bağlanılırken şifre kullanılır.
- Kurumun e-posta sistemi SSL serfikası ile şifrelenmektedir.

P18 KAMERA POLİTİKASI

1. Amaç

Üniversite bünyesindeki IP kameralar ile oluşturulan verilerin, belirli bir süre saklanması ve muhafazası konusunda gerekli önlemleri almaktır.

2. Kapsam

Bu politika kurumun bütün çalışanlarını kapsamaktadır.

3. Politika

- Üniversitemiz bünyesinde IP kameraların kayıtlarını tutmak için NVR (Network Video Recorder) sunucuları kullanılmaktadır.
- Bütün IP kameraların kayıtları son 30 günü sunucularda tutulmaktadır.
- Bilgi İşlem Daire Başkanlığı bütün IP kameraların bakımlarını, onarımlarını kendi bünyesindeki personeli ya da anlaştığı herhangi bir şirket personeli vasıtasıyla yapacak veya yaptıracaktır.
- IP kamera haricindeki analog kameralar için veri saklama ya da bakım hizmeti verilmemektedir. Analog kameralar birimlerin kendi sorumluluğundadır.
- Üniversite bünyesindeki kameralar tarafından alınan video kayıtlarının canlı görüntülerinin izlenmesine güvenlik amirliğine bağlı birimler hariç izin verilmemektedir.
- Bilgi İşlem Daire Başkanlığı yeni kamera kurulumları için gelen talepleri güvenlik amirliğinin uygun görmesi ve ilgili birim talebi doğrultusunda yapmaktadır. Diğer yapılan kamera kurulum talepleri ise gerekli görüldüğü takdirde gerçekleştirilecektir.
- Geçmişe dönük olan kamera kayıt izleme taleplerini, başvuran kişi ve güvenlik amirliğinin görevlendirdiği bir kişi ile beraber başvurması kaydıyla, Bilgi İşlem Daire Başkanlığı tarafından gösterilen yerde ve zamanda izlenilmesine izin verir. Kayıt izleme talepleri tutanak veya formla kayıt altına alınır.
- Görüntü kayıtları Üniversite yönetiminin izni ve talebi ile resmi belge karşılığında verilir. Kayıtların depolanacağı alanı talepte bulunan kişi veya kurum sağlar.
- Güvenlik görevlileri, güvenlik kamerası izleme noktalarını Bilgi İşlem Daire Başkanlığının hazırladığı bilişim politikaları kuralları dâhilinde kullanabilir.
- Güvenlik görevlileri, güvenlik amirliği tarafından belirlenen sorumlusu olduğu noktanın kendi mesai saati içinde (bina, nizamiye, spor salonu vs.) güvenlik kameralarını izleyebilir.
- Güvenlik görevlileri, güvenlik kamerası görüntülerini, güvenliği sağlama amacı ile izler, üçüncü şahıslara izletemez, hiçbir şekilde kayıt altına alamaz, kopyalayamaz ve paylaşamaz.

- Güvenlik görevlileri, güvenlik kamerası izleme yazılımına Bilgi İşlem Daire Başkanlığının izni dışında müdahale edemez ve üçüncü şahısların müdahalesine izin veremez.

- Bilgi İşlem Daire Başkanlığı güvenlik kamerası izleme noktalarının amacı dışında kullanıldığını ve Anayasanın 20. maddesindeki "özel hayatın gizliliği" ve "kişisel verilerin korunması" hükmünün gözetilmediğini tespit ettiğinde, birim yetkililerine ve Üniversite yönetimine bilgi vererek gerekli tedbirleri alır.

P19 YEDEKLEME POLİTİKASI

1. Amaç

Üniversite ağı ve cihazları üzerinde oluşturulan, kullanılan ve devamlılığı gerekli görülen verilerin saklanması ve muhafazası konusunda gerekli önlemleri almaktır.

Bu politikanın uygulanmasından bütün personel sorumludur.

2. Kapsam

Bilgi İşlem Daire Başkanlığının kontrolünde olan ve Üniversite bünyesinde oluşturulan verilerin (yedekleme üniteleri ve sunucularda) güvenli olarak yedeklenmesi, gerektiğinde kullanıma açılması ve ihtiyaç sonunda silinmesi için gerekli yöntemlerin belirlenmesini tanımlar.

Üniversite bünyesinde yedekleme Bilgi İşlem Daire Başkanlığının kurmuş olduğu sistem ve sanal sunucuların veri yedeklerini kapsar.

3. Politika

- Bilgi İşlem Daire Başkanlığı kendi kontrolünde olan ve gerekli gördüğü bütün cihazların, sistemlerin, ağların vs. kayıtlarını kendi belirlediği süre içerisinde düzenli olarak almaktadır. Belirlenen zaman boyunca saklamakta ve belirlenen zaman dolduğunda da silmektedir.

- Bilgi İşlem Daire Başkanlığı kontrolünde olmayan kullanıcıların kullandığı cihazlara ve sistemlere vs. ait olan kişisel ve özel verilerin yedeklenme ve saklanma işlemlerinden kullanıcı kendisi sorumludur. Bilgi İşlem Daire Başkanlığı herhangi bir veri kaybından ya da kaybolan verilerin kurtarılmasından sorumlu tutulamaz.

- Üniversitede elektronik ortamda veriyi üretme ve/veya yönetme ile görevlendirilen bütün personel sorumludur.

- Üniversite bünyesinde kullanılan sunucu ve sistemlerin düzenli aralıklarla önem sırasına göre yedekleri alınmaktadır.

- Sunucu yedeklerinin belirlenen yedekleme süre periyotları ölçüsünde veri kaybı kabul edilebilir. (Üç günde bir yedeği alınan sunucunun arızalanması durumunda 3 günlük ara kabul edilebilir veri kaybı olarak kabul edilmektedir.)

P20 WEB TAHSİSİ POLİTİKASI

1. Amaç

Bartın Üniversitesinin, kurumsal kullanıcılarına sağladığı alan adlarının kullanım yönergesini oluşturmak ve kullanım ilkelerini belirlemek.

2. Kapsam

Bu politika kuruma ait web sayfası kullanan bütün birimlerini/çalışanlarını kapsamaktadır.

3. Politika

- Bartın Üniversitesi, alan adı (subdomain) yerine hizmetini yalnızca kurum bünyesindeki fakülteler, enstitüler, yüksekokullar, meslek yüksekokulları, birimler, bölümler, müdürlükler, koordinatörlükler, öğrenci grupları, konferanslar, toplantılar, sempozyumlar, kongreler, çalıştaylar, paneller vs. gibi kurumsal yapılara sağlamaktadır.

- Üniversite bünyesindeki fakülteler, enstitüler, yüksekokullar, meslek yüksekokulları, birimler, bölümler, müdürlükler, koordinatörlükler, öğrenci grupları, konferanslar, toplantılar, sempozyumlar, kongre, çalıştay, panel vs. gibi yapılar üniversitenin kurumsal kimliğinin bozulmaması için Bilgi İşlem Daire Başkanlığı tarafından sağlanan web sitelerini kullanacaklardır.

- Rektörlük oluruyla kendi web sitesini oluşturmuş olan birimlerin sitelerine ise Bilgi İşlem Daire Başkanlığı tarafından barındırma hizmeti dışında herhangi bir destek verilmeyecektir. Sunucu ve sistem güvenliği birimin kendi sorumluluğu altındadır. Oluşabilecek bütün yasal ve teknik sorunlardan ilgili birim ve web site yöneticisi sorumlu olacaktır.

- Alan adı (subdomain) alma talepleri, Bilgi İşlem Daire Başkanlığının http://bim.bartin.edu.tr adresinde formlar kısmında bulunan Web Site Talep Formu'nun talebi yapan kurumsal birimin yöneticisi tarafından imzalanması ve bir görevli personel ataması yapılarak üst yazı ile başvurmasıyla yapılır.

- Alan adı ve site içeriği ile ilgili olarak olası hukuki süreçlerden ve sorunlardan adına web alanı tahsis edilen kullanıcı sorumludur.

- Üniversitemiz bünyesinde Bilgi İşlem Daire Başkanlığı tarafından açılan web sitesi ve alt alanlar (subdomain) dışında yapılan web sitesi veya alt alanların (subdomain) yönlendirilme taleplerine destek verilmemektedir.

- Üniversite ve öğrenci toplulukları tarafından organize edilen veya katılımda bulunulan ulusal/uluslararası etkinlik ve organizasyonlar için verilen alan adresleri ilgili birim ya da topluluklardan resmi yazı ile talep gelmesi üzerine açılmaktadır.

- Kullanıcı web kota bilgisi sadece Bilgi İşlem Daire Başkanlığının verdiği alanla sınırlıdır. Sonradan yapılan kota artırım talepleri ise Bilgi İşlem Daire Başkanlığının kaynak durumuna göre, gerekli görülmesi ve uygun ortamın bulunması durumunda sağlanacaktır.

- Web sitesi ve alt alan adı tahsis edilen birim, personel, etkinlik ve organizasyonlar yayınladıkları web sitelerinde Bartın Üniversitesi Bilgisayar, Ağ ve Bilişim Kaynakları Kullanım Yönergesine uymak zorundadırlar. Kullanıcı, web alanı hizmetinden faydalanırken Bilgi İşlem Daire Başkanlığı tarafından yayınlanan her türlü ihtar ya da bildirime uymayı beyan, kabul ve taahhüt eder. Kullanıcı, almış olduğu web alanı hizmetini üçüncü kişilere her ne ad altında olursa olsun kullandıramaz.

- Kullanıcı kişisel web alanında barındırdığı bütün dosya, doküman ve programlardan, web sitesi ve eposta hizmetleri ile kullanacağı ve faydalanacağı bütün işlemlerden kendisinin sorumlu olduğunu; söz konusu veri, bilgi, beyanların yasalara aykırılığından ve web alanında barındırdığı web sayfası ya da programların güvenlik açıkları nedeniyle başka bir sunucuya yapılacak saldırıdan doğabilecek bütün hukuki ve cezai sorumluluğu kendisi karşılamayı kabul ve taahhüt eder. Bu konuda doğabilecek sorunlardan Bilgi İşlem Daire Başkanlığına herhangi bir sorumluluk yüklenemez.

- Bilgi İşlem Daire Başkanlığı kullanıcıların hizmet aldığı merkezi sunucular üzerinde herhangi bir zamanda teknik değişiklikler yapma hakkına sahiptir. Bu değişiklikleri önceden kullanıcılara bildirebileceği gibi, anlık olarak yapılabilecek değişikliklerin önceden duyurulamaması da mümkün olabilir. Kullanıcılar oluşacak veri kaybı vs. gibi konularda herhangi bir hak talep edemez.

- Bilgi İşlem Daire Başkanlığı, birimlerin kendi imkânları ile hazırlamış oldukları web siteleri için güvenlik testi yapmaz, güvenlik açıklarını kontrol etmez, kurulan eklentilerinin güvenlik açıklarını test etmez, doğrulamaz, ciro etmez veya kullanıcı tarafından yapılmış sayfalar için herhangi bir şekilde bir sorumluluk almaz.

- Bilgi İşlem Daire Başkanlığı, birimlerin kendi imkânları ile hazırlamış oldukları web sitelerinde güvenlik açığı bulunmasından dolayı hizmet alan diğer kullanıcılarına veya üçüncü şahıslara herhangi bir şekilde zararlı olduğuna karar verdiği durumlarda hizmeti kesebilir veya müdahale edebilir.

- Bilgi İşlem Daire Başkanlığı hukuka aykırı fiil ve eylemleri öğrendiğinden itibaren kullanıcıya haber vermeden kullanıcı hesaplarını geçici veya sürekli olarak kapatmak veya silmek hakkına sahiptir.

- Bilgi İşlem Daire Başkanlığı, sağladığı hizmet içerisinde bulunan kullanıcı verilerinin hatalı kullanımlarından, veri içeriklerinden, e-posta ile kullanılan bütün verilerden doğabilecek hiç bir maddi

veya manevi zararlardan sorumlu tutulamaz. Bu verilerin yedekleme ve saklama yükümlükleri kullanıcıya aittir.

- Bilgi İşlem Daire Başkanlığı yedekleme işlemlerini bilişim politikalarında belirttiği yedekleme politikasına uygun olarak yapmaktadır.

- Bilgi İşlem Daire Başkanlığının kontrolü dışında oluşturulmuş web sayfalarının içeriği üzerinde herhangi bir sorumluluğu yoktur. Bu sayfaların içeriğini kontrol ve takip etmez; bu sayfaların içeriği ile ilgili güvence sağlamaz.

- Bilgi İşlem Daire Başkanlığı hiç bir durumda, doğrudan veya dolaylı olarak, bu sayfalarda sunulan içeriğin kullanımı veya referans gösterilmesi ile ilgili oluşabilecek veya oluştuğu iddia edilebilecek sorun veya zararlardan sorumlu tutulamaz.

- Bilgi İşlem Daire Başkanlığı web programlama konusunda sadece gelen taleplere göre Üniversite bünyesindeki fakülteler, enstitüler, yüksekokullar, meslek yüksekokulları, birimler, bölümler, müdürlükler, koordinatörlükler, öğrenci grupları, konferanslar, toplantılar, sempozyumlar, kongreler vs. gibi kurumsal yapılara ve gruplara gerekli gördüğü takdirde web yazılım desteği sağlamaktadır.