İÇİNDEKİLER

İÇİNDEKİLER....1
1. AMAÇ....2
2. KAPSAM....2
3. SORUMLULAR....2
4. TANIMLAR....2
5. UYGULAMA....2
5.1. ERİŞİM POLİTİKASI....2
5.1.1. DIŞARDAN ERİŞİM POLİTİKASI....2
5.1.2. UYULMASI GEREKEN KURALLAR....3
5.1.2.1. SSL-VPN....3
5.1.2.2. E-POSTA YAZILIMI....3
5.1.2.3. MOBİL CİHAZLAR....3
5.1.2.4. TAŞINABİLİR HARD DİSK....3
5.1.2.5. DİZÜSTÜ BİLGİSAYARLAR....4
5.1.2.6. UZAK MASAÜSTÜ BAĞLANTILARI....4
5.1.3. AĞLARA ve AĞ HİZMETLERİNE ERİŞİM HAKKI....4
5.1.4. DOKÜMAN ERİŞİLEBİLİRLİK KURALLARI....5
5.2. İNTERNET ERİŞİM HAKKI....6
5.2.1. İNTERNET ERİŞİMİ....6
5.2.2. İNTERNET ERİŞİM PROSEDÜRÜ....6
5.3. İNTERNET VE E-POSTA KULLANIM HAKKI....6
5.3.1. İNTERNET AŞAĞIDAKİ AMAÇLAR İÇİN KULLANILMAZ....6
5.3.2. KURUMSAL E-POSTA KULLANIM KURALLARI....7
5.4. AYRICALIKLI ERİŞİM HAKLARI....7
5.4.1. AYRICALIK YÖNETİMİ....7
5.4.2. KULLANICI HAKLARI....8
5.4.2.1 KONFİGÜRASYON ve GÜVENLİK AYARLARI....8

Bayburt Üniversitesi'nin, KVKK-DDO ve BGYS ile ilgili uyması gereken bazı kurallar aşağıda belirtilmiştir.

1. AMAÇ

Bayburt Üniversitesi içinde kullanıcı erişim politikası ve buna bağlı olarak internet erişim hakkı, internet kullanım hakkı, E-mail kullanım haklarını ve ayrıcalıklı erişim kurallarını tanımlamaktadır.

2. KAPSAM

Kapsama dâhil Bilgi işlem olanaklarından yararlanan tüm kullanıcı ve birimleri kapsar.

3. SORUMLULAR

Kapsama dâhil tüm çalışanların bu politikaya ve erişim haklarına uygun hareket etmesinden Bayburt Üniversitesi Rektörlüğü sorumluluğundadır.

4. TANIMLAR

BAYÜ: Bayburt Üniversitesi

KVKK: Kişisel Verileri Koruma Kanunu

CB: Cumhurbaşkanlığı

DDO: Dijital Dönüşüm Ofisi

BGYS: Bilgi Güvenliği Yönetim Sistemi

KVYS: Kişisel Verileri Yönetim Sistemi

5. UYGULAMA

5.1. ERİŞİM POLİTİKASI

5.1.1. DIŞARDAN ERİŞİM POLİTİKASI

Bayburt Üniversitesi kapsam dâhilinde tüm bilişim teknolojisi kullanıcılarının ve üçüncü taraf firmaların erişim hakları ve uyması gereken kurallar, Bilgi İşlem Daire Başkanlığı tarafından belirlenen yol ve yöntemler ile sağlanmaktadır. Erişim izinleri en az yılda bir kez kontrol edilmektedir.

5.1.2. UYULMASI GEREKEN KURALLAR

5.1.2.1. SSL-VPN

- Dışarıdan kullanıcıların bağlanabilmesi için güvenlik seviyesi yüksek gerekli ortamın hazırlanması (SSL-VPN)

- SSL-VPN yapılabilmesi için kullanıcı bazlı açılan hesap bilgilerinin gizli tutulması
- Gizlilik sözleşmesi gereği "Kullanıcı Bilgileri" nin sorumluluğunun kullanıcılara ait olduğunun iletilmesi
- Üçüncü taraf firmaların erişim hakları ve sürelerinin Bilgi İşlem Daire Başkanlığı'nın kontrolünde sağlanması
- Kullanıcılar kendi alanı yetkileri dışında 3. taraflara erişimleri EBYS üzerinden ilgili birimine talepte bulunur. Bilgi İşlem Daire Başkanlığı tarafından uygun görüldüğü takdirde onay veya red verilmektedir.

5.1.2.2. E-POSTA YAZILIMI

- BAYÜ uzantılı kurumsal e-posta sunucuları üzerinden yönetilmektedir.
- E-postanın kurulu olduğu sunucularda, şifre sorgulaması yapılmaktadır.
- Personel ve öğrenci epostaları ayrı sunucularda hizmet vermektedir.
- E-posta yazılımı bağlantısının güvenilirliğinin arttırılabilmesi için özel sertifika yazılımları mevcuttur.

5.1.2.3. MOBİL CİHAZLAR

- Kapsama dâhil personellerin mobil cihaz kullanımı mevcut olup ilgili personelin kendi mobil cihazı vardır.
- İsteğe bağlı olarak personelin şahsına ait olan mobil cihazlar üzerinde kurumsal e-posta hesaplarına erişim gerçekleştirilebilmektedir.
- Mobil cihazlar üzerinden e-posta erişim esnasında kullanıcı adı ve şifre zorunluluğu bulunmaktadır.
- Mobil cihazlar üzerinde şifre koyma zorunluluğu ilgili kullanıcı sorumluluğundadır. Kişisel ve kurumsal bilgilerin çalınması ve kaybolması durumunda tüm mesuliyet ilgili kullanıcıya aittir.

5.1.2.4. TAŞINABİLİR HARD DİSK

- BAYÜ ait tüm bilişim cihazlarının USB portları açık olup, sorumluluk tamamen kullanıcıya aittir.
- BAYÜ bünyesinde tahsis edilmiş veya personele ait olan taşınabilir hard disklere ilişkin riskler kullanıcı sorumluluğundadır. Buna ilişkin riskler risk envanterinde işlenmiştir.
- Bilginin 3.taraflar ile paylaşılması durumunda bilgi güvenliği politikalarına ve prosedürlerine uygun davranmayan kullanıcılar hakkında 2547, 657 ve 6698 sayılı kanun hükümleri ve diğer kanunlara ilişkin olarak disiplin yönetmeliği hükümleri uygulanır.

5.1.2.5. DİZÜSTÜ BİLGİSAYARLAR

- Dizüstü bilgisayar kullanımındaki güvenliğin sağlanması ve açılışta parola konulması kullanıcı sorumluluğundadır.

- Kullanıcı bilgisayarları üzerindeki kuruma ait önemli bilgi ve belgelerin bulundurulmaması gerekmektedir. Kuruma ait önemli bilgi ve belgelerin BAYÜ bulut ortamında bulundurulması gerekmektedir.
- Elektronik ekipmanlar varlıkların kabul edilebilir kullanım prosedürüne uygun olarak kullanılmaktadır.
- Kurum envanterine kayıtlı tüm cihazlarda lisanslı anti-virüs yazılımlarının kullanılması zorunludur. Yazılımın değiştirilmesi, kapatılması, durdurulması veya silinmesi durumlarında oluşabilecek her türlü bilgi güvenliği ihlallerinden kullanıcı sorumlu olup; ilgili disiplin hükümleri (2547, 657 ve 6698) uygulanacaktır.
- Güvenliği ihlal eden (virüs, trojan vb.) zararlı yazılımlar içerecek 3. parti programların cihazlara kurulması durumunda yaşanılabilecek bilgi güvenliği ihlallerinden kullanıcı sorumludur.

5.1.2.6. UZAK MASAÜSTÜ BAĞLANTILARI

- Üçüncü parti yazılımlar ile uzak bağlantı talepleri resmi yazışmalar yapılıp yönetici onayı alındıktan sonra gerçekleştirilmektedir.

5.1.3. AĞLARA ve AĞ HİZMETLERİNE ERİŞİM HAKKI

- BAYÜ kullanıcılarının uygulama erişim yetkileri kendi birimlerinin alanı ile sınırlandırılmıştır.
- BAYÜ kullanıcı adı ve şifresine sahip olmayan personellerin internete çıkışları mümkün değildir.
- BAYÜ kullanıcı adı ve şifresi bulunan personeller internet çıkışları Mac adresi ve IP adresleri sunucu üzerinde kayıt altına alınmaktadır.
- Erişim kısıtlamaları veya erişim izinleri kullanılan program üzerinden yapılmaktadır.
- Kurum ile ilişkisi kesilen öğrenci ve personelin ilgili birimler tarafından OBS ve Personel Özlük İşleri Otomasyonu üzerinden durumları pasif edilerek kurum içerisindeki internet ve tüm otomasyonlara erişimleri engellenmektedir.
- Birim değişikliklerinde erişim yetkileri yeniden tahsis edilmektedir.Talepler EBYS üzerinden alınmaktadır.
- Kullanıcı hakları en az yetki prensibi göz önünde bulundurularak sadece ihtiyaç duyulan kullanıcı ve gruplara verilmelidir.
- Ağlar VLAN yapısı ile ayrılmıştır (fakülteler, kamera sistemleri, geçiş sistemleri, aktif sunucular, yazar kasalar, vb.).
- Ağ üzerinde ilgili kurallarla (internet kullanım kısıtlamaları) uygulanır.
- Sunucuların normal işleyişi için gerekli olmayan tüm servisler kapatılmalıdır. Sistemlerde çalışan servisler ihtiyaçları olan en az yetki ile çalışmalıdır.
- Admin yetkisi olan kullanıcıların yetkileri ayrıca kısıtlanmalıdır. Servislerin döndüğü başlık bilgileri (banner) bilgi ifşasına yol açmayacak şekilde değiştirilmelidir.

- Fakülte ve MYO ayrı VLAN'lar da bulunmakta ve ağ erişim yetkileri Omurga üzerinde tanımlanmaktadır.
- Ayrıcalıklı erişim hakları, kullanıcı grubuna uygun olarak tahsis edilmiştir.
- Ayrıcalıklı kullanıcı grubu hakkı için kullanıcı, önce ilgili birime resmi talepte bulunur. Bilgi İşlem Daire Başkanlığı talebi uygun bulursa yetki tahsisi yapılır.
- Ayrıcalıklı kullanıcı grubuna dâhil personellerin erişim sürelerinde istihdamın sonlandırılması veya ilgili amirin talebi ile değişiklik yapılmaktadır.
- AD üzerinden yerel hesaplar ve dâhil tüm uygulama hesapları yönetilmektedir.
- Kurumdaki sistemler bir yönetici hesabı oluşturulduğunda veya silindiğinde kayıt tutmaktadır.
- Kurum interneti üzerinden dışarı çıkan tüm ilgili taraflar (personel, öğrenci ve misafir) internet LOG kayıtları 5651 sayılı internet ortamındaki yayınların düzenlenmesi kanununa uygun olarak en az 2 yıl süre ile muhafaza edilmektedir.

5.1.4. DOKÜMAN ERİŞİLEBİLİRLİK KURALLARI

Tüm bilişim teknolojileri kullanıcılarının, doküman güvenliğinde uyması gereken bazı kurallar aşağıda belirtilmiştir.

Klasör ve Doküman Kullanım Kuralları:

- BAYÜ ile ilgili tüm dokümanlar sunucu üzerinde tutulmalıdır.
- Şahsi doküman, müzik, resim, video gibi veriler sunucu üzerinde bulundurulmamalıdır.
- 3. taraflar ile dosya veya klasör paylaşımı yapılırken kullanıcı tarafından şifrelenerek BAYÜ bulut üzerinden paylaşılmalıdır.
- Şifrelenerek 3. taraflar ile paylaşılan dosyalarda; şifreler ilgili kişilere farklı yöntem ve metotlarla bütünlüğü bozularak aktarılmalıdır.
- Sunucu üzerinde açılan klasörlere ulaşım esnasında problem yaşandığı takdirde hiçbir işlem yapılmadan Bilgi İşlem Daire Başkanlığı'na haber verilmelidir.

İşe Giriş Yapan Yeni Personel

- Kurumda yeni işe başlayan personelin ilgili birim tarafından Personel Özlük İşleri Otomasyonu üzerinden kullanıcı bilgileri tanımlanarak kurum içerisindeki internet ve tüm otomasyonlara erişim izinleri tahsis edilmektedir.
- Yeni personelin tanımlamaları yapıldıktan sonra BAYÜ bulut ve benzeri ortamlara erişimleri otomatik olarak yapılmaktadır.

5.2. İNTERNET ERİŞİM HAKKI

5.2.1. İNTERNET ERİŞİMİ

5651 sayılı Kanun (İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun) gereğince,

Sistem ve Ağ güvenliğinin ihlal edilmesi yasaktır, cezai ve hukuki mesuliyetle sonuçlanabilir. Bayburt Üniversitesi bu tür ihlallerin söz konusu olduğu durumları inceler ve eğer bir suç oluştuğundan şüphe duyulursa yasa uygulayıcı ile iş birliği yapar.

5.2.2. İNTERNET ERİŞİM PROSEDÜRÜ

- Konuk evinde konaklayan misafirler; telefon numarası ile doğrulama yaparak, IP ve MAC adresi kayıt altına alınarak konukevi kablosuz ağıyla internet hizmeti alabilmektedir.
- BAYÜ internet ağını kullanan personel ve öğrencilerin kullanıcı adı, mac adresi ve ip adresleri kayıt altına alınmaktadır.
- BAYÜ internet ağına EDUROAM ile bağlanan kullanıcıların kullanıcı adı, mac adresi ve ip adresleri kayıt altına alınmaktadır.

5.3. İNTERNET VE E-POSTA KULLANIM HAKKI

5.3.1. İNTERNET AŞAĞIDAKİ AMAÇLAR İÇİN KULLANILMAZ

- Ticari amaçlı reklamlar ve haber duyuruları gibi istenmeyen mesajlar (SPAM iletiler) göndermek,
- İnternet üzerindeki servis kalitesini etkileyecek, bozacak, karışıklık yaratacak trafik düzenlemeleri oluşturmak,
- Kullanım amaçlarına uygun olmayan; müstehcen, bölücü/yıkıcı faaliyetler, rahatsız edici materyal vb. üretmek ve dağıtmak,
- Güvenli olmadığı bilinen sitelere (mp3, program, oyun, forum, sohbet ya da cinsel içerikli vb.) girmek,
- Gerçek dışı, rahatsızlık verici, gereksiz yere sıkıntı ve korku yaratacak materyalin üretimi ve dağıtımını yapmak,
- İftira ve karalama mahiyetindeki materyalin üretim ve dağıtımını yapmak,
- Bayburt Üniversitesi İnternet Ağı üzerinden ulusal veya uluslararası hizmetlerin kasıtlı olarak yetkisiz kullanımı,
- Kurumsal ve kişisel verileri tahrip etmek,
- Başkalarına ait kişisel bilgileri (kişisel veri ve özel nitelikli kişisel veri) ifşa etmek,

- Başkalarına ait çalışmaları bozmak, tahrip etmek,
- Bayburt Üniversitesi İnternet trafiğini engelleyecek kullanımlarda bulunmak.

5.3.2. KURUMSAL E-POSTA KULLANIM KURALLARI

- E-Postalar ile ilgili tüm kontroller Bilgi İşlem Daire Başkanlığı tarafından yapılmaktadır.
- Yeni kullanıcı hesapları Bilgi İşlem Daire Başkanlığı tarafından oluşturulmaktadır.
- Kurumdan ayrılan öğrenci ve personelin kullanıcı hesapları Bilgi İşlem Daire Başkanlığı tarafından pasif hale getirilmektedir.

5.4. AYRICALIKLI ERİŞİM HAKLARI

5.4.1. AYRICALIK YÖNETİM

Ayrıcalıklar yalnızca ağ ayarları, genel internet kullanımı, uzaktan çalışma / erişim ile sınırlandırılmıştır. En az yılda bir kez gözden geçirilmekte, ayrıca işe giriş veya işten ayrılış ve görev değişikliği sebepleri ile yeniden yetkilendirmeler yapılmaktadır.

Ayrıcalık Yönetimi: Üst yöneticiler için;

- Ayrıcalıklı erişim hakkı; talep eden yönetici onayına istinaden Bilgi İşlem Daire Başkanlığı tarafından sağlanır
- Ayrıcalık yönetimi, kurum personeli tarafından talep edilmişse;
- Personel ayrıcalık talebini amirine yapar.
- Amirin kabul etmesi halinde, talep BİDB'ye gönderilir.
- Ayrıcalık erişim hakkı yönetici'nin uygun gördüğü süre boyunca erişim yetkisi verilir. Sürenin bitiminde verilen hak sistem yöneticisi tarafından kaldırılır.
- Ayrıca, kullanıcı hakları gözden geçirilerek gereksiz olarak tanımlanmış ve/veya ihtiyaç duyulmayan yetkiler kaldırılmalıdır.

Ayrıcalık Yönetimi: Hizmet sağlayıcılar için;

- Hizmet sağlayıcı ilgili birime ayrıcalık talebini yapar.
- Talep yönetici' ye gönderilir.
- Ayrıcalık erişim hakkı hizmet sözleşmesinin başlamasıyla başlar, sözleşmenin bitimiyle sonlandırılır. Bu süreç BİDB tarafından yürütülür.

5.4.2. KULLANICI HAKLARI

5.4.2.1 KONFİGÜRASYON ve GÜVENLİK AYARLARI

- Kullanıcılar, teknik olarak mümkün olsa bile bilgisayarlarındaki güvenlik ayarlarının düzeyini düşüremezler. Güvenlik ayarlarına örnek olarak;
- MS Internet Explorer etkileyen güvenlik alanları ayarları (Internet Explorer securityzone settings),
- Virüs koruma program ayarları,
- İşletim sistemi güncelleme ayarları,
- Kişisel koruma duvarı (firewall) ayarları,
- BIOS ayarları ve diğer donanımsal ve yazılım güvenlik ayarları sayılabilir.
- Kullanıcı teknik olarak mümkün olsa bile kişisel bilgisayarları üzerinden ağ servislerini (web sunucusu, veri tabanı sunucusu, FTP sunucusu vb.) çalıştıramaz.
- Bilgisayarlar üzerinde yeni kullanıcı ve kullanıcı grubu tanımlayamaz, var olan kullanıcıların haklarını ve kullanıcı gruplarını değiştiremez.
- Eğer ihtiyaçları gereği konfigürasyon ve güvenlik ayarlarının değiştirilmesi gerekiyor ise BİDB onayına sunulması zorunludur.
- Konfigürasyon ve güvenlik ayar değişiklikleri sadece BİDB tarafından ve gerekli olan süre için yapılır.