1. AMAÇ

Bu prosedürün amacı, Bursa Uludağ Üniversitesi bünyesindeki Bilgi İşlem Daire Başkanlığı kapsamındaki bilgi ve bilgi işleme tesislerine erişimin kısıtlanmasını sağlamaktır.

2. KAPSAM

Bu prosedür, Bursa Uludağ Üniversitesi bünyesindeki Bilgi İşlem Daire Başkanlığı bilgi ve bilgi işleme tesislerine erişimin kısıtlanmasını kapsamaktadır.

3. TANIMLAR VE KISALTMALAR

Özel bir tanım bulunmamaktadır.

4. SORUMLULUK

Erişim Kontrol Prosedürü düzenlenmesi ve kontrol edilmesinden Bilgi İşlem Daire Başkanlığı sorumludur.

5. UYGULAMA

5.1 Erişim Kontrolünün İş Gereklilikleri

5.1.1 Erişim Kontrol Politikası

Erişim Kontrol Politikası, BURSA ULUDAĞ ÜNİVERSİTESİ BİLGİSAYAR, AĞ VE BİLİŞİM KAYNAKLARI KULLANIM YÖNERGESİ"nde belirlenen esaslara göre belirlenir.

Varlık ve süreç sahipleri, ayrıntı miktarı ile kendi varlıkları veya süreçlerine yönelik özel kullanıcı rolleri için ve ilişkili bilgi güvenliği risklerini yansıtan kontrolleri, erişim kontrol kurallarını, erişim haklarını ve kısıtlamaları ve sıklığını belirler.

Erişim kontrolleri hem mantıksal hem de fizikseldir ve her ikisi birlikte dikkate alınır.

Kullanıcılara ve hizmet sağlayıcılara, erişim kontrolleri aracılığı ile karşılanacak iş gereksinimleri hakkında bildirimler verilir.

Erişim talepleri için www.uludag.edu.tr/bilgiislem sayfasından indirebilecek olan ilgili talep formları ile ilk amirine ıslak imza ile onaylatarak elden ya da dijital ortamda BIDB'ye iletir. BIDB uygun gördüğü talepleri gerçekleştirir ve dönüş yapar.

- İş uygulamaları ile ilgili güvenlik gereksinimleri, ilgili iş uygulamasının özelinde belirlenir,
- Erişim taleplerinin resmi yetkilendirilmesi için gereksinimler belirlenir, erişim talepleri kayıt altına alınır,
- Erişim haklarının süresi tamamlandığında kaldırılır,
- Kullanıcı kimlik bilgileri ve gizli kimlik doğrulama bilgileri kullanımı ve yönetimi ile ilgili tüm önemli olayların kayıtlarının saklanması sağlanır,
- Üniversitenin Kalite Web Sayfasından ulaşılabilen Geçici İnternet Hizmeti Talep Formu, Personel Kullanıcı Kodu Talep Formu, Birim Kullanıcı Kodu Talep Formu, Öğrenci Toplulukları, Sempozyum, Konferans,etkinlik vs. Kullanıcı Talep Formu, Kurumsal Birim Bazlı E-Posta Hesabı Yönetici Değişiklik Formu aracılığıyla hesap açma işlemleri gerçekleştirilir.

  Bu formlardan "Birim Kullanıcı Kodu Talep Formu" nun resmi elektronik belge ve yazışma sistemi olan UDOS üzerinden iletilmesi esastır. Diğer formlar ise kullanıcının görevli/ilgili olduğu birimin resmi e-posta hesabı üzerinden Bilgi İşlem Daire Başkanlığı resmi e-posta hesabı olan bidb@uludag.edu.tr adresine iletilebilir. Eksik bilgi veya eksik imza içeren hiçbir form işleme alınmaz.

5.1.2 Ağlara ve Ağ Hizmetlerine Erişim

Ağ ve ağ hizmetlerinin kullanımı ile ilgili aşağıdaki ilkeler benimsenmiştir.

- Ağ hizmetlerine erişim güvenlik duvarı üzerinden kontrol edilmektedir.
- Kurum içi kablolu ağdan internet hizmetine erişim kimlik kontrolü ile yapılır.
- Kurum içi kablosuz ağa erişim kimlik kontrolü ile yapılır.
- Misafirlerin internet erişimleri, FR 3.3.2_02 Geçici İnternet Hizmeti Talep Formu"'nun iletilmesi üzerine

tanımlanan süre boyunca sağlanır.
- Kablosuz internet erişiminde sadece WPA2 şifre algoritması kullanılır.

5.2 Kullanıcı Erişim Yönetimi

5.2.1 Kullanıcı Kaydetme, Kayıt Silme ve Yetkilendirme

Erişim haklarının atanmasını sağlamak için, resmi bir kullanıcı kaydetme ve kayıt silme prosesi uygulanır. Kullanıcı kimlik bilgisi yönetimi prosesi aşağıdaki hususları içerir:

- Üniversiteye atanan veya göreve başlayan kişilere, FR 3.3.2_03 Personel Kullanıcı Kodu Talep Formunu şahsi olarak BİDB'ye getirmesi, göreve başladığı birim üzerinden e-posta veya kurumsal yazışma programı (UDOS) üzerinden iletmesi halinde kullanıcı kimliği açılır. Kişinin kendisine özel ve tekil olan, parola politikasına uygun biçimde belirlenmiş olan geçici bir şifre tanımlanır.
- Paylaşımlı kimliklerin kullanımına sadece iş ve işletimsel nedenler için gerekli olduğundan istisnai izin verilir.
- Kurumdan ya da hesap sahibinin kendisinden yazılı talep gelmedikçe hiçbir kullanıcı kimliği kaldırılmaz.
- Personel kurumdan ayrıldığında e-posta hesabını kullanmaya devam edebilir ancak yetkili olduğu otomasyon ve uygulamalara erişim yetkisi; ilgili otomasyon ve uygulamaların süreç sahiplerince kaldırılır.
- Emekli olan personelin Kurum e-posta adresi kişi talep etmediği sürece kapatılmaz.
- Kurumdan atılan veya geçici olarak uzaklaştırılan personelin hesapları askıya alınır.
- Tüm kullanıcı kimlik talepleri onay sürecinden geçirilir ve süreç kayıt altına alınır.
- Kurumumuzdan ayrılan personelin mevcut otomasyon ve uygulamalardaki (personel otomasyonu, öğrenci işleri otomasyonu, UKEY, UDOS, vb.) mevcut yetkilerinin; personelin görevden ayrılma tarihinden itibaren yine aynı uygulama veya otomasyon üzerinden "personelin en son görev yaptığı birim yetkilileri tarafından kaldırılması/kaldırılmasının sağlanması" esas olup, bu işlemin yazılı tutanak ile kayıt altına alınması ve istenildiği takdirde iletilmek üzere biriminizde saklanması gerekmektedir.

5.2.2 Kullanıcılara Ait Gizli Kimlik Doğrulama Bilgisinin Yönetimi

Gizli kimlik doğrulama bilgisinin tahsis edilmesi, resmi bir yönetim prosesi yoluyla kontrol edilir. Bu proses aşağıdaki gereksinimleri içerir:

- Kullanıcıların gizli kimlik bilgilerini korumak için ilk kullanımda değiştirmek zorunda olacakları güvenli geçici gizli kimlik doğrulama bilgileri başlangıçta sağlanır,
- Geçici gizli kimlik doğrulama bilgileri kullanıcılara yüz yüze verilir,
- Geçici gizli kimlik doğrulama bilgileri Parola Politikasına göre oluşturulur.
- Varsayılan tedarikçi kimlik doğrulama bilgileri, sistemlerin ya da yazılımın kurulumunu müteakiben değiştirilir.

5.2.3 Kullanıcı Erişim Haklarının Gözden Geçirilmesi

Varlık sahipleri kullanıcıların erişim haklarını düzenli aralıklarla gözden geçirir. Erişim haklarının gözden geçirilmesinde aşağıdaki hususlar dikkate alınır:

-Kullanıcıların durumlarında değişiklik olması halinde (terfi, görev tanımının değişmesi, vs) uygulamalar ve otomasyonların süreç sahiplerince erişim yetkileri değiştirilir.

-Öğrencilerin mezuniyet veya ayrılma durumlarından sonra erişim kısıtlamasını uygulamalar kendi içinde sınırlamalar ile yapar.

6. İLGİLİ DOKÜMANLAR

TS ISO / IEC 27001 Bilgi Güvenliği Yönetim Sistemi
TS ISO / IEC 27002 Bilgi Teknolojisi-Güvenlik Teknikleri Bilgi Güvenliği Yönetimi için Uygulama Kuralları
FR 3.3.2_03 Personel Kullanıcı Talep Formu
FR 3.3.2_02 Geçici İnternet Talep Formu
FR 3.3.2_05 Birim Kullanıcı kodu Talep Formu
FR 3.03.2_15 Kurumsal Birim Bazlı E-Posta Hesabı Yönetici Değişiklik Formu
FR 4.2.1_16 Öğrenci Toplulukları, Sempozyum, Konferans Etkinlik vs. Kullanıcı Kodu Talep Formu