İÇİNDEKİLER

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	SEVİNÇ ÇOLAK	DİLEK ÇELİK

1 Amaç

Bu politikanın amacı, ESOGÜ BİDB bünyesinde yer alan ağ, sistem ve servislere erişim için minimum gereksinimlerin tanımlanmasıdır.

2 Kapsam

ESOGÜ BİDB kontrolünde bulunan tüm ağ, sistem ve servisler bu politika kapsamındadır.

3 Tanımlar ve Kısaltmalar

ESOGÜ: Eskişehir Osmangazi Üniversitesi
BİDB: Bilgi İşlem Daire Başkanlığı
VPN: Virtual Private Network / Sanal Özel Ağ
IP: Internet Protocol / İnternet Protokolü

4 Sorumlular

Bu politikanın oluşturulmasından Bilgi Güvenliği Birimi sorumludur. Politikanın uygulanmasından BİDB ve dış kullanıcılar sorumludur.

5 Kurallar

Politika kuralları ifade edilirken tüm ağ, sistem ve servisleri kapsayıcı bir ifade olarak "sistem" ifadesi kullanılacaktır.

5.1 Genel Kurallar

- Internet üzerinden kurumun herhangi bir yerindeki bilgisayar ağına erişen kişiler VPN teknolojisini kullanmaktadır. Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlamaktadır.
- VPN bağlantısı için Global Protect lisanslı uygulaması kullanılır.
- Uzaktan erişim yöntemi ile sunucuya erişen bütün bilgisayarlar güncel anti-virüs yazılımına sahiptir.
- Periyodik olarak yapılan kontrollerle kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların hesapları kaldırılır.
- Dış kullanıcılar ve personel için erişim izni PL.04-FR.01 - ÖZEL ERİŞİM ve UZAKTAN ERİŞİM YETKİLENDİRME FORMU" nu doldurulup idareye onaylatılarak verilir.

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	SEVİNÇ ÇOLAK	DİLEK ÇELİK

- Dış kullanıcılar için bu formda belirtilen süre kadar erişim yetkisi verilir. Bu süre sonunda eğer çalışma devam ediyorsa form(PL.04-FR.01 - ÖZEL ERİŞİM ve UZAKTAN ERİŞİM YETKİLENDİRME FORMU) yeniden doldurulur.
- ESOGÜ BİDB bünyesinde bulunan tüm sistemlere erişim için "need to know-bilmesi gereken" ve "need to use- kullanması gereken" prensibine uygun olarak erişim kontrolü uygulanır.
- Tüm sistemlere erişimde kullanıcı kimlik doğrulama için merkezi kimlik yönetimi servisi kullanılmaktadır.
- Sistem Yöneticileri tarafından ESOGÜ BİDB içinden ve dışından sistemlere erişmesi gereken tüm kullanıcılar için profiller ve kimlik doğrulama yöntemleri tanımlanmıştır.
- Kullanıcılar sistemlere kişisel bilgileri ile bağlı tekil UserID kullanılarak kaydedilir.
- Erişim yetkileri verilirken "minimum yetki prensibi" esas alınır. Bu kapsamda kullanıcıların bir noktaya erişim ihtiyacı ve hakkı açık bir şekilde ortada değilse, yetkilendirme gerekmediği değerlendirilir.
- Kullanıcılara erişim haklarının verilmesi ancak sistem yöneticilerine yazılı olarak talimat verilmesi ile mümkün olur. BİDB bünyesinde görevli personele, uygulamalara ya da sunuculara erişim yetkisi verilirken, "PL.04-FR.01 - ÖZEL ERİŞİM ve UZAKTAN ERİŞİM YETKİLENDİRME FORMU" nu doldurup idareye onaylatmalıdır.
- Kurumun bilgi güvenliği gereksinimleri göz önünde bulundurularak üçüncü taraflar ile yapılan demo ve kavram ispatı (PoC) çalışmalarında, kurum dışından erişim yetkisi verilecek kişiler için "PL.04-FR.01 - ÖZEL ERİŞİM ve UZAKTAN ERİŞİM YETKİLENDİRME FORMU" doldurulup idareye onaylatılmalıdır.
- Tedarikçiler ve dış kullanıcılar tarafından erişilen kurum varlıklarının korunmasını sağlamak, tedarikçilerin kurumun bilgi varlıklarına erişimi ile ilgili riskleri azaltmak için erişim yetkileri verilirken "minimum yetki prensibi" esas alınır.
- Kurumdan ayrılma ve bunun gibi nedenlerle erişim hakkının kaldırılması gereken kullanıcı ile ilgili işlemler en kısa sürede sistem yöneticileri tarafından yerine getirilir.
- Uygulama/sunucu vb erişim yetkilerinin iptali için ise PL.17-FR.03 - UYGULAMA ERİŞİMİ YETKİ İPTAL FORMU doldurularak işleme konulur ve takip edilir.

5.2 Veritabanı Erişim Kuralları:

- Veri tabanı kullanıcı oluşturmak için "PL.04-FR.04 - VERİ TABANI KULLANICI OLUŞTURMA TALEP FORMU" doldurulup onaylanmalıdır.
- Veri tabanı kullanıcı işlemleri ve yetkilendirilmeler için "PL.04-FR.03 - VERİ TABANI KULLANICI İŞLEMLERİ VE YETKİLENDİRME TALEP FORMU" doldurulup onaylanmalıdır.

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	SEVİNÇ ÇOLAK	DİLEK ÇELİK

5.3 Sunucu Sistemlerine Erişim Kuralları:

- Sunucuya uzaktan bağlantı yetkisi verilen personel ve dış kullanıcılar bağlantı esnasında aynı anda başka bir ağa bağlı (split tunnel- aynı anda iki vpn bağlantısı) olmadıklarından emin olunur.
- Sunucu talep edilmesi durumunda "PL.04-FR.05 - SUNUCU TALEP FORMU" sunucuyu talep eden kişi ya da birim sorumlusu tarafından doldurulup imzalanır.

5.4 Sorumluluklar:

- Kurum çalışanları bağlantı bilgilerinin gizliliğinden sorumlu olup hiç kimse ile paylaşılmaz.
- Bağlantıyı gerçekleştiren kişi bağlantı esnasında kurumun "temiz masa temiz ekran politikası" içinde belirtilen esasları dikkate alınır.
- Özel erişim etkisi verilen dış kullanıcının görevden ayrılması durumunda, bağlı olduğu firmanın durumu kuruma resmi olarak bildirilir.

5.5 Parola Gizliliği İçin Sorumluluklar

- ESOGÜ BİDB bünyesinde bulunan tüm kullanıcılar ve dış kullanıcılar kendilerine sistemlere erişim için verilen kimlik doğrulama verilerini korumaktan sorumludur.
- Kullanıcılar için; kimlik doğrulama bilgilerinin güvenli bir şekilde oluşturulması, kullanıcılara teslim edilmesi Sunucu ve İnternet Sistemleri Birimi sorumluluğundadır.

5.6 Erişim Sürecine Dair Kurallar

- Kullanıcı bilgisayarlarında, bilgisayara ağ üzerinden erişim yetkisi, sadece yönetici hesapları ve uzak masaüstü kullanıcıları veya grupları ile sınırlandırılır.
- Kullanıcılara kimlik doğrulama ve yetkilendirme için kolay kullanılabilir ve anlaşılabilir menüler/ekranlar sağlanır.
- Yetkilendirme yapılırken okuma, değiştirme, silme gibi farklı aksiyon türleri dikkate alınmalıdır.
- Kimlik doğrulama süreci deneme yanılma yöntemi gibi temel yöntemlerle devre dışı bırakılmaz.
- Belirli süre işlem yapılmadığında kullanıcılar otomatik olarak sistemden çıkarılmalıdır veya işlem yapılmayan oturumlar belirli bir süre sonra sonlandırılır.
- Erişim kontrolü yapan programların kaynak kodlarına erişim kapalı olur.

5.7 Kimlik Doğrulama ve Erişim Yönetimine Dair Kurallar

- Erişim kontrol politikaları kapsamında oluşturulan formlar ilgili kişiler ve birimler tarafından doldurulur ve onaylatılır.

- İmzalanan/onaylanan formlar destek.ogu.edu.tr üzerinden çağrıya eklenerek kayıt altına alınmalı, ıslak imzalı nüshalar birimlerce saklanır.
- Her kullanıcı için kendine ait ve kendisini benzersiz olarak tanımlayan bir kullanıcı hesabı tanımlanmalı, tüm kullanıcı hesaplarına ait bir parola ataması yapılır. Kullanıcı hesaplarına ait parolalar belirlenirken dikkat edilmesi gereken kurallar tanımlanır ve uygulanır.
- Oturum açma mekanizmasına yapılacak saldırıları engellemek amacıyla uygun güvenlik önlemleri (istek sınırlandırma, IP bloklama, CAPTCHA vb.) alınır. Başarısız oturum açma denemeleri Auditlog vb ile kayıt altına alınır.
- Kurum bilgi sistemindeki herhangi bir varlıkta varsayılan kullanıcı adı ve parolalar kullanılmaz. Test ortamlarında kullanımda olan tüm varsayılan kullanıcılar ve parolalar, canlıya alınmadan önce silinir veya değiştirilir.
- Sistem yöneticilerinin yüksek haklar gerektiren işlemleri yapmak için ayrı bir hesapları olur. Yönetici hesaplarıyla yapılan işlemler için denetim kayıtları oluşturulur.
- Sistem yöneticilerinin ve kullanıcılarının yetkileri düzenli olarak gözden geçirilmeli, görev değişikliklerinde erişim yetkileri güncellenir.
- Yerel veya uzak servis sağlayıcılarında bulunanlar da dâhil olmak üzere, kurumun tüm kimlik doğrulama sistemlerinin ve bu sistemlerle entegre uygulamaların envanteri “PL.04-FR.02 - KİMLİK DOĞRULAMA SİSTEMLERİ ENVANTERİ” formunda tutulur.
- Kurum ağına dışarıdan yapılan erişimler çok faktörlü kimlik doğrulaması ile sağlanır.
- Tüm kimlik doğrulama bilgileri güçlü kriptografik algoritmalar kullanılarak saklanmalı ve şifreli *kanallar kullanılarak iletilir.*
- Gizlilik dereceli verilerin saklandığı/işlendiği sistemler üzerinde sistem yönetimi amacıyla açılan oturumlar sırasında gerçekleştirilen faaliyetler kayıt altına alınır.
- Tüm sistem yöneticisi görevleri belirli IP adresleri kullanılarak yapılır. Yönetim işlemlerini gerçekleştiren sistem yöneticileri, sadece yönetimsel haklar gerektiren işler için ilgili hesapları kullanır.
- Veri ve parolaların güvenliğinin sağlanması gerektiğinde otomatik parola yönetim aracı (password vault) kullanılır (Keepass).

5.8 Servis hesaplarına yönelik kurallar

- Servis hesapları en az yetki prensibi göz önünde bulundurularak oluşturulur. Kullanıcı veya yetkili hesaplar servis hesabı olarak kullanılmaz. Servis hesaplarının kurum içerisinde bir sahibi olur.

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	SEVİNÇ ÇOLAK	DİLEK ÇELİK

- ESOGÜ bünyesinde bulunan Masaüstü bilgisayarlarda servis hesaplarının kullanımına yönelik kurallar "PL.04 -TL.01- KULLANICI VE YÖNETİCİ HESAPLARININ KULLANIM TALİMATNAMESİ" 'nde yer almaktadır.

6 Yaptırım

Bu politikanın ihlal edilmesi durumunda BİDB yönetimi tarafından gerekli personel desteği de alınarak ihlal nedeni incelenir. İhlal kasıtsız olup personelin eğitim vb. bir eksikliğinden kaynaklanıyorsa problemin kaynağını oluşturan eksikliği kapatmak için çalışma yapılır. Personel BİDB yönetimi tarafından e-posta üzerinden yazılı olarak uyarılır.
Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller 3'ten fazla tekrar ederse 657 sayılı devlet memurları kanunu ve Üniversite resmi yazısıyla belirtilen ilave yaptırımlar gereğince personel hakkında işlem yapılır.
Tüm çalışanlar, güvenlik ihlali olaylarını ve bu politikanın ihlallerini, Olay İhlal Yönetimi Prosedüründe tanımlanan şekilde en kısa sürede bildirme sorumluluğundadır.

7 İlgili Dokümanlar

PR.12 - OLAY İHLAL YÖNETİM PROSEDÜRÜ
PL.04-FR.01 - ÖZEL ERİŞİM ve UZAKTAN ERİŞİM YETKİLENDİRME FORMU
PL.12 - PAROLA POLİTİKASI
PL.04-FR.01 - KİMLİK DOĞRULAMA SİSTEMLERİ ENVANTERİ
PL.04 -TL.01- KULLANICI VE YÖNETİCİ HESAPLARININ KULLANIM TALİMATNAMESİ
PL.04-FR.03 - VERİ TABANI KULLANICI İŞLEMLERİ VE YETKİLENDİRME TALEP FORMU
PL.04-FR.04 - VERİ TABANI KULLANICI OLURTURMA TALEP FORMU
PL.04-FR.05 - SUNUCU TALEP FORMU
PL.17-FR.03 - UYGULAMA ERİŞİMİ YETKİ İPTAL FORMU

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	SEVİNÇ ÇOLAK	DİLEK ÇELİK