T.C. Sağlık Bakanlığı	**GİRESUN İL SAĞLIK MÜDÜRLÜĞÜ ERİŞİM KONTROL POLİTİKASI**			T.C. Sağlık Bakanlığı Giresun İl Sağlık Müdürlüğü
Kodu	**Yayınlama tarihi**	**Revizyon Tarihi**	**Revizyon No**	**Sayfa**
BG.PO.01				**1/3**

Erişim Kontrolünün Amacı, Giresun İl Sağlık Müdürlüğü ve bağlı sağlık tesislerinde bilgi ve bilginin işlendiği tüm veri erişimlerinin kısıtlanması, sadece yetki verilen kişilerin kontrollü ve kayıt altına alınarak bilgiye erişmesine imkân verecek bir sistemin tesis edilmesidir.

Politika Maddeleri:

1.Kurumun erişim sağlanacak sunucularına admin/root yetkili yönetici kullanıcılar, sudo ve runas yetkili kısıtlı yönetici kullanıcılar ve dış dünyadan erişen, uygulamayı kullanan kullanıcılardan oluşmaktadır.

2. Bakanlık sunucularına erişim için IP/SEC ya da SSL VPN kullanılmalıdır. Mümkünse kullanıcıların erişimi için SSL ve VPN tercih edilmelidir. Güvenlik Birimi tarafından sağlanmalıdır.

3. Sunuculara kullanıcı erişimi için SSH, RDP gibi protokollerle sunucu yönetimi için belirli portlar erişim verilmelidir.

4. Sunucuların kendi aralarında servis ve yönetimleri için belirli portlarla erişim sağlanması gerekmektedir.

5. Kullanıcıların sunucu yönetim için sağlanan erişimde admin/root yetkisi sistem grubu dışında verilmemelidir. Parola yönetimi bakanlık bilgi güvenliği kılavuzundaki parola yönetim politikaları ile yürütülmelidir.

6. Kullanıcıların sunucu yönetim için sağlanan erişimde merkezi kullanıcı yönetimi (MS AD, LDAP, ssh-key) ile yapılmalıdır.

7. Kullanıcıların sunucu yönetim için sağlanan erişimde sudo, runas gibi erişim kısıtlı erişim yetkileri tanımlanmalıdır.

8. Dış dünyadan sunucular üzerindeki servislere erişim için 80, 443, 7001, 8080, 8443 gibi servis portları da özel durumlarda verilmelidir. Güvenlik Birimi tarafından bu işlem sağlanmalıdır.

9. Sunucu servislerinin yönetim işlemlerinde yetkili kullanıcı bilgileri, sistem gurubuna teslim edilmelidir. Sistem birimi nezaretinde ve tarafından yürütülmelidir.

10. Sunucu servislerinin yönetim işlemleri merkezi kullanıcı yönetimi ve kısıtlı erişim yetkileriyle kullanıcılara sağlanmalıdır.

11. Kurumun yedekleme sistemlerine sadece Bilgi İşlem Biriminde çalışan memurlar erişim yapmaktadır. Firmaların yapacakları tüm işlemler sistem birimi nezaretinde yürütülmelidir.

12. Herhangi bir gizliliği olmayan, herkesin erişimine açık olan (tasnif dışı gizlilik dereceli) bilgiler için özel bir erişim kontrol tedbiri alınmasına gerek yoktur. Bu tür bilgiler, kurumların İnternet sitelerinin vatandaşlara açık bölümlerine konulabilir. Bina ve tesislerde duyuru panosu vb. ortamlarda yayımlanabilir.

13. Bilgiye verilen gizlilik derecesi yükseldikçe, uygulanacak olan erişim kontrol politikalarının sıkılaştırılması (zorlaştırılması) gerekir.

14. Bilgiye kimin hangi yetki ile erişeceği kararı, bizzat bilgi varlıklarının sahipleri tarafından verilir.

15. Bilgiye erişim talepleri ve ilgili makamlarca bu taleplere yapılan işlemlerin takip edilebilirliğini sağlamak üzere yazılı kurallar oluşturulur.

16. Erişim izinleri ile ilgili kayıtlar, varsa ilgili mevzuatta belirtilen sürelerce, yoksa varlığın sahibi tarafından belirlenecek süre boyunca saklanır.

17. Erişim izinleri verilirken, "görevlerin ayrılığı" ve "bilmesi gereken" prensiplerine göre hareket edilir.

18. "Görevlerin ayrılığı" prensibi uyarınca; kritik iş süreçlerinin gerçekleştirilmesi için birden fazla kullanıcı görevlendirilir. Bilgiye erişim için aşamalı yetkilendirme yapılarak, bir kişinin kendi başına tüm bilgi varlıklarına erişimi engellenir. Teknik nedenlerle görev ayrımı yapılamayan süreçlerin (örneğin etki alanı yöneticisi, veri tabanı yöneticisi vb.) kontrolü için ilave tedbirler alınır. Gerekiyorsa idari kontrol mekanizmaları oluşturulur.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
Celal KÖSE Bilgi Güvenliği Yetkilisi	Kamil AKTAŞ Bilgi İşlem Sorumlusu-Uzman	Mehmet ŞAHİN Personel ve Destek Hizmetleri Başkanı

19. "Bilmesi gereken" prensibi uyarınca; sistemde bulunan süreçler ve kullanıcılara, sistem kaynaklarına erişirken, kendilerine atanmış görevlerini gerçekleştirmelerine yetecek kadar yetki verilir.
20. Kullanıcıların kimliklerinin doğrulanması için asgari teknik önlem olarak, parola kullanımı zorunlu tutulur. Yapılacak risk değerlendirmesine göre daha kritik sistemler için farklı kimlik doğrulama yöntemleri (token, akıllı kart, tek kullanımlık parola, parmak izi/retina/avuç içi tarama vb.) kullanılabilir.
21. Bilgi varlıklarına yapılan erişimler için iz kayıtları oluşturulur. Erişim ile ilgili hangi kullanıcı hareketlerinin izleneceği hususu, varlık sahipleri tarafından belirlenir.
22. Sağlık Bilişim Ağı dışındaki ağlar güvensiz ağ olarak kabul edilir. Yetkisiz erişimler de dâhil olmak üzere iç ağı dış tehditlerden korumak için sınır güvenlik sistemleri (güvenlik duvarı vb.) tesis edilir.
23. Kullanıcı ve sunucuların bulunduğu ağlar, güvenlik duvarları ve/veya ağ cihazları erişim kontrol listeleri vasıtasıyla ayrılır. Veri tabanı yönetim sistemi sunucularının bulunduğu ağ kesimlerine, normal kullanıcı erişimleri engellenir.
24. Bilgi varlıklarına fiziksel olarak yapılacak erişimler için bu yönergenin A.8 maddesinde belirtilen önlemler alınır.
25. Özel nitelikli kişisel verilere (kişisel sağlık verileri) erişim için Kişisel Verileri Koruma Kurulu'nun 2018/10 sayılı kararında belirtilen teknik ve idari tedbirlerin alınmış olması gerekir.

AYRICALIKLI ERİŞİM HAKKI TALEP FORMU

KİMLİK TANIMLAMA

Ayrıcalık Talebi Yapan Personel:
Adı Soyadı:
Telefonu:
Kullanıcı Adı:
Birimi:

Değişikliği Yapan Personel:
Adı Soyadı:
Telefonu:
Birimi:

DEĞİŞİKLİK

AYRICALIKLI ERİŞİM				
Talep Edilen Ayrıcalık	Sebep	Yetki Seviyesi / Açıklama	Ekle	Kaldır
			☐	☐
			☐	☐
			☐	☐
			☐	☐
			☐	☐
			☐	☐

YETKİLENDİRME

T.C. Giresun Valiliği İl Sağlık Müdürlüğü bilgi güvenliği ve bilgi sistemlerinin kullanımına dair politikaları okuduğumu, anladığımı ve bunlara uyma sorumluluğum olduğunu ve bu ayrıcalıklı erişim hakkı isteğinin işlerimi tamamlayabilmem için gerekli olduğunu ve sadece iş amaçlı kullanacağımı beyan ederim.

Personel İmzası _____ Tarih _____

Ayrıcalıklı erişim hakkının kurum politikasına uygun ve başvuranın işlerini tamamlayabilmesi açısından gerekli olduğunu başvuranın statüsü değiştiğinde ayrıcalıklı erişim hakkının iptalini bildireceğimi, aksi takdirde bu kullanıcının ayrıcalıklı erişim haklarından doğacak zararların sorumluluğunu kabul ettiğimi beyan ederim.

Birim Sorumlusu _____ Tarih _____

Ayrıcalıklı erişim hakkı talebinde bulunan personele, erişim hakkı verilmesi uygundur.

Personel ve Destek Hizmetleri Başkanı Başkanı _____ Tarih _____