ANKARA İL SAĞLIK MÜDÜRLÜĞÜ - ANKARA DESTEK HİZMETLERİ BAŞKANLIĞI İSTATİSTİK VE BİLGİ İŞLEM BİRİMİ
29/07/2019 22:28 - 72108019 - 719 - E.1948
00098335050

T.C.
ANKARA VALİLİĞİ
İl Sağlık Müdürlüğü

Sayı : 72108019-719
Konu : Bilgi ve İletişim Güvenliği Tedbirleri Hakkında Cumhurbaşkanlığı Genelgesi

DAĞITIM YERLERİNE

İlgi : Bakanlığımız Sağlık Bilgi Sistemleri Genel Müdürlüğü'nün 25/07/2019 tarihli ve 67523305-719-67523305-719-4996 sayılı yazısı.

Sağlık Bilgi Sistemleri Genel Müdürlüğü'nün ilgi kayıtlı yazısında; bilgilerin dijital ortamda taşınması, bilgiye erişimin kolaylaşması, altyapıların dijital hale gelmesi ve bilgi yönetim sistemlerinin yaygın olarak kullanılması nedeniyle oluşan güvenlik risklerinin bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması için alınacak tedbirleri açıklamak maksadıyla, ekte yer alan 2019-12 sayılı "Bilgi ve İletişim Güvenliği Tedbirleri" konulu Cumhurbaşkanlığı Genelgesi yayınlanmış olup, ekte yer almaktadır.

Bu kapsamda; ilgili tüm kişi ve kurumlar tarafından Cumhurbaşkanlığı Genelgesi ve Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu'nda belirtilen tedbirlerin alınması hususunda;

Gereğini bilgilerinize arz/rica ederim.

e-imzalıdır.
Osman BAHÇEKAPILI
Başkan a.
Destek Hizm. Başkan Yardımcısı

Ek: 2019-12 Sayılı Cumuhurbaşkanlığı Genelgesi

Dağıtım:
Devlet Hastaneleri, EAH, ADSM ve ADSH'ler
İlçe Sağlık Müdürlükleri
Başkanlıklar ve Bağlı Birimler

Destek Hizmetleri Başkanlığı İstatistik ve Bilgi İşlem Birimi
Adres: Mehmet Akif Ersoy Mah. Bağdat Cad. No:62 Yenimahalle / ANKARA
Telefon: 0312 5924400 Faks No: +90 312 592 45 46
e-Posta: fulya.zor@saglik.gov.tr İnternet Adresi: http://www.asm.gov.tr/
Bilgi için: Fulya KIZILKUŞ
Mühendis
Telefon No: (0 312) 592 47 66
Evrakın elektronik imzalı suretine http://e-belge.saglik.gov.tr adresinden fca504df-4054-47c1-800d-f88496dabf8a kodu ile erişebilirsiniz.
Bu belge 5070 sayılı elektronik imza kanuna göre güvenli elektronik imza ile imzalanmıştır.

T.C.
SAĞLIK BAKANLIĞI
Sağlık Bilgi Sistemleri Genel Müdürlüğü

Sayı : 51317919-719
Konu : Bilgi ve İletişim Güvenliği Tedbirleri Hakkında Cumhurbaşkanlığı Genelgesi

DAĞITIM YERLERİNE

İlgi: (a) 2019/12 sayılı Cumhurbaşkanlığı Genelgesi.
(b) Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi.
(c) Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu.
(ç) Kişisel Verileri Koruma Kurulunun 2018/10 Sayılı Kararı.

Bilgilerin dijital ortamlara taşınması, bilgiye erişimin kolaylaşması, altyapıların dijital hale gelmesi ve bilgi yönetim sistemlerinin yaygın olarak kullanılması nedeniyle oluşan güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması için alınacak tedbirleri açıklamak maksadıyla ilgi (a) genelge yayımlanmıştır.

Esasen ilgi (a) genelgede yer alan hususlar da dâhil olmak üzere bilgi ve iletişim güvenliği için Bakanlık merkez birimleri ve taşra teşkilatı ile bağlı ve ilgili kuruluşlarda alınması gereken tedbirler, ilgi (b) yönerge ve bu yönergenin ayrılmaz bir parçası olarak yayımlanan ilgi (c) kılavuzda ayrıntılı olarak düzenlenmiş durumdadır. Bu kapsamda ilgi (a) genelgede yer alan ve son kullanıcı düzeyinde tüm personel tarafından hassasiyetle üzerinde durulması gereken hususlar, takip eden maddelerde sıralanmıştır.

1. Kurumsal faaliyetler ile ilgili veriler, veri aktarımı vb. maksatlarla geçici süre için olsa dahi Bakanlığımız kontrolünde olmayan depolama alanlarında (Google Drive, iCloud, Yandex Disk, We Transfer, Rapid Share) bulundurulmayacaktır. Bu amaçla kurum iç ağında tesis edilmiş ve İnternet erişimi olmayan dosya sunucuları ve/veya Bakanlığımız tarafından merkezi bir hizmet olarak işletilen ve https://sbtransfer.saglik.gov.tr/ adresinden ulaşılabilen dosya paylaşım ortamı kullanılabilecektir.

2. Mobil uygulamalar (WhatsApp, Massenger, Line, Viber, Telegram, WeChat, Skype, SnapChat vb.) ve sosyal medya platformları (Facebook, Youtube, Instagram, Twitter, Linkedln vb.) üzerinden gizlilik dereceli veri paylaşımı ve haberleşme yapılmayacaktır.

3. Kritik veri, doküman ve belgelerin bulunduğu ve/veya görüşmelerin gerçekleştirildiği çalışma odalarında/ortamlarında, mobil cihazlar ve veri transferi özelliğine sahip cihazlar bulundurulmayacaktır.

4. Gizlilik dereceli veya kurumsal mahremiyet içeren veri, doküman ve belgeler, kişilerin kendilerine ait cihazlarda (dizüstü bilgisayar, akıllı telefon, harici bellek vb.) bulundurulmayacaktır.

5. Kişilerin kendilerine ait cihazlar da dâhil olmak üzere kaynağından emin olunmayan taşınabilir cihazlar (dizüstü bilgisayar, akıllı telefon, harici bellek, CD/DVD vb.) kurum sistemlerine bağlanmayacak/takılmayacaktır.

Üniversiteler Mah. 6001. Cad. No: 9, 06800 Bilkent, Ankara
Telefon No: 0 (312) 471 83 50
İnternet Adresi: https://sbsgm.saglik.gov.tr/
Bilgi için: Erdal YILDIZ
e-Posta:erdal.yildiz2@saglik.gov.tr

T.C.
SAĞLIK BAKANLIĞI
Sağlık Bilgi Sistemleri Genel Müdürlüğü

6. Gizlilik dereceli verilerin saklandığı cihazlar, ancak içerisinde yer alan veriler donanımsal ve/veya yazılımsal olarak şifrelenmek (kriptolanmak) suretiyle kurum dışına çıkarılabilecek, bu amaçla kullanılan cihazlar kayıt altına alınacaktır. Şifreleme işlemleri için https://bilgiguvenligi.saglik.gov.tr/Home/KullaniciElKitaplari adresinde yer alan sürücü şifreleme el kitapları veya ilgi (c) kılavuzun A.7.2.6 (Dosya ve Klasör Şifreleme İşlemleri) maddesinde açıklanan araçlar kullanılabilecektir.

7. Kurumsal olmayan şahsi e-posta adreslerinden (*@gmail.com, *@yandex.com vb.) kurumsal iletişim yapılmayacak, kurumsal e-posta hesapları (*@saglik.gov.tr) şahsi amaçlarla (özel iletişim, kişisel sosyal medya hesapları vb.) kullanılmayacaktır. Belirli bir protokol veya sözleşme kapsamında çalışanlar da dâhil olmak üzere tüm Bakanlığımız personeli için kurumsal ve tüzel e-posta hesabı açılması için başvuru usulleri ilgi (c) kılavuzun A.6.5 (Merkezi Aktif Dizin ve E-Posta Sistemine Erişim) maddesinde ve https://eposta.saglik.gov.tr/ adresinde açıklanmıştır.

8. Kişisel Verileri Koruma Kurulunun ilgi (ç) kararı uyarınca özel nitelikli kişisel verilerinin (sağlık verilerinin) e-posta yoluyla aktarılması gerekiyorsa, şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması gerekmektedir.

Başta yukarıda sıralanan kişisel bilgi güvenliği tedbirleri olmak üzere, ilgili tüm kişi ve kurumlar tarafından, ilgi (a) genelge ve İlgi (c) Kılavuzda belirtilen tedbirlerin alınması hususunda gereğini bilgilerinize rica ederim.

Dr. Şuayip BİRİNCİ
Bakan a.
Bakan Yardımcısı

Ek: 2019/12 sayılı Cumhurbaşkanlığı Genelgesi (2 sayfa)

Dağıtım:
Gereği:
A1 Planı
81 İl Valiliğine

Üniversiteler Mah. 6001. Cad. No: 9, 06800 Bilkent, Ankara
Telefon No: 0 (312) 471 83 50
İnternet Adresi: https://sbsgm.saglik.gov.tr/
Bilgi için: Erdal YILDIZ
e-Posta:erdal.yildiz2@saglik.gov.tr

GENELGE

Cumhurbaşkanlığından:

Konu: Bilgi ve İletişim Güvenliği Tedbirleri

GENELGE
2019/12

Bilginin dijital ortamlara taşınması, bilgiye erişimin kolaylaşması, altyapıların dijital hale gelmesi ve bilgi yönetim sistemlerinin yaygın olarak kullanılması, ciddi güvenlik risklerini beraberinde getirmektedir. Karşılaşılan güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla aşağıdaki tedbirlerin alınması uygun görülmüştür.

1. Nüfus, sağlık ve iletişim kayıt bilgileri ile genetik ve biyometrik veriler gibi kritik bilgi ve veriler yurtiçinde güvenli bir şekilde depolanacaktır.

2. Kamu kurum ve kuruluşlarında yer alan kritik veriler, internete kapalı ve fiziksel güvenliği sağlanmış bir ortamda bulunan güvenli bir ağda tutulacak, bu ağda kullanılacak cihazlara erişim kontrollü olarak sağlanacak ve log kayıtları değiştirilmeye karşı önlem alınarak saklanacaktır.

3. Kamu kurum ve kuruluşlarına ait veriler, kurumların kendi özel sistemleri veya kurum kontrolündeki yerli hizmet sağlayıcılar hariç bulut depolama hizmetlerinde saklanmayacaktır.

4. Mevzuatta kodlu veya kriptolu haberleşmeye yetkilendirilmiş kurumlar tarafından geliştirilen yerli mobil uygulamalar hariç olmak üzere, mobil uygulamalar üzerinden, gizlilik dereceli veri paylaşımı ve haberleşme yapılmayacaktır.

5. Sosyal medya üzerinden gizlilik dereceli veri paylaşımı ve haberleşme yapılmayacaktır.

6. Sosyal medya ve haberleşme uygulamalarına ait yerli uygulamaların kullanımı tercih edilecektir.

7. Kamu kurum ve kuruluşlarınca gizlilik dereceli bilgilerin işlendiği yerlerde yayma güvenliği (TEMPEST) veya benzeri güvenlik önlemleri alınacaktır.

8. Kritik veri, doküman ve belgelerin bulunduğu ve/veya görüşmelerin gerçekleştirildiği çalışma odalarında/ortamlarında mobil cihazlar ve veri transferi özelliğine sahip cihazlar bulundurulmayacaktır.

9. Gizlilik dereceli veya kurumsal mahremiyet içeren veri, doküman ve belgeler kurumsal olarak yetkilendirilmemiş veya kişisel olarak kullanılan cihazlarda (dizüstü bilgisayar, mobil cihaz, harici bellek vb.) bulundurulmayacaktır.

10. Kişisel olarak kullanılanlar da dâhil olmak üzere kaynağından emin olunmayan taşınabilir cihazlar (dizüstü bilgisayar, mobil cihazlar, harici bellek/disk, CD/DVD vb.) kurum sistemlerine bağlanmayacaktır. Gizlilik dereceli verilerin saklandığı cihazlar, ancak içerisinde yer alan veriler donanımsal ve/veya yazılımsal olarak kriptolanmak suretiyle kurum dışına çıkarılabilecek; bu amaçla kullanılan cihazlar kayıt altına alınacaktır.

11. Yerli ve milli kripto sistemlerinin geliştirilmesi teşvik edilerek, kurumlara ait gizlilik dereceli haberleşmenin bu sistemler üzerinden gerçekleştirilmesi sağlanacaktır.

12. Kamu kurum ve kuruluşlarınca temin edilecek yazılım veya donanımların kullanım amacına uygun olmayan bir özellik ve arka kapı (kullanıcıların bilgisi/izni olmaksızın sistemlere erişim imkânı sağlayan güvenlik zafiyeti) açıklığı içermediğine dair üretici ve/veya tedarikçilerden imkânlar ölçüsünde taahhütname alınacaktır.

13. Yazılımların güvenli olarak geliştirilmesi ile ilgili tedbirler alınacaktır. Temin edilen veya geliştirilen yazılımlar kullanılmadan önce güvenlik testlerinden geçirilerek kullanılacaktır.

14. Kurum ve kuruluşlar, siber tehdit bildirimleri ile ilgili gerekli tedbirleri alacaktır.

15. Üst düzey yöneticiler de dahil olmak üzere, personelin sistemlere erişim yetkilendirmelerinin, fiilen yürütülen işler ve ihtiyaçlar nazara alınarak yapılması sağlanacaktır.

16. Endüstriyel kontrol sistemlerinin internete kapalı konumda tutulması sağlanacak, söz konusu sistemlerin internete açık olmasının zorunlu olduğu durumlarda ise gerekli güvenlik önlemleri (güvenlik duvarı, uçtan uca tünelleme yöntemleri, yetkilendirme ve kimliklendirme mekanizmaları vb.) alınacaktır.

17. Milli güvenliği doğrudan etkileyen stratejik önemi haiz kurum ve kuruluşların üst yöneticileri ile kritik altyapı, tesis ve projelerde görev alacak kritik önemi haiz personel hakkında ilgili mevzuat çerçevesinde güvenlik soruşturması veya arşiv araştırması yaptırılacaktır.

18. Kamu e-posta sistemlerinin ayarları güvenli olacak biçimde yapılandırılacak, e-posta sunucuları, ülkemizde ve kurumun kontrolünde bulundurulacak ve sunucular arasındaki iletişimin şifreli olarak yapılması sağlanacaktır.

19. Kurumsal olmayan şahsi e-posta adreslerinden kurumsal iletişim yapılmayacak, kurumsal e-postalar şahsi amaçlarla (özel iletişim, kişisel sosyal medya hesapları vb.) kullanılmayacaktır.

20. Haberleşme hizmeti sağlamak üzere yetkilendirilmiş işletmeciler Türkiye'de internet değişim noktası kurmakla yükümlüdür. Yurtiçinde değiştirilmesi gereken yurtiçi iletişim trafiğinin yurtdışına çıkarılmamasına yönelik tedbirler alınacaktır.

21. İşletmeciler tarafından, kritik kurumların bulunduğu bölgelerdeki veriler, radyolink ve benzeri yöntemlerle taşınmayacak, fiber optik kablolar üzerinden taşınacaktır. Kritik veri iletişiminde, radyolink haberleşmesi kullanılmayacak; ancak kullanımın zorunlu olduğu durumlarda veriler milli kripto sistemlerine sahip cihazlar kullanılarak kriptolanacaktır.

Güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla ulusal ve uluslararası standartlar ve bilgi güvenliği kriterleri çerçevesinde, kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerde uygulanmak üzere farklı güvenlik seviyeleri içeren "Bilgi ve İletişim Güvenliği Rehberi" Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı koordinasyonunda, ilgili kamu kurum ve kuruluşları tarafından gereken katkı sağlanarak hazırlanacak ve *www.cbddo.gov.tr* adresinde yayımlanacaktır. Rehber ihtiyaçlar, gelişen teknoloji, değişen şartlar ile Ulusal Siber Güvenlik Stratejisi ve eylem planlarında yapılacak değişiklikler göz önünde bulundurularak güncellenecektir.

Tüm kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerde yeni kurulacak bilgi sistemlerinde, Rehberde yer verilen usul ve esaslara uyulması zorunludur. Mevcut bilgi teknolojisi altyapıları, güvenlik seviyesi öncelikleri dikkate alınarak yayımlanmasını müteakip Rehberde yer alacak plan çerçevesinde kademeli olarak bu esaslara uyumlu hale getirilecektir. Uyum çalışmalarında ve yeni kurulacak bilgi sistemlerinde, belirtilen adreste yayımlanan güncel sürüm dikkate alınacaktır.

Milli güvenliğin sağlanması ve gizliliğin korunması kapsamında yürütülen görev ve faaliyetler hariç olmak üzere kurum ve kuruluşlar, Rehberin uygulanmasına ilişkin denetim mekanizmalarını oluşturacak ve yılda en az bir defa uygulamayı denetleyecektir. Denetim sonuçları ile yapılan düzeltici ve önleyici faaliyetler, Rehberde belirtilen usul ve esaslara göre bir rapor halinde Dijital Dönüşüm Ofisine iletilecektir.

Bilgilerini ve gereğini rica ederim.

5 Temmuz 2019

Recep Tayyip ERDOĞAN
CUMHURBAŞKANI