SAĞLIK BAKANLIĞI SAĞLIK BİLGİ SİSTEMLERİ GENEL MÜDÜRLÜĞÜ İZ KAYITLARI YÖNETİMİ YÖNERGESİ

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1- (1) Bu Yönerge'nin amacı, Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü tarafından işletilen bilgi sistemleri üzerinde gerçekleştirilen iş ve işlemlerin takip edilebilirliğini sağlamak maksadıyla; her seviyedeki sistem bileşeni tarafından üretilmesi gereken iz kayıtlarının asgari düzeyde içeriğini, bu kayıtların saklama süresi ve koşullarını belirlemektir.

Kapsam

MADDE 2- Bu Yönerge Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğünü kapsar.

Dayanak

MADDE 3- (1) Bu Yönerge, 10/7/2018 tarihli ve 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinin 358 inci maddesinin birinci fıkrası (a) bendine ve 508 inci maddesinin birinci fıkrasına dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4- (1) Bu Yönerge'nin uygulanmasında;

a) Bakanlık: Sağlık Bakanlığını,
b) Bilgi: Kurum için değeri olan, uygun bir şekilde korunması gereken ve bilgi sistemleri üzerinde işlenen tüm kaynakları,
c) Bilgi işleme: Veri ve bilgilerin manuel veya bir otomasyon sisteminin parçası olarak elde edilmesi, kaydedilmesi, depolanması, muhafazası, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veri ve bilgiler üzerinde gerçekleştirilen her türlü işlemi,
d) Bilgi sistemleri: Bilginin toplanması, işlenmesi, saklanması, dağıtımı ve kullanımına yönelik insan kaynağı, operasyonel faaliyetler ve süreçler ile bunlarla etkileşim içinde bulunan bilgi teknolojilerini,
e) Bilgi teknolojileri: Herhangi bir biçimdeki verinin, girişinin yapılması, saklanması, işlenmesi, iletilmesi ve çıktılarının alınması için kullanılan donanım, yazılım, iletişim altyapısı ve ilgili diğer teknolojileri,
f) Genel Müdürlük: Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğünü,
g) Genel Müdür: Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürünü,
h) İşletim güvenliği verisi: Bilgi teknolojileri tarafından donanım, yazılım veya cihazların desteklediği yetenekler çerçevesinde bilgi sistemleri iş sürekliliği, sistem işletim güvenliği ve hata ayıklama gibi maksatlarla üretilen verileri,
i) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü veriyi,

j) Kişisel sağlık verisi: Kimliği belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgileri,

k) Kritik veri: Kişisel sağlık verileri başta olmak üzere; özel nitelikli kişisel veriyi, insan kaynakları yönetimi faaliyetleri kapsamında kişilerin özlük bilgilerini, ilgili mevzuat ve kurum içi düzenlemeler gereği sır olarak saklanması gereken verileri,

l) Kurumsal veri: Kritik veriler ve işletim güvenliği verileri haricinde kalan, kişisel verileri de içeren diğer verileri,

m) Veri: Bilginin işlenmemiş halini,

n) Veri işleme: Verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olarak elde edilmesi, kaydedilmesi, depolanması, muhafazası, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veri ve bilgiler üzerinde gerçekleştirilen her türlü işlemi,

ifade eder.

İKİNCİ BÖLÜM
İz Kayıtları Oluşturma Esasları ve Saklama Süreleri

MADDE 5 – (1) Bilgi sistemlerinin ve bu sistemler vasıtasıyla yürütülen faaliyetlerin boyutu ve karmaşıklığıyla orantılı olacak şekilde, bilgi sistemleri dâhilinde gerçekleşen işlem ve olaylara ilişkin iz kayıtları alınır. İz kayıtları, işlemin doğasına uygun detay ve içerikte, asgari olarak aşağıdaki bilgileri barındırır:

a) Kaydı oluşturan sistem,

b) Kaydın oluşturulduğu tarih, saat ve zaman dilimi bilgisi,

c) Kaydı oluşturan işlem ya da olayla birlikte, varsa gerçekleştirilen değişikliğin ne olduğunu gösteren bilgi,

ç) Kaydın ilişkili olduğu tekil kullanıcıyı veya sistemi gösteren bilgi.

(2) Alınan iz bilgilerinin, yaşanan bilgi güvenliği olaylarının sonradan incelenmesine ve bunlar hakkında güvenilir delillerin elde edilmesine imkân tanıyacak nitelikte olması sağlanır.

(3) Kritik verilere; erişim, sorgulama, görüntüleme, kopyalama, değiştirme ve silme işlemleri ile bu bilgilerin işlendiği bilgi varlıklarına yönelik erişim yetkilerinin verilmesi, değiştirilmesi ve geri alınması işlemlerine ilişkin iz kayıtları asgari üç yıl boyunca saklanır.

(4) Kurumsal verilere; erişim, sorgulama, görüntüleme, kopyalama, değiştirme ve silme işlemleri ile bu bilgilerin işlendiği bilgi varlıklarına yönelik erişim yetkilerinin verilmesi, değiştirilmesi ve geri alınması işlemlerine ilişkin iz kayıtları asgari iki yıl boyunca saklanır.

(5) Başkaca bir yasal düzenleme bulunmaması halinde işletim güvenliği iz kayıtları için daha farklı saklama süreleri belirlenebilir.

ÜÇÜNCÜ BÖLÜM
Diğer Hususlar

MADDE 6 – (1) Bakanlık bilgi sistemleri tarafından oluşturulması gereken iz kayıtları ile ilgili detaylar Ek-1 Çizelge'de olduğu gibidir.

(2) İz kayıtlarının saklama koşulları, saklama süreleri, yedekleme koşulları, varsa aktarılma koşulları; ilgili sistem veya uygulamanın sahipleri tarafından belirlenir ve Ek-2 Form'a uygun olarak kayıt altına alınır.

(3) Üretilen iz kayıtlarının zamansal olarak tutarlılığını sağlamak maksadıyla iz kaydı üreten sistem ve uygulamaların zaman sunucuları ile senkronize edilmesi sağlanır.

(4) İz kayıtlarının bütünlüğünün bozulmasının önlenmesine ve herhangi bir bozulma durumunda bunun tespit edilebilmesine ilişkin gerekli tedbirler alınır.

(5) İz kayıtlarına, bilmesi gereken prensibine uygun olarak sadece erişim yetkisi verilen kişilerin ulaşabilmesi ve iz kayıtlarının yetkisiz müdahalelere karşı korunması sağlanır.

DÖRDÜNCÜ BÖLÜM
Çeşitli ve Son Hükümler

Eklerin Güncellenmesi

MADDE 7- (1) Ek-1 Çizelge ve Ek-2 Form; yasal mevzuatta meydana gelen değişiklikler, sistemsel gereksinimler ve kapsam dahilinde yer alan birimler tarafından yapılan geri bildirimler doğrultusunda Genel Müdürlük tarafından güncellenir. Güncellenen Çizelge ve Form, Genel Müdürlüğün web sayfasında yayımlanır.

Yürürlük

MADDE 8- (1) Bu Yönerge hükümleri onaylandığı tarihten altı ay sonra yürürlüğe girer.

Yürütme

MADDE 9- (1) Bu Yönerge hükümlerini Genel Müdür yürütür.

İZ KAYITLARI YÖNETİMİ YÖNERGESİ EK-1 ÇİZELGE						
Sıra No	İz Bilgisi Üreten Sistem	Kayıt Türü	Kayıt Türü Açıklaması	Zorunluluk Durumu	Üretilecek İz Bilgisi Detayı	Saklama Süresi
1	Uygulamalar	Uygulama İz Kayıtları	Otomatik olarak üretilmeyen, uygulama ihtiyaçlarına binaen uygulama geliştirici tarafından özel olarak yapılan kayıt işlemleridir. Diğer iz kayıt türlerine göre daha anlamsal veriler ve mesajlar içerebilir.	Açıklama 1 uygulanacaktır.	•Kullanıcı Id/Kullanıcı Adı: (Zorunlu) •Proje Adı/Proje Id: (Zorunlu) •Log Açıklama: (Zorunlu) •Tarih ve Saat: (Zorunlu) •Hash verisi: (Zorunlu) Log yapısında olan tüm işlemlerin Json olarak toplandıktan sonra SHA256 algoritmasına göre hash değerinin saklandığı alandır.	Yönerge m.5/3 veya m.5/4 uygulanacaktır.
2	Uygulamalar	İç Servis - API (Application Programming Interface) İz Kayıtları	Uygulama arka planında "MicroService" ya da servis tabanlı mimari gibi çok fazla servisin çalıştığı uygulamalar için kullanılır.	Açıklama 1 uygulanacaktır.	•Kullanıcı Id/Kullanıcı Adı: (Zorunlu) •Erişim Sağlanan Servis Adı: (Zorunlu) •Erişim Sağlanan Metot: (Zorunlu) •Kaynak IP: (Opsiyonel) •Gönderilen URL: (Zorunlu) •Gönderilen İstek Mesajı: opsiyonel (verinin kritikliği baz alınarak saklanmalıdır.) •Cevap Mesajı : opsiyonel (özel nitelikli kişisel verilerde saklanmalıdır) •İstek Tarih ve Saat: (Zorunlu) •Metot cevap süresi: •Hash verisi: (Zorunlu) Log yapısında olan tüm işlemlerin Json olarak toplandıktan sonra SHA256 algoritmasına göre hash değerinin saklandığı alandır.	Yönerge m.5/3, m.5/4 veya m.5/5 uygulanacaktır.
3	Uygulamalar	Dış Servis İz Kayıtları	Servisler üzerinden dış uygulamalar ile yapılan erişimleri kayıt altına almak amacıyla kullanılır.	Açıklama 1 uygulanacaktır.	•Kullanıcı Id/Kullanıcı Adı: (Zorunlu) •Erişim Sağlanan Servis Adı: (Zorunlu) •Erişim Sağlanan Metot: (Zorunlu) •Kaynak IP: (Opsiyonel) •Gönderilen URL: (Zorunlu) •Gönderilen İstek Mesajı: Opsiyonel(verinin kritikliği baz alınarak saklanmalıdır.) •Cevap Mesajı : Opsiyonel (özel nitelikli kişisel verilerde saklanmalıdır) •İstek Tarih ve Saat: (Zorunlu) •Metot cevap süresi: Opsiyonel •Hash verisi: (Zorunlu) Log yapısında olan tüm işlemlerin Json olarak toplandıktan sonra SHA256 algoritmasına göre hash değerinin saklandığı alandır.	Yönerge m.5/3, m.5/4 veya m.5/5 uygulanacaktır.
4	Uygulamalar	Uygulama Denetim (Veri Tabanı Hareketleri) Kayıtları	Uygulamada yapılan veri tabanı hareketlerini kayıt altına almak için kullanılır.	Açıklama 1 ve Açıklama 2 uygulanacaktır.	•Kullanıcı Id/Kullanıcı Adı: (Zorunlu) •Veritabanı Kullanıcı Adı: (Zorunlu) •Kaynak IP: (Opsiyonel) •İşlem Tipi: (Zorunlu) EKLEME/GÜNCELLEME/SİLME/SORGULAMA •Eski Veri: (Zorunlu) SİLME ve GÜNCELLEME işlemlerinde JSON olarak saklanacaktır. •Yeni Veri: (Zorunlu)EKLEME ve GÜNCELLEME işlemlerinde JSON olarak saklanacaktır. •Sorgu Koşulu: (Zorunlu) SORGULAMA, SİLME ve GÜNCELLEME işlemlerinde saklanacaktır. •İstek Tarih ve Saat: (Zorunlu) •Hash verisi: (Zorunlu) Log yapısında olan tüm işlemlerin Json olarak toplandıktan sonra SHA256 algoritmasına göre hash değerinin saklandığı alandır.	Yönerge m.5/3 veya m.5/4 uygulanacaktır.
5	Uygulamalar	Oturum Açma İz Kayıtları (Logon/ Logoff)	Başarılı ve başarısız kimlik doğrulama olaylarını kayıt altına almak amacıyla kullanılır.	Oturum açma işlemi varsa tutulması zorunludur.	•Kullanıcı Id/Kullanıcı Adı: (Zorunlu) •Kaynak IP: (Opsiyonel) •İstek Tarih ve Saat: (Zorunlu) •Login Başarı Durumu: (Zorunlu) •Hash verisi: (Zorunlu) Log yapısında olan tüm işlemlerin Json olarak toplandıktan sonra SHA256 algoritmasına göre hash değerinin saklandığı alandır.	Yönerge m.5/3 veya m.5/4 uygulanacaktır.
6	Uygulamalar	Hata Mesajları İz Kayıtları	Uygulamalarda oluşan hata ve datalarının kayıtlarıdır. Sistem yönetimi için gereklidir.	Tutulması zorunludur.	•Kullanıcı Id/Kullanıcı Adı: (Opsiyonel) •Sunucu Adı: (Opsiyonel) •Erişim Sağlanan Metot: (Opsiyonel) •Kaynak IP: (Opsiyonel) •Gönderilen URL: (Opsiyonel) •Hata Mesajı: (Opsiyonel) •StackTrace: (Opsiyonel)	Yönerge m.5/5 uygulanacaktır.
7	Orta Katman Yazılımları	Orta Katman Yönetim İz Kayıtları	Orta katman uygulamasının yönetimi ve izlenmesi için gerekli olan iz kayıtlarıdır.	Tutulması zorunludur.	Orta katman uygulama log kayıtları	Yönerge m.5/5 uygulanacaktır.
8	Orta Katman Yazılımları	Orta Katman Erişim İz Kayıtları	Orta katman uygulamasının erişim iz kayıtlarıdır.	Çizelge'nin 10 sıra numaralı maddesi kapsamında iz kayıtları tutulmayan erişimler için tutulması zorunludur.	•Erişim Zamanı: (Zorunlu) •Kaynak IP: (Opsiyonel) •Kaynak Port: •Hedef IP: (Zorunlu) •Hedef Adres (URL): (Zorunlu) •Hedef Port: •HTTP Durum Kodu: (Zorunlu) •İstek Metodu: (Opsiyonel)	Çizelge'nin 10 sıra numaralı maddesi kapsamında tutulmayan erişimler için 2 yıl saklanır. Bunun dışında Yönerge m.5/5 uygulanır.
9	Orta Katman Yazılımları	Orta Katman Hata İz Kayıtları	Orta katman uygulamasının hata iz kayıtlarıdır	Tutulması zorunludur.	Orta katman hata log kayıtları	Yönerge m.5/5 uygulanacaktır.
10	Ağ ve Güvenlik Sistemleri	Yer Sağlayıcı Trafik Bilgisi	Bakanlık uygulamalarına yapılan erişimleri kayıt altına almak amacıyla kullanılır.	Tutulması zorunludur.	•Erişim Tarihi: (Zorunlu) •Kaynak IP: (Opsiyonel) •Kaynak Port: •Hedef IP: (Zorunlu) •Hedef Adres (URL): (Zorunlu) •Hedef Port: •HTTP Durum Kodu: (Zorunlu) •İstek Metodu: (Zorunlu)	2 Yıl

11	Ağ ve Güvenlik Sistemleri	Kullanıcı İnternet Erişim İz Kayıtları	Kurumsal ağ üzerinden kullanıcıların internet erişimlerini kayıt altına almak için kullanılır.	Tutulması zorunludur.	•Erişim Tarihi: (Zorunlu) •Kaynak IP: (Opsiyonel) •Kaynak Mac Adresi: (Zorunlu) •Kullanıcı Adı: (Zorunlu) •Hedef Host adı: (Zorunlu) •Hedef Port: (Zorunlu) •İstek Metodu: (Zorunlu) •Uygulama Protokolü: (Zorunlu) •HTTP Durum Kodu: (Zorunlu)	2 Yıl
12	Ağ ve Güvenlik Sistemleri&Sistem Yönetim Birimi	DHCP İz Kayıtları	Kurumsal ağa bağlı olarak çalışan ve IP adreslerini DHCP vasıtası ile dinamik olarak alan bilgisayarlara verilen IP adresleri ve makine bilgilerinin eşleştirilmesi amacıyla kullanılır.	Tutulması zorunludur.	•Kiralama Tarihi: (Zorunlu) • Tahsis Edilen IP Adresi: (Opsiyonel) •İstemcinin Mac Adresi: (Zorunlu)	2 Yıl
13	Sunucu Bilgisayarları	İşletim Sistemi İz Kayıtları	Sunucu bilgisayarları üzerinde işletim sistemi seviyesinde yapılan işlemleri kayıt altına almak amacıyla kullanılır	Tutulması zorunludur.	İşletim sistemi seviyesinde oluşmuş iz kayıtları Sunucu ağ olayları ile ilgili iz kayıtları Sunucu işletim sistemi dosya erişim iz kayıtları(Opsiyonel) Sunucu hata olayları ile ilgili iz kayıtları	Yönerge m.5/5 uygulanacaktır.
14	Sunucu Bilgisayarları	Kimlik Doğrulama ve Oturum Açma İz Kayıtları (Logon/ Logoff)	Sunucu üzerinde başarılı ve başarısız kimlik doğrulama olaylarını kayıt altına almak amacıyla kullanılır.	Tutulması zorunludur.	•Kullanıcı Id/Kullanıcı Adı: (Zorunlu) •İstek Tarih ve Saat: (Zorunlu) •Login Başarı Durumu: (Zorunlu)	6 ay saklanacaktır.
15	Kurumsal E-Posta Sistemi	E-Posta İleti Takip İz Kayıtları	E-posta gönderim ve alma işlemlerinin kayıt altına alınması amacıyla kullanılır.	Tutulması zorunludur.	•Gönderen Adresi: (Zorunlu) •Alıcı Adresi: (Zorunlu) •Tarih ve Saat: (Zorunlu) •Konu: (Zorunlu) •Kaynak Ip : (Zorunlu) •Başarı Durumu: (Zorunlu) •Mesaj Boyutu :	2 Yıl
16	Kurumsal E-Posta Sistemi	Web Tabanlı E-Posta Orta Katman İz Kayıtları	E-posta gönderim ve alma işlemlerinin kayıt altına alınması amacıyla kullanılır	Tutulması zorunludur.	•Tarih ve Saat: (Zorunlu) •Kaynak Ip : (Zorunlu) •Server Ip: (Zorunlu) •Kullanıcı: (Zorunlu) •İstek: (Zorunlu) •Client Tipi: (Zorunlu)	2 Yıl
17	Veri Tabanı Yönetim Sistemi	VTYS Sistem İz Kayıtları	VTYS üzerinde sistemi yürütmek ve idamesini sağlamak için gerekli olan kayıtlardır.	Tutulması zorunludur.	• İşletim Sistemi İz Kayıtları • VTYS İz Kayıtları • Cluster İz Kayıtları(Opsiyonel) • CellNode İz Kayıtları(Oracle sistemleri için) •Hata Logları(Opsiyonel)	Yönerge m.5/5 uygulanır. Opsiyonel olanlar haricinde en az 1 ay saklanır.
18	Veri Tabanı Yönetim Sistemi	VTYS Denetim (Audit) İz Kayıtları	VTYS üzerinde kullanıcılar tarafından yapılan hareketlerin kayıt altına alınması amacıyla kullanılır.	Açıklama 2 ve Açıklama 3 uygulanacaktır.	•Veri Tabanı tanımsal ve yapısal işlemleri(DDL vb) •Veri Tabanı veri işleme işlemleri(DML vb) •Veri Tabanı yetki ve kontrol işlemleri(DCL vb)	Yönerge m.5/3 veya m.5/4 uygulanacaktır.
19	Veri Tabanı Yönetim Sistemi	VTYS Oturum Açma İz Kayıtları (Logon/ Logoff)	Veri tabanına başarılı ve başarısız kimlik doğrulama olaylarını kayıt altına almak amacıyla kullanılır.	Tutulması zorunludur.	•Kullanıcı Id/Kullanıcı Adı: (Zorunlu) •İstek Tarih ve Saat: (Zorunlu) •Login Başarı Durumu: (Zorunlu)	Yönerge m.5/5 uygulanacaktır. En az 6 ay saklanacaktır.
20	Yetkili Kullanıcı Hesap Yönetim Sistemi (YKHYS)	YKHYS İz Kayıtları	YKHYS Yöneticileri tarafından YKHYS uygulaması vasıtasıyla yapılan yönetimsel işlemler ve sistem kullanıcılarının yetkilendirildikleri kaynaklarda yaptıkları işlemleri kayıt altına almak amacıyla kullanılır.	Tutulması zorunludur.	• Yönetimsel işlemler (kullanıcı ekleme, kullanıcı silme, kullanıcı yetki güncelleme, video görüntüleme)	2 Yıl
21	Merkezi Log Yönetim Sistemi (MLYS)	Merkezi Log Yönetim Sistemi Kayıtları	MLYS yöneticileri tarafından MLYS uygulaması vasıtasıyla yapılan yönetimsel işlemleri kayıt altına almak amacıyla kullanılır.	Tutulması zorunludur.	• Yönetimsel İşlemler (kullanıcı ekleme, kullanıcı silme, arşiv verileri üzerinde yapılan EKLEME, SİLME, GÜNCELLEME, SORGULAMA, DIŞA AKTARMA)	2 Yıl
22	Son Kullanıcı Bilgisayarları	Son Kullanıcı Yerel Bilgisayar İz Kayıtları	Son kullanıcı bilgisayarlarında gerçekleşen olayların kayıt altına alınması amacıyla kullanılır	Tutulması zorunlu değildir.	Günlük Dosyaları / Bilgi Düzeyine Kadar Uygulama ve Hizmet Günlükleri/Bilgi Düzeyine Kadar (Uç Nokta Güvenlik Yazılımı İz Kayıtlarını da İçerecek Şekilde)	Yönerge m.5/5 uygulanacaktır.

Açıklamalar:

1. Uygulama iz kayıtları, iç web servis-API iz kayıtları, servis iz kayıtları, veri tabanı denetim iz kayıtları Yönerge m.5/2 kapsamında ihtiyaçların tamamını karşılayacak şekilde bir arada ya da ayrı ayrı kullanılabilir. Hangi iz kayıtlarının kullanılacağı uygulama sahibinin sorumluluğuna bırakılmıştır. Uygulama sahipleri Yönerge m.5/5 kapsamında yapılacak çalışmalarda bahsi geçen iz kayıtlarına ihtiyaç bulunması halinde ayrıca tutabilir.
2. SORGULAMA işlemini kayıt altına almak çok maliyetli olacağından başka bir alternatif olmaması durumunda tutulur.
3. Uygulama sahibi tarafından resmi olarak talep edilmesi gerekir.

İZ KAYITLARI YÖNETİMİ YÖNERGESİ EK-2 SİSTEM VE UYGULAMALAR İÇİN İZ KAYDI DETAYLARI GÖSTERİR FORM

İz Bilgisi Üreten Sistemin/Uygulamanın Adı	:
Sistemin / Uygulamanın İşletme Yönetiminden Sorumlu Birim	:
Formdaki Bilgilerin En Son Güncellendiği Tarih	:
Formdaki Bilgilerin En Son Güncelleyen Kişi	:

Sıra No	Kayıt Türü (A1)	Saklama Durumu	Saklandığı Yer	Zaman Damgası	Saklama Süresi (A2)	Yedekleme Bilgisi	Aktarım Bilgisi	Açıklamalar
1	Uygulama İz Kayıtları (A3)							
2	İç Web Servis API İz Kayıtları (A3)							
3	Servis İz Kayıtları (A3)							
4	Uygulama Denetim Kayıtları (Veri Tabanı Hareketleri) (A3)							
5	Oturum Açma İz Kayıtları (Logon/ Logoff)							
6	Hata Mesajları İz Kayıtları							
7	Orta Katman Yönetim İz Kayıtları							
8	Orta Katman Erişim İz Kayıtları							
9	Orta Katman Hata Mesajları İz Kayıtları							
10	Yer Sağlayıcı Trafik Bilgisi							
11	DHCP İz Kayıtları							
12	Kullanıcı İnternet Erişim İz Kayıtları							
13	İşletim Sistemi İz Kayıtları							
14	Kimlik Doğrulama ve Oturum Açma İz kayıtları (Logon/ Logoff)							
15	Exchange Message Tracking İz Kayıtları							
16	Exchange IIS İz Kayıtları							
17	VTYS Sistem İz Kayıtları							
18	VTYS Denetim (Audit) İz Kayıtları							
19	VTYS Oturum Açma İz Kayıtları (Logon/ Logoff)							
20	Son Kullanıcı Yerel Bilgisayar İz Kayıtları							

Açıklamalar

Genel: Bu form İz Kayıtları Yönetimi Yönergesi uyarınca iz kaydı üreten tüm sistem/uygulamalar için ayrı ayrı tutulur.

(A1) Bu formda yer alan kayıt türleri, ilgili iz kaydını üretecek kaynak dikkate alınarak farklı renkler ile gruplandırılmıştır. Formun doldurulduğu uygulama/sistem dikkate alınarak sadece ilgili satırların doldurulması yeterlidir.

(A2) Yönerge m.5'in ilgili fıkrası ve EK-1 Çizelge "Saklama Süresi" sutünü dikkate alınarak elle doldurulur. Bu alana "5 yıl", "2 yıl", "6 ay", "1 hafta", "3 gün", "50 MB disk alanı" gibi belirgin bir değer girilmesi gerekir. İz kaydı tutulan sistem veya uygulanının özelliğine bağlı olarak aynı kayıt türü içinde yer alan ancak niteliği (Yönerge m.5/3, 4 veya 5) farklı iz kayıtları bulunabileceği dikkate alınarak her biri için ayrı saklama süresi belirlenebilir. Bu durumda İlgili kayıt türünün altına yeni satırlar açılır. Her biri için detaylı bilgiler açıklamalar sütununa yazılır.

(A3) Uygulama İz kayıtları, İç Servis-API İz Kayıtları, Dış Servis İz Kayıtları, Veri Tabanı Denetim İz kayıtları ; Yönerge m.5/2 kapsamında tanımlanan ihtiyaçların tamamını karşılayacak şekilde bir arada ya da ayrı ayrı kullanılabilir. Hangi iz kayıtlarının tutulması gerektiği uygulama sahiplerinin sorumluluğuna bırakılmıştır. Uygulama sahipleri bu kayıtlardan bir ya da birkaçını, ihtiyaç olması halinde Yönerge m.5/5 kapsamında yapılacak çalışmalar için de ayrıca tutabilir.

(A4) Kısmen seçilmesi durumunda açıklamalar sütununun doldurulması gerekir.

(A5) İz kayıtlarının saklandığı yerin dosya adı ve yolu açıklamalar sütununa yazılır.

(A6) Kullanılan VTYS'nın adı, şema ve tablo bazında detaylar açıklamalar sütununa yazılır

(A7) Seçenekler arasında yer alan hiçbir şık uygulanabilir değil ise diğer seçilir ve açıklama sütununa gerekli açıklamalar yapılır.

(A8) İz bilgileri Merkezi Log Yönetim Sistemi haricinde bir başka yere aktarılıyor ise açıklama sutününa gerekli açıklamalar yazılır.