T.C.
İÇİŞLERİ BAKANLIĞI
Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü

17/06/2014

Sayı : 74185003-719-.5462?
Konu : Kimlik Paylaşımı Sistemi

T.C. NAMIK KEMAL ÜNİVERSİTESİ REKTÖRLÜĞÜ TEKİRDAĞ

Başbakanlık Teftiş Kurulu Başkanlığının 27.12.2013 tarih ve 1417 sayılı Yazıları ile gönderilen Cumhurbaşkanlığı Devlet Denetleme Kurulu Başkanlığının *"Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları"* konusunda düzenlenen Denetleme Raporunda yer alan ve Kimlik Paylaşımı Sistemi (KPS) üzerinden bilgi paylaşılan kurum ve kuruluşlarda alınması gereken güvenlik önlemlerine ilişkin tedbirler ekte gönderilmiştir.

Bu hususların değerlendirilerek gerekli tedbirlerin yerine getirilmesi hususunda,

Bilgi ve gereğini arz/rica ederim.

Seyfullah HACIMÜFTÜOĞLU
Bakan a.
Vali
Müsteşar

EK :
Yazı (1 sayfa)

DAĞITIM :
Kimlik Paylaşımı Sistemine Bağlı Tüm Kurum ve Kuruluşlara

Çamlıca Mh. 408. Cd. No:136 Pk:06200 Yenimahalle / Ankara
Telefon: (312)591 2332 Dahili: 2332 Faks: (312)397 30 78
e-posta: Elektronik Ağ: www.icisleri.gov.tr

Tedbirler

Kimlik Paylaşımı Sistemi (KPS) kapsamında bilgi paylaşılan kurum ve kuruluşlarda gerekli güvenlik önlemlerinin alınmasını temin etmek üzere;

1. Ağlarında bulunan bilgisayarların Kimlik Paylaşımı Sistemine erişiminin IP adresi bazında kısıtlanması,
2. KPS'nin kullanılacağı bilgisayar sayısı ve KPS'yi kullanmaya yetkili kişilerin sayısının belirlenmesi,
3. KPS kullanıcıların isim, soy isim ve T.C. kimlik numaralarının mutlaka kayıt altında tutulması,
4. Personelin görev ve yetkilerine göre KPS kullanıcıları arasında farklı yetkilerin tanımlanması,
5. Kullanıcıların yapmış oldukları sorguların kayıtlarının mutlaka tutulması ve bu kayıtların en az 8 yıl süreyle saklanması,
6. KPS sorgusu sonucunda elde edilen kişisel bilgilerin ayrı bir veri tabanı oluşturacak şekilde kurum sistemlerine kayıt edilecekse alınacak güvenlik tedbirlerine ilişkin detaylı düzenlemelerin yapılması,
7. KPS erişimi olan bilgisayarlar ile internet arasında mutlaka Firewall olması,
8. KPS erişimi olan bilgisayarlar ile internet arasında mutlaka Saldırı Tespit ve Önleme Cihazı (IPS) olması,
9. KPS erişimi olan bilgisayarlarda imzaları devamlı güncellenen anti-virüs programı olması,
10. KPS'ye giriş için mutlaka kullanıcı adı ve şifre kullanılması,
11. KPS erişimi olan bilgisayarlara giriş için kullanılan parolaların güvenlik için gerekli şartları taşıması ve bu güvenlik önlemlerinin yer aldığı bir parola politikasının oluşturulması,
12. KPS kullanım yetkisi verilmiş olanlara, bu sistemden sadece kurumun tanımlanmış iş ve işlemleri için sorgu yapacakları, başka amaçlar için kullanmayacakları, kullanmaları durumunda Türk Ceza Kanunu, kamu görevlisi ise ilgili disiplin hükümleri ve diğer tazminat hükümlerinin söz konusu olacağı hususunun yazılı olarak imza karşılığında mutlaka bildirilmesi,
13. KPS sistemini amacı dışında kullandığı tespit edilen personelin vakit kaybetmeksizin yetkili makamlara bildirilmesi, gerekmektedir.