



T.C.
MİLLÎ EĞİTİM BAKANLIĞI
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü

Sayı : 81576613/605/6696800

17.06.2016

Konu:Araştırma uygulama izin talebi

Sayın Hanife Güliz YAYLA
(Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü Teknikokullar/ANKARA)

İlgi: a) 17/06/2016 tarihli dilekçeniz

b) 07/03/2012 tarih ve B.08.0.YET.00.20.00.0/3616 sayılı genelge

İlgi (a) dilekçe ile Ankara Üniversitesi Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalında yüksek lisans öğrenimini devam eden Hanife Güliz YAYLA'nın "Fatih PROJESİ Uygulanan ve Uygulanmayan Okullardaki Öğretmenlerin Bilgi Güvenliği Farkındalığının İncelenmesi" konulu yüksek lisans tezi kapsamında hazırlanmış olan veri toplama aracının Iğdır, Ağrı, Malatya, Muş, Batman, Şırnak, İstanbul, Tekirdağ, Balıkesir, Muğla, Afyon, Bursa, Yalova, Ankara, Karaman, Antalya, Osmaniye, Kayseri, Yozgat, Karabük, Çankırı, Rize ve Gümüşhane illerindeki tüm okul türlerinde görev yapan öğretmenlere elektronik ortamda uygulanmasına yönelik araştırma izin talebi Genel Müdürlüğümüz tarafından incelenmiştir.

Denetimi il, ilçe millî eğitim müdürlükleri ve okul/kurum idaresinde olmak üzere, eğitim öğretim faaliyetlerini aksatmadan, gönüllülük esasına göre; onaylı bir örneği Bakanlığımızda muhafaza edilen ve uygulama sırasında da mühürlü ve imzalı örnekten elektronik ortama aktarılmış veri toplama aracının Iğdır, Ağrı, Malatya, Muş, Batman, Şırnak, İstanbul, Tekirdağ, Balıkesir, Muğla, Afyon, Bursa, Yalova, Ankara, Karaman, Antalya, Osmaniye, Kayseri, Yozgat, Karabük, Çankırı, Rize ve Gümüşhane illerindeki tüm okul türlerinde görev yapan öğretmenlere ilgi (b) genelge doğrultusunda uygulanması hususunda;

Gereğini ve bilgilerinizi rica ederim.

Bilal TIRNAKÇI
Bakan a.
Genel Müdür

Ek: Veri toplama araçları (üç sayfa)

Güvenli Elektronik İmzalı
Aslı İle Aynıdır

17 Haziran 2016

Erdoğan GÜRLER
Bilgisayar İşletmeni

Konya Yolu Nu:21/ANKARA
Elektronik Ağ: www.meb.gov.tr
atillademirbas@meb.gov.tr

Ayrıntılı bilgi için: Atilla DEMİRBAŞ
Seyda KARABULUT
Telefon:0-312-2969400/9582



9. Kaç yıldır bilgisayar kullanıyorsunuz:

10. Kaç yıldır internet kullanıyorsunuz :

11. Çalışmakta olduğunuz okulunuz FATİH Projesi kapsamında mı?

- Evet
 Hayır

Cevabınız EVET ise:

11.1 -Okulunuz hangi yıl Fatih Projesi kapsamına alındı?

- 2011 2012 2013 2014 2015 2016

11.2- Kaç yıldır bu kapsamda etkileşimli tahta ile eğitim yapıyor?

- 1 2 3 4 5 6

12- Bilgi güvenliği ve bilinçli güvenli internet eğitimi aldınız mı?

- Evet
 Hayır

Cevabınız EVET ise:

12.1- Bilgi güvenliği ve Bilinçli internet eğitimi hangi yılda aldınız?

- 2011 2012 2013 2014 2015 2016

12.2- Aldığımız Bilgi güvenliği ve bilinçli güvenli internet eğitimi yeterli buluyor musunuz?

- Evet
 Hayır

13. Bilgi Güvenliği Farkındalık Ölçeği	Kesinlikle katılıyorum(5)	Katılıyorum(4)	Kısmen katılıyorum(3)	Katılmıyorum(2)	Kesinlikle katılmıyorum(1)
Aşağıda bilgi güvenliği farkındalığına yönelik görüşlerinizi tanımlayan 67 madde bulunmaktadır. Aşağıdaki ifadelere ne derece katılıp-katılmadığınızı seçeneğin altındaki kutuya (X) işareti koyarak belirtiniz. Lütfen her soruyu dikkatli okuyunuz ve boş madde bırakmayınız.					
1. Bilgi güvenliğinin ne anlama geldiğini biliyorum.	5	4	3	2	1
2. Bilgi güvenliği ile ilgili sorumluluklarımın ne olduğunu biliyorum.	5	4	3	2	1
3. Bilgi güvenliği için şifreleri düzenli değiştirmenin gerekli olduğunu düşünüyorum.	5	4	3	2	1
4. Politika değişimi, yazılım güncellemeleri veya ilave şifreler gibi beni etkileyecek olan bilgi güvenliği değişiklikleri hakkında zamanında bilgilendiriliyorum.	5	4	3	2	1
5. Kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum.	5	4	3	2	1
6. Yönetim tarafından bilgi güvenliği gereksinimleri ile ilgili yeterince bilgilendirildiğimi düşünüyorum.	5	4	3	2	1
7. Güvenlik duvarının (firewall) ne işe yaradığını biliyorum.	5	4	3	2	1
8. Güvenlik duvarı kullanmanın korunmak için kesinlikle yeterli olduğunu düşünüyorum.	5	4	3	2	1
9. Çocukların bilgisayar güvenli kullanmaları için yapılması gerekenleri biliyorum.	5	4	3	2	1
10. Kişisel verilerimi nasıl korumam gerektiğini biliyorum	5	4	3	2	1
11. İş ile ilgili verilerimi nasıl korumam gerektiğini biliyorum.	5	4	3	2	1
12. Kötü niyetli yazılımın (malware) ne olduğunu biliyorum.	5	4	3	2	1
13. Kötü niyetli yazılımlara karşı alınması gereken güvenlik tedbirlerini biliyorum.	5	4	3	2	1
14. Aldatmaca (hoax) nedir biliyorum.	5	4	3	2	1
15. Zincir e-postalara (chain e-mail) karşı nasıl hareket etmem gerektiğini biliyorum.	5	4	3	2	1
16. Casus yazılım (spyware) nedir biliyorum.	5	4	3	2	1
17. Bilgisayarım casus yazılım olup olmadığını anlayabilirim.	5	4	3	2	1

Değerli Öğretmenim,

Bilgi güvenliğine yönelik yapılan bu çalışmadan toplanacak bilgiler bilimsel amaçla kullanılacak ve gizli tutulacaktır. Çalışmadaki ifadeleri tam ve içtenlikle doldurmanız araştırmanın sağlıklı ve güvenilir sonuçlara ulaşması ve problemi tam olarak ortaya koyabilmesi açısından önem taşımaktadır.

Katkılarınız için şimdiden teşekkür eder, çalışmalarınızda başarılar dilerim.

1. Cinsiyetiniz : () Kadın () Erkek

2. Yaşınız :

3-Branşınız

- 1 () Sınıf öğretmeni
2 () Branş öğretmeni(Branşınıza uygun alanı seçiniz):.....
() Fen Grubu(fizik, kimya, biyoloji)
() Matematik
() Yabancı Dil
() Edebiyat
() Sosyal(felsefe, tarih, coğrafya)
() Meslek Dersleri(teknik)
() Meslek Dersleri(sosyal)
() Meslek Dersleri(dil)
() Bilişim Teknolojileri/Bilgi ve İletişim Teknolojisi
3 () Diğer (Lütfen belirtiniz):

4-Kıdeminiz:

- () 5 yıl ve daha az
() 6-10 Yıl
() 11-15 Yıl
() 16-20 Yıl
() 21 Yıl ve üzeri

5-Görev yaptığınız okul aşağıdakilerden hangisidir?

- () İlkokul
() Ortaokul
() İmam-Hatip Ortaokulu
() Anadolu Lisesi
() Anadolu İmam Hatip Lisesi
() Fen Lisesi
() Çok Programlı Anadolu Lisesi
() Sosyal Bilimler Lisesi
() Spor Lisesi
() Güzel Sanatlar Lisesi
() Mesleki ve Teknik Anadolu Lisesi
() Bilim ve Sanat Merkezi
() Mesleki ve Teknik Eğitim Merkezi

6-Görev yaptığınız

İl:

İlçe:

7-Okulunuzun bulunduğu yer

- () Köy-kasaba
() İlçe merkezi
() İl merkezi
() Büyükşehir merkezi

8-Öğrenim durumunuz:

- () Lisans
() Yüksek Lisans
() Doktora
() Diğer belirtiniz:.....



18. Bilgisayarına casus yazılım yüklenmesinin engelleme yöntemlerini biliyorum.	5	4	3	2	1
19. Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum.	5	4	3	2	1
20. Sahte virüs koruma yazılımının ne olduğunu biliyorum.	5	4	3	2	1
21. Hizmet aksatma (Denial of Service - DoS) saldırısı nedir biliyorum.	5	4	3	2	1
22. Kimlik avı (phishing) saldırısı nedir biliyorum.	5	4	3	2	1
23. Sosyal mühendislik (social engineering) saldırısı nedir biliyorum.	5	4	3	2	1
24. Sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum.	5	4	3	2	1
25. Siber zorbalık (cyberbullying) nedir biliyorum.	5	4	3	2	1
26. Siber zorbalığa karşı kendimi nasıl koruyacağımı biliyorum.	5	4	3	2	1
27. Siber zorbalığa karşı çocukları nasıl koruyacağımı biliyorum.	5	4	3	2	1
28. Kişisel dijital yardımcılarının (PDAs) maruz kalabileceği saldırılara karşı alınması gereken güvenlik tedbirlerini biliyorum.	5	4	3	2	1
29. Web sayfalarında kullanılan aktif içeriğin (active content) ne işe yaradığını biliyorum.	5	4	3	2	1
30. Web sayfalarında kullanılan çerezlerin (cookies) ne işe yaradığını biliyorum.	5	4	3	2	1
31. Dijital imza (digital signature) nedir biliyorum.	5	4	3	2	1
32. Şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum.	5	4	3	2	1
33. E-posta gönderirken "Gizli" (BCC) alanının sağladığı avantajları biliyorum.	5	4	3	2	1
34. İstenmeyen elektronik posta (spam) nedir biliyorum.	5	4	3	2	1
35. İstenmeyen elektronik posta miktarını azaltmak için gerekli bilgiye sahibim.	5	4	3	2	1
36. Sosyal ağ sitelerini güvenli olarak nasıl kullanacağımı biliyorum.	5	4	3	2	1
37. USB sürücülerini kullanırken dikkat edilmesi gereken hususları biliyorum.	5	4	3	2	1
38. Taşınabilir cihazlara (portable devices) yönelik fiziksel güvenliği sağlamak ile ilgili dikkat edilmesi gereken konuları biliyorum.	5	4	3	2	1
39. Taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konuları biliyorum.	5	4	3	2	1
40. Cep telefonlarının maruz kalabileceği saldırılara karşı alınması gereken güvenlik tedbirlerini biliyorum.	5	4	3	2	1
41. Kablosuz ağların (wireless networks) güvenliği ile ilgili alınması gereken tedbirleri biliyorum.	5	4	3	2	1
42. İnternete bağlanabilen cihazlarla (internet-enabled devices) seyahat ederken dikkat	5	4	3	2	1
43. Kişisel mahremiyet nedir biliyorum.	5	4	3	2	1
44. Bilgi güvenliği konusunda yasal sorumluluklarımı biliyorum.	5	4	3	2	1
45. Bilgi güvenliği konusunda sorun yaşadığımda kime ve nereye başvuracağımı biliyorum.	5	4	3	2	1
46. İnternette gezinirken mahremiyetimi korumak için alınması gereken tedbirleri biliyorum.	5	4	3	2	1
47. Çevrimiçi güvenli alışveriş yapmak için gerekli olan güvenlik tedbirlerini biliyorum.	5	4	3	2	1
48. Mavidiş (Bluetooth) teknolojisi ile veri aktarımı konusunda bilgi sahibiyim.	5	4	3	2	1

Katılımınızdan dolayı teşekkür ederiz...

