



BİLGİ NEDİR?

20

• BİLGİ
GÜVENLİĞİ VE
FARKINDALIK

24

KURUMLARDA
BİLGİ GÜVENLİĞİ



DİJİTAL İÇERİK

Tüm içeriklere alanlarda bulunan
QR kodlardan ulaşabilirsiniz.

www.aile.gov.tr

20

• BİLGİ
GÜVENLİĞİ VE
FARKINDALIK

24

Aile ve Sosyal Hizmetler Bakanlıđımız; “toplumun her bir ferdine ulařarak etkin sosyal hizmet sunumuyla ÷lkemizin sosyal kalkınmasında öncü kurum olmak” vizyonu dođrultusunda, bireyden aileye, aileden topluma uzanan çok geniř bir kesimi kapsayacak řekilde sosyal hizmetleri ulařtırmakta ve sosyal yardımları sunmaktadır.

Bakanlık olarak sosyal adalet ve sosyal refahın sađlanmasını temin etmek amacıyla bařta kadın, çocuk, engelli ve yařlılarımız ile řehit yakını, gazi ve gazi yakınlarımız olmak üzere özel politika gerektiren vatandaşlarımıza yönelik koruyucu ve önleyici programlarımızı katılımcı anlayıřla, adil, arz odaklı ve etkin bir řekilde uygulamaktayız.

Bakanlıđımız hizmetlerinin gerçekeřmesinde emeđi geçen mesai arkadaşlarıma teřekkür ederim.

Mahinur ÖZDEMİR GÖKTAř

Aile ve Sosyal Hizmetler Bakanı



içindekiler

- 01 Bilgi Nedir?
- 02 Bilgi Güvenliđini Tehdit Eden Unsurlar
- 03 Saldırı Türleri
- 04 Tehditlere Karşı Önlemler
- 05 Kurumlarda Bilgi Güvenliđi Önlemleri Açısından Personel Yükümlölükleri
- 06 Ekler (Bakanlık Dökümanları)



Bilgi Nedir?

Bilgi kök itibariyle bilmek kelimesinden gelmektedir. Anlam itibariyle ise insan aklının alabileceği gerçek, olgu ve ilkelerin tümüne verilen addır. 'Bilmek' insanoğlunun çok önem verdiği konulardan biridir.

Hatta bilgiye verilen önem ilk insanlardan itibaren görülmektedir. İnsanlığın ilk zamanlarından itibaren din, felsefe ve ilim alanlarında bilgi çok kıymetli bir varlık olmuştur.

"Hiçbir şeyin yüzde birinin milyonda birini bile bilmiyoruz."

Thomas Edison



Günümüzde bilgi kelimesi sıkça kullanılmasına rağmen kesin bir tanım yapmak mümkün değildir. Sparrow (2008)' a göre bilgi günlük yaşamda öğreti, sezgi, his ve yargı gibi kavramlarla iç içe geçmiştir. İngilizcede kullanılan data, information, knowledge gibi kavramlarının çoğunun karşılığının dilimizde bilgi olarak karşılık bulması da kafa karışıklığını artırmaktadır. Bu terimlerin karşılığını bilgi piramidi ile anlatmak aradaki farkın anlaşılmasına yardımcı olacaktır.

Bilgi piramidine bakıldığında bilgiye ulaşmanın kolay bir iş olmadığı anlaşılır. En alt katmandan yukarıya doğru çıkmak çaba, özveri ve çalışma gerektirmektedir. Her bir aşama genellikle atlanmadan geçilir ve yukarı doğru çıkıldıkça elde bulunanın miktarı azalırken değeri inanılmaz derecede artar.





Bilgi güvenliği, bilgiye erişim yetkisi olan kişilerce, güvenilir ve daima erişilebilir bir ortamda gönderici ve alıcı arasında bozulmadan güvenli bir şekilde iletilmesi olarak tanımlanmıştır.

Bilgi güvenliği bilginin koruyucusu ve sahibine göre çeşitli şekillerde gruplanabilmektedir.



Kişisel veri güvenliği , Kişisel Verileri Koruma Kanunu'na göre (KVKK, 2018), belirli bir kimliğe sahip veya kimliği tespit edilebilir gerçek kişiye ait her türlü veri olarak tanımlanmıştır. Bu tanım çerçevesinde kişinin kimlik bilgileri, banka bilgileri, bilgisayarının ip adresi, elektronik posta adresi, fotoğrafı, eğitim bilgileri, parmak izi, sağlık bilgileri, kurum sicili, emeklilik bilgileri, sosyal medyada yazdığı yayımladığı her türlü yazı, fotoğraf, ses ve görüntü kayıtları vb. veriler kişisel veri olarak kabul edilebilir

Kurumsal bilgi güvenliği, kurumların önceden belirlenmiş bilgi varlıkları güvenlik zafiyetlerine göre bu varlıkları her türlü tehdit ve saldırılardan korumak için gerekli olan güvenlik altyapılarının oluşturulması ve tedbirlerin alınması şeklinde tanımlanabilir. Kurumsal bilgi güvenliği, sistem, teknoloji, insan, eğitim gibi pek çok faktörü tek çatı altında topladığı için yönetilmesi zor bir süreçtir. Bu süreçte güvenlik, sistem ve politikaların uluslararası standartlarda yönetilmesi, yapılandırılması ve tüm dünyada kurumsal bilgi güvenliğinin standartlaştırılması yönünde çalışmalar yapılmaktadır.

Ulusal bilgi güvenliği bir organizasyon ya da kurumun kurumsal bilgi güvenliği çalışmalarından çok daha kapsamlı olup kurumsal bilgi güvenliğinin sağlanmasındaki gerekliliklerle birlikte uluslararası işbirliği, siber suçlarla mücadele, kamu- özel işbirliği, ulusal güvenlik gibi kavramları da bünyesinde toplamaktadır.

Amaç

Bilgi güvenliği, bilgi sistemlerinin işleyişinin kesintisiz, kaliteli ve güvenilir bir şekilde devam ettirilmesini sağlamaktır. Böylece kurum ve ülke imajının zedelenmemesi güvenliğin sağlanması ile bilgi varlıklarının korunması ve yetkisiz kişilerin erişiminin engellenmesidir.

Konu

Bilgi güvenliği, bilgiyi gizlilik, bütünlük ve kullanılabilirliğine yönelik her türlü saldırı ve tehditlere karşı korumak ve bu tehditlerin yararlanabileceği güvenlik açıklarını belirleyerek önlem almaktır. İlk bakışta basit ve anlaşılır görünse de tehdit ve saldırıların çeşitlenmesi, çoğalması ve karmaşıklaşması sebebiyle bilgi güvenliğini sağlamak giderek zorlaşmaktadır.

Unsur

Bilgi güvenliği Solomon'un bilgi güvenliği üçgeninde anlattığı gibi gizlilik, bütünlük ve erişilebilirlik olmak üzere bu üç unsurun bileşimi kabul edilmekte ve bu üç unsur üzerine kurulmaktadır. Bilgi güvenliği denildiğinde akla gelen kendimize ait olan bilginin başkasının eline geçmemesidir. Aslında güvenlik sadece bilginin başkasının eline geçmemesi anlamına gelmez. Güvenlik, "gizlilik", "bütünlük" ve "erişilebilirlik" olarak isimlendirilen 3 unsurdan oluşur. Yanda listelenen 3 temel güvenlik ögesinden herhangi biri zarar görürse güvenlik zafiyeti oluşur.

Bu kapsamda, kurumsal bilgilerimizin gizliliğinin, bütünlüğünün ve Erişilebilirliğinin korunması için ISO27001 Bilgi Güvenliği Yönetim Sistemine uygun olarak çalışmalarımız devam etmektedir.



Gizlilik

Bilginin yetkisiz kişilerin eline geçmemesidir.

Bütünlük

Bilginin yetkisiz kişiler tarafından değiştirilememesidir.

Erişilebilirlik

Bilginin yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olmasıdır.

Bilgi Güvenliğini Tehdit Eden Unsurlar

Türkiye ve Dünyada internet kullanım rakamlarına bakıldığında internetin hayatımızda ne kadar yer aldığı anlaşılmaktadır. İnternet, sağladığı pek çok kolaylık, rahatlık ve avantajın yanı sıra çeşitli güvenlik sorunlarını da beraberinde getirmektedir. Bu durum kullanıcılar için birçok risk ortaya çıkarmaktadır.

Bu riskler saldırı, atak veya tehdit olarak adlandırılmaktadır. Kısaca bilgi veya bilgisayar güvenliğinde kötü niyetli kişiler tarafından yapılan saldırılardır.

Bilgi sistemini geçmek veya aldatmak, zayıflıklarını kullanmak, kişilere veya sistemlere direkt veya dolaylı olarak zarar vermek, sistemlerin sürdürülebilirliğini bozmak, durdurmak, işlemez hale getirmek gibi kötü amaçlarla yapılan eylemler saldırı veya atak olarak isimlendirilmektedir.



Saldırı Türleri

İlk zamanlar kurumlarda notların yazıldığı kâğıt çöplerini karıştırma ve parola tahmin etme gibi basit saldırıların yerini günümüzde çok daha karmaşık ve kapsamlı, çok daha detaylı, çok daha anlaşılması zor ve önlem alınması uğraştırıcı ve maliyetli saldırılar almıştır.

Çapraz Site Betikleme Saldırıları (Cross-Site Scripting XSS)

Bu saldırı türünde, kötü niyetli bir kullanıcı web uygulamasına zararlı betikler enjekte eder.

Bu betikler, kullanıcıların tarayıcılarında çalışır ve kötü niyetli eylemlere yol açabilir. Örneğin, kullanıcıların oturum bilgilerini çalmak veya kullanıcıları yanıltarak zararlı sitelere yönlendirmek için kullanılabilir.

Oto Koordineli Saldırılar

Bu saldırı türünde, saldırganlar otomatik araçlar veya botlar kullanarak hedef sistemlere karşı saldırı düzenler. Bu otomatik araçlar, saldırganların saldırıyı yönetmelerini kolaylaştırır ve saldırıyı daha etkili hale getirir.

Hizmet Aksatma Saldırıları (Denial of Service DoS)

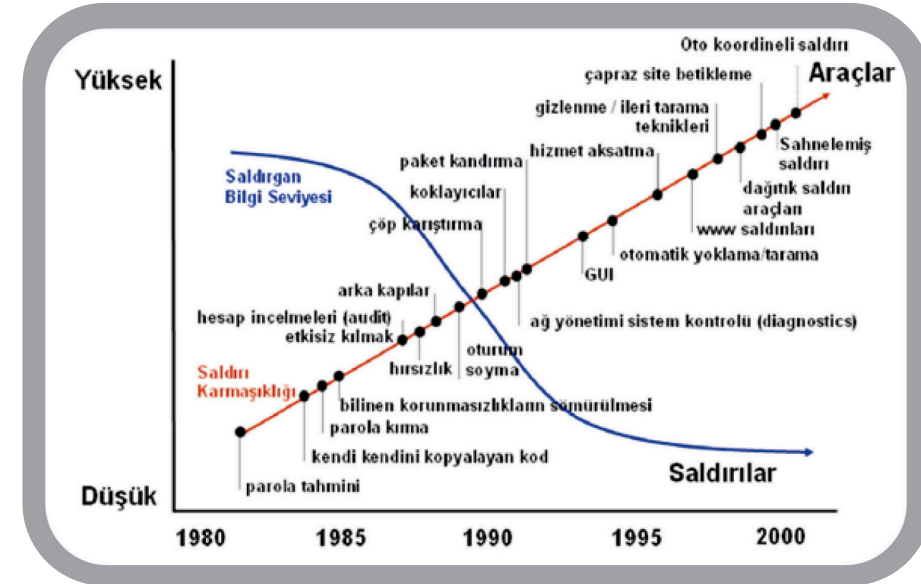
Bu, bir hizmetin normal işlevselliğinin aksamaya uğramasıdır. Bunun birçok nedeni olabilir, ancak saldırı durumunda, hizmetin hedef alındığı ve kullanıcıların normal şekilde erişim sağlayamadığı bir durum olabilir.

Dağıtık Hizmet Engelleme Saldırıları (Distributed Denial of Service DDoS)

Bu saldırı türünde, saldırganlar çok sayıda bilgisayar veya cihazı kullanarak hedef sistem veya ağa aşırı miktarda istek gönderirler. Bu, hedef sistemi normal hizmetlerini sunamaz hale getirerek, erişimi engeller.

Sahnelenmiş Saldırılar

Bu tür saldırılarda, saldırganlar saldırılarını dikkatlice planlar ve adım adım gerçekleştirirler. Bu, saldırganların hedef sistemdeki zayıf noktaları arayıp, suistimal etmek için zaman ayırarak dikkatlice hazırlık yapmalarını içerir. Bu tür saldırılar genellikle daha komplike ve etkili olabilir.





Tehditlere Karşı Önlemler

- Web sayfalarında istemsiz olarak açılan pencerelerin kapatılması
- Web sayfalarında güvenlik sertifikalarının kontrol edilmesi
- Bilgisayarda güncel güvenlik yazılımının bulundurulması
- Lisanslı işletim sistemleri ve lisanslı yazılımların kullanılması
- Bilgisayarda kullanılan yazılımların (özellikle antivirüs ve işletim sistemi) güncel olması
- Farklı amaçlar için kullanılan şifrelerin birbirinden bağımsız olması, farklı simge, rakam, karakter içermesi ve en az 8 karakterden oluşması,
- Şifre hatırlatma için kullanılan gizli soruların ve yanıtlarının zor olması
- Bilgisayarda yer alan önemli olduğu düşünülen dosyaların güvenli bir ortama yedeklerinin alınması
- Güvenli olmayan ve kaynağı bilinmeyen e-postaların açılmadan silinmesi
- Şifreli işlemlerde sayfadan 'Oturumu Kapat' komutuyla çıkılması
- E-postalarda gelen bilinmeyen web sayfalarına giriş işlemi yapılmaması
- Kablosuz ağ modemlerinin şifresiz kullanılmaması ve belirli aralıklarla değiştirilmesi.

Bilgi güvenliği üzerine yapılan çalışmalarda insan ve teknoloji faktörünün aynı oranda etkili olduğu görülmektedir. Güvenlik açıklarının çoğu kullanıcı hatalarından kaynaklanmakta, bilinçli ya da bilinçsiz olarak yapılan yanlışlar bilgi kaybına neden olmaktadır. Kötü niyetli olmanız şart değil. Belki de sadece deneme amacı ile "paylaşımları kıran programları", "port taraması yapan programları" kullandınız.

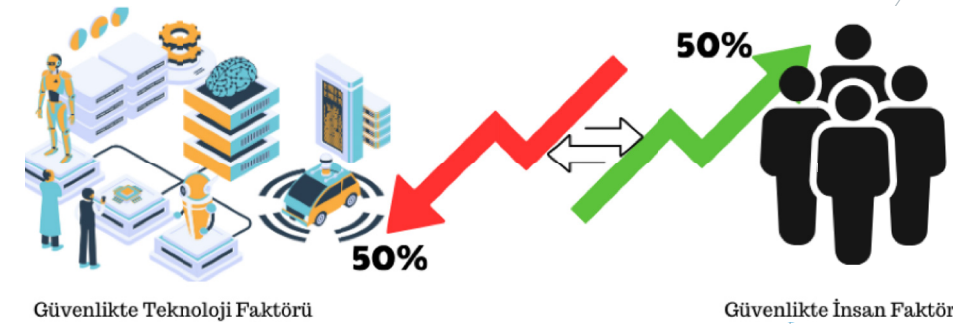
Farkında bile olmadan bilgi güvenliği açıklığı oluşturuyor olabilirsiniz. Bu durum bilgi güvenliği bilinci ve farkındalık düzeyinin yüksekliğinin kişisel veri güvenliği yanında kurumsal bilgi güvenliğini de sağladığını göstermektedir. Kurumsal bilgi güvenliğinin sağlanması da ulusal siber güvenliği getirecektir.

Sistemi içeriden yani kullanıcıdan gelebilecek hatalara ve zararlara karşı koruyan bir mekanizma yoktur. Hatta dışardan gelen saldırganın herhangi bir kullanıcı adı ve şifresi mevcut değilken, içerideki kullanıcının kullanıcı adı ve şifresiyle bazı haklara sahip olması, içerideki tehdidin önemini artırır.

Bu nedenle bilinçli kullanıcılar olmamız şart olduğu gibi, çevremizdeki kişilerin de bilinçli kullanıcılar olması için üstümüze düşeni yapmalıyız.

Kullanıcı güvenlik ihlalleri ne gibi sonuçlar doğurur?

Bir kullanıcının hatası tüm sistemi etkileyebilir.



Kurumlarda
Bilgi Güvenliđi Önlemleri
Açısından **Personelin**
Yükümlölükleri



Kurumlarda
Bilgi G¼venliđi ¼nlemleri
Açısından Personelin
Y¼k¼ml¼l¼kleri

**Gizli bilgiler
her zaman gizli
kalmalıdır!**



Kuruma ait gizli bilgiler (yasal y¼k¼ml¼l¼kler ve resmi izinler hariç) ilgili yasal d¼zenlemelerle korunur.

Kurumdan izin alınmaksızın bu bilgiler;

- Kullanılamaz,
- Başka kiřilere veya kurumlara aktarılamaz,
- Yayımlanamaz,
- İfřa edilemez,
- Kiřisel kopyalar elde edilemez.



Kurumlarda
Bilgi Güvenliği Önlemleri
Açısından Personelin
Yükümlülükleri

**Kuruma ait
bilgi ve belgeler “
gizli tutulmalıdır.**





Kuruma ait her türlü bilgi ve belge
gizli tutulmalıdır.

Personel, bu bilgileri;

- Gizli tutmak,
- Üçüncü taraflara ifşa etmemek,
- Paylaşmamak,
- Aktarmamak ve açıklamamakla sorumludur.

İnternet, bilgiye ulaşmanın en kısa ama en güvensiz yollarından biridir.

“Bazı kullanıcılar, zaten paylaştığım dosyalarımı neden koruma ihtiyacı duyayım ki” diye düşünebilir. Fakat basit bir dosya erişimi ve paylaşımı nedeni ile çok farklı problemlerle karşılaşmak mümkündür.

“Paylaştırılmış klasörler” başkasının erişimine izin verdiğiniz ve çoğu zaman dosya paylaşmak amacıyla kullandığınız klasörlerdir. Paylaştığınız bir klasöre ya da dosyaya herkesin, bütün haklarla ve kullanıcı sınırı olmadan erişmesine izin vermeniz, bu paylaşımdan gelebilecek tüm tehlikelere imkan vermeniz anlamına gelir. Sizin haberiniz olmadan aynı ağdaki bir kişi paylaştığınız dosyalara erişebilir, değiştirebilir hatta silebilir. Sizin istemediğiniz ya da bilmediğiniz kimseler tarafından da elde edilerek size ve bilgisayarınıza çeşitli zararlar verilebilir.

Yine bu gibi paylaşımlar çoğu zaman virüslerin ve zararlı yazılımların yayılmak için kullandıkları alanlardır. Başka birinin bilgisayarına bulaşmış bir virüs, sizin paylaşım alanınızdan bilgisayarınıza kolaylıkla bulaşabilir.

Kurumlarda
Bilgi Güvenliđi Önlemleri
Açısından Personelin
Yükümlölükleri

**Sosyal medyada
her şey
paylaşılmaz** //





"Kuruma ait gizli bilgiler sosyal medya platformlarında paylaşılmaz"

Sosyal medya hesaplarının kullanımında (kurumsal ve kişisel sosyal medya hesapları), görevin gerektirdiği özen ve dikkat gösterilmelidir.

Kamu Görevlilerinin Sosyal Medya Kullanımında Gözetmesi Gereken Etik İlkeler

Kamu Görevlileri Etik Kurulu 20.09.2021 tarih ve 2021/81 sayılı İlke Kararı'nda iletişim teknolojilerinde yaşanan gelişim ile bireylerin görüşlerini özgürce ifade imkanlarının çoğaldığını ve bununla birlikte etik dışı tutum ve davranışlardan kaçınmanın büyük önem arz ettiğini ifade etmiştir. Bu ilkeler;

Tarafsızlık

Kamu Hizmetine Ayrılan Zamanda Sosyal Medya Kullanımı

Paylaşılan Bilginin İçeriği

Kurum İtibarını Koruma

İnsan Haklarına Saygı

Yöneticilerin Sorumluluğu

Çıkar Çatışmasından Kaçınma

Kurumsal Sosyal Medya Hesabının Kullanımı

Kurumlarda
Bilgi Güvenliđi Önlemleri
Açısından Personelin
Yükümlölükleri

Her
uygulama
dost deđildir





Kuruma ait gizli kalması gereken bilgiler, Bakanlığımızın denetimi dışındaki depolama alanlarında (Google Drive, iCloud, Yandex Disk, We Transfer, Rapid Share vb.) bulundurulamaz.

Ayrıca, bu bilgiler mobil uygulamalar (WhatsApp, Messenger, Line, Viber, Telegram, WeChat, Skype, Snapchat vb.) ve sosyal medya platformları (Facebook, YouTube, Instagram, Twitter, LinkedIn vb.) üzerinde işlenemez. Personel, kişisel e-posta hesapları (*@gmail.com, *@yandex.com vb.) aracılığıyla da bu bilgileri aktaramaz.

Sosyal ağlarda; Kimlik Hırsızlığı, Dolandırıcılık, Profil Klonlama, İstenmeyen e-postalar, Kötü bağlantı istekleri, sahte ürün satışı vb. güvenlik tehditleri ile karşılaşılabilir.

Sosyal ağlarda en önemli husus paylaşımlardır. Paylaşmak güzeldir fakat özellikle sosyal ağlarda hangi bilginin kiminle paylaşıldığı çok önemlidir. Çünkü;

Paylaşılan her türlü bilgi paylaşan tarafından silinse dahi internet ortamında silinmeden kalabilmektedir.

Paylaşımlar kolaylıkla gönderilebilir ancak, kolaylıkla geri alınamayabilir.

Unutulmamalıdır ki, İnternet ortamında bilinçsiz kullanıma bağlı olarak en büyük güvenlik tehdidi bizzat kullanıcının kendisi olmaktadır. Bu nedenle özellikle sosyal ağları yoğun bir şekilde kullanan her kullanıcının gerekli güvenlik ve gizlilik tedbirlerini alması gerekmektedir.

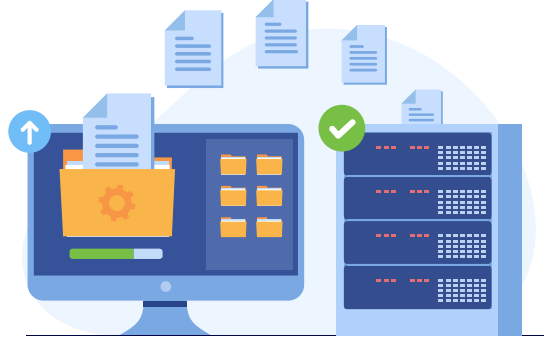


Kurumlarda
Bilgi Güvenliđi Önlemleri
Açısından Personelin
Yükümlölükleri

**Sanal izler
kaybolmaz**

“





Kurum tarafından onaylanmış sistemler, uygulamalar, kullanıcı faaliyetleri ve bilgi sistem ağındaki verilerin ve veri akışının iz kayıtları, hukuki ve idari süreçlerde kullanılmak üzere toplanır. Ayrıca, sistemlerin güvenli bir şekilde işletilmesini sağlamak amacıyla da toplanır.

Kurum tarafından sağlanan İnternet erişimi kayıtları, 5651 sayılı Kanun gereğince öngörülen süreler boyunca tutulur.

Usulüne uygun olarak kayıt altına alınan işlemlerdeki yasal sorumluluk, ilgili kullanıcıya aittir.

Loglama Sistemi

İnternet hizmet sağlayıcı tarafından verilen IP adresi ile cihazların İnternet gezintilerinin kaydedilmesi prensibine dayanır. NAT (Ağ Adresi Çevrimi) sayesinde, yerel IP adresleri public IP adresine dönüşür ve İnternete bu IP üzerinden çıkarılır. Loglama sayesinde, hangi kullanıcıların ne zaman, hangi private IP adresi ile bağlandığı takip edilebilir.

IP adresi, farklı rakamlardan oluşan ve İnternete bağlanan cihazlara İnternet sağlayıcılar tarafından otomatik olarak atanan çok haneli numaralardır.

Cihazların tekertekertanımlanabilmelerini sağlayan IP adresi için bilgisayarların kimlik numaraları ya da sanal parmak izleri de denebilir.

Çalışanlar, kendilerine tahsis edilen kullanıcı adı/parola ikilisi ve/veya IP/MAC adresini kullanılarak gerçekleştirilen her türlü etkinlikten kişisel olarak sorumludur.

Aynı şekilde kurum bilişim kaynakları kullanılarak oluşturulan ve/veya tahsis edilen bilişim kaynağı üzerinde bulundurulanan her türlü bilgi, belge, doküman, yazılım vb. içeriğinden ilgili kişi şahsen sorumludur.



Kurumlarda
Bilgi Güvenliđi Önlemleri
Açısından Personelin
Yükümlölükleri

**Teknolojik
aletleri
kullanırken
dikkat!**

//





Çalışanlar, kurum tarafından kendisine verilen bilgisayar, tablet, telefon, taşınabilir medya gibi cihazları sadece göreve yönelik, kurumsal faaliyetler için kullanır. Yürütülecek adli ve idari soruşturmalar kapsamında olmak şartıyla, söz konusu cihazlar ve çalışanların kurum bilişim sistemleri üzerinde yapmış olduğu işlemler, ilgili personele ayrıca herhangi bir bilgilendirme yapılmaksızın kontrol edilebilir.

Bilhassa güvensiz ortamlarda, kurum bilgisayarlarının fiziki güvenliği için azami çaba sarf edilir.

Çalışanlar, bilgisayarlarını kendilerine tahsis edilen kullanıcı adını ve parolayı oturum açmak için kullanır.

Çalışma sona erince ilgili oturum veya bilgisayar kapatılarak, üçüncü kişilerin bilgisayardaki bilgilere erişimi engellenir.

Mobil uygulama izinlerinin iyi yönetilmesi önemlidir. Her uygulamanın, işlevi için gerekli olmayan izinlere sahip olmaması gerekir. Bu, kişisel verilerinizi gereksiz yere riske atmamak için önemlidir.

Mobil cihazlarda bulunan ve çoğu kullanıcı tarafından kullanılan ekran kilidi, telefon, tablet ve bilgisayar gibi cihazları yetkisiz erişime karşı korur. Parmak izi tanıma, yüz tanıma veya PIN kodu gibi farklı ekran kilidi seçenekleri vardır.

Mobil cihazlar genellikle Wi-Fi ve Bluetooth gibi kablosuz iletişim teknolojilerini kullanır. Bu teknolojilerin sürekli açık olması, cihazın saldırılara karşı daha savunmasız hale gelmesine neden olabilir. Bu yüzden kullanılmadığında bu özelliklerin kapatılması gereklidir.

Kurumlarda
Bilgi Güvenliđi Önlemleri
Açısından Personelin
Yükümlölükleri

**Kullanıcı adı
ve parola
paylaşılmaz**

”





Çalışanlara tahsis edilen kullanıcı adı ve parola bilgileri hiçbir şekilde üçüncü kişiler ile paylaşılmaz.

Kurumumuzda birçok sistemimize ve en azından bilgisayarlarımıza erişmek için parola kullanılmaktadır. Bu sayede sadece yetkisi olan kişilerin sistemlere ve bilgisayarlara erişebilmesi sağlanmaktadır. Yetkisiz erişimden korunmak için etkin parola kullanımı önem arz etmektedir.

Parolaların Ele Geçirilmesi

Parolalar genel olarak iki şekilde ele geçirilebilir.

- » Tahmin ederek ya da deneme yanılma yolu ile ele geçirilebilir.
- » Parolanızın çalınması ile yani hırsızlık yaparak ele geçirilebilir.

Olası Senaryolar

- » Tanıdığınız bir kişi sizin hakkınızda bildikleriyle parolanızı tahmin edebilir.
- » Tanımadığınız bir kişi ise herkesin sık kullandığı bilinen, basit parolaları deneyerek şifrenizi bulabilir.
- » Parolanızı bulmak isteyen kişi özel programlar kullanarak sık kullanılan yüzlerce parola örneğini ya da sözlüklerdeki binlerce kelimeyi hızlıca deneyerek parolanızı belirleyebilir.
- » İyi korunmayan, yazılı ya da sözlü olarak paylaşılan parolalar, yazılı bulunduğu ortama ulaşılarak ya da kulak misafiri olunarak ele geçirilebilir.
- » Bilgisayar virüsleri gibi zararlı programlar bilgisayardaki işlemlerinizi izleyerek parolanızı ele geçirebilir.

Parolanızı ele geçirdiklerinde ne yapmalıyız?

Parolanız başkası tarafından ele geçirilirse veya böyle bir şüpheniz varsa;

- » İlk işiniz parolanızı değiştirmek olmalıdır.
- » Eğer aynı parolayı ya da çok benzerlerini başka sistemlerde de kullanıyorsanız, diğer parolalarınız da değiştirilmelidir.
- » Bu durumdan etkilenebilecek diğer kişilere haber vermeniz olası başka problemleri önlemenize de yardımcı olacaktır.
- » Benzer problemleri tekrar yaşamamak için, yeni oluşturacağınız parolalar, tahmin edilmesi zor, yani güçlü parolalar olmalıdır.

Güçlü Parola Oluşturma

- » Tahmin edilmesi kolay olmayan ya da deneme yanılma yolu ile ele geçirilmesi oldukça zor olan parolalara güçlü parola denir.
- » Oluşturulan bir parolanın “güçlü” kabul edilebilmesi için aşağıdaki özellikleri göstermelidir.
- » En az 8 karakterden oluşur.
- » Harflerin yan sıra, rakam ve “?, @, !, #, %, +, -, *, %” gibi özel karakterler içerir.
- » Büyük ve küçük harfler bir arada kullanır.
- » Bu krallara uygun parola oluştururken genelde yapılan hatalardan dolayı saldırganların ilk olarak denedikleri parolalar vardır. Bu nedenle parola oluştururken aşağıdaki önerileri de dikkate almak gerekir.
- » Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır. (Örneğin doğum tarihiniz, çocuğunuzun adı, soyadınız, ... gibi)
- » Sözlükte bulunabilen kelimeler parola olarak kullanılmamalıdır.
- » Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş parolalar kullanılmamalıdır.

Parolaların Korunması

Güçlü parolalar vermek gerekli ama yeterli değildir. Verdiğiniz parolanın korunması ve paylaşılmaması da bir o kadar önemlidir. Parolanızı korumak için:

- » Kâğıt ya da elektronik, herhangi bir ortamda açıkça yazılmış olarak bulundurulmamalıdır. Yazılı bulundurulması gerektiğinde saklanan ortamın güvenliği sağlanmalı ve parolalar kilit altında saklanmalıdır.
- » Farklı sistemlerde farklı parola kullanılması olası riskleri azaltacaktır.
- » Parolalar belirli aralıklarla değiştirilmelidir.
- » Tüm bunlar, uygulaması basit tedbirler olsa da, bu konuda çok sıklıkla hatalar yapılmakta ve dikkatsiz davranılmaktadır.



Kurumlarda
Bilgi Güvenliđi Önlemleri
Açısından Personelin
Yükümlölükleri

Yasal Sorumluluklar

//





Bilişim suçu;

bilgisayar, çevre birimleri (yazıcı, faks vb.), pos makinesi, cep telefonu gibi her türlü teknolojinin kullanılması ile işlenen suçlardır. Bilgi Güvenliği Yönetim Sistemi kapsamında hazırlanan politika ve prosedürler hem kurumsal bilgileri hem de çalışanları korumak amacıyla hazırlanmıştır.

Politika ve prosedürlerde yer alan sorumluluklarımızı yerine getirmezsek Türk Ceza Kanununun ilgili yasa ve Hükümleri gereğince hakkımızda yasal işlem başlatılır.

Bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme, tüzel kişiler hakkında güvenlik tedbiri uygulanması, banka ve kredi kartlarının kötüye kullanılması kapsamındaki suçları tanımlayan kanun maddeleri TCK'nin 243 -246. maddelerinde yer almaktadır.

Ayrıca, Bilişim Vasıtalı Suçlar, Fikri ve Sanat Eserleri Kanunu, Ceza Muhakemesi Kanunu ve 5651 Sayılı Kanun gibi birçok kanun maddesi bilgisayar, çevre birimleri (yazıcı, faks vb.), pos makinesi, cep telefonu gibi cihazlar kullanarak işlenen suçlar ile ilgili yaptırımları içermektedir.



Kurumlarda
Bilgi Güvenliđi Önlemleri
Açısından Personelin
Yükümlölükleri

Sosyal Mühendislik

“





Bilgi güvenliği bağlamında sosyal mühendislik, eylemleri gerçekleştirmeye veya gizli bilgileri ifşa etmeye yönelik olarak insanların psikolojik manipölasyonudur. Çoğu kişi, kandırılma olasılığının çok düşük olduğunu düşünür ve genellikle güvenlik gündeme geldiğinde teknik tedbirlerden bahseder. Oysa bilgi güvenliği sağlanırken insan faktörünün payı teknik önlemlerden çok daha büyüktür!

“

Bu yanlış inancın farkında olan saldırganlar, isteklerini o kadar akıllıca sunar ki hiç kuşku uyandırmadan, kurbanın güvenini kazanıp, kolaylıkla istedikleri bilgiye ulaşabilirler.

“Bilmesi Gerektiği Kadar” prensibine dikkat edilmelidir.

Kimliğinden emin olunmayan kişiler ile telefon ya da e-posta ile bilgi paylaşılmamalıdır.

Şüphelenilen e-postalara cevap verilmemeli hatta açılmamalıdır.

Sosyal medya kullanırken dikkat edilmelidir. Meşru kullanıcılar (bankalar, diğer kamu kurumları, Bilgi İşlem Dairesi Başkanlığı vb.) “ASLA” sizden kullanıcı adınızı ve parolanızı istemezler.

Sosyal mühendislik saldırılarına karşı her zaman temkinli olmalıyız.

Sosyal mühendislerin başarılarının sırrı insanların aldatılmaya fazlasıyla açık olmasıdır. Çünkü insanlar belli şekillerde yönlendirildiklerinde yanlış şeylere güven duyabilirler.

Başarılı bir sosyal mühendis, kurbanın sorabileceği soruları önceden tahmin eder ve bu sorulara karşı daima hazırlıklı olur.

Önce problem yaratıp, sonra da yardımcı olmayı teklif etmek sosyal mühendislerin sıklıkla uyguladıkları bir yöntemdir.

Saldırganlar bazen kendini acındırarak kurbandan yardım ister.

“

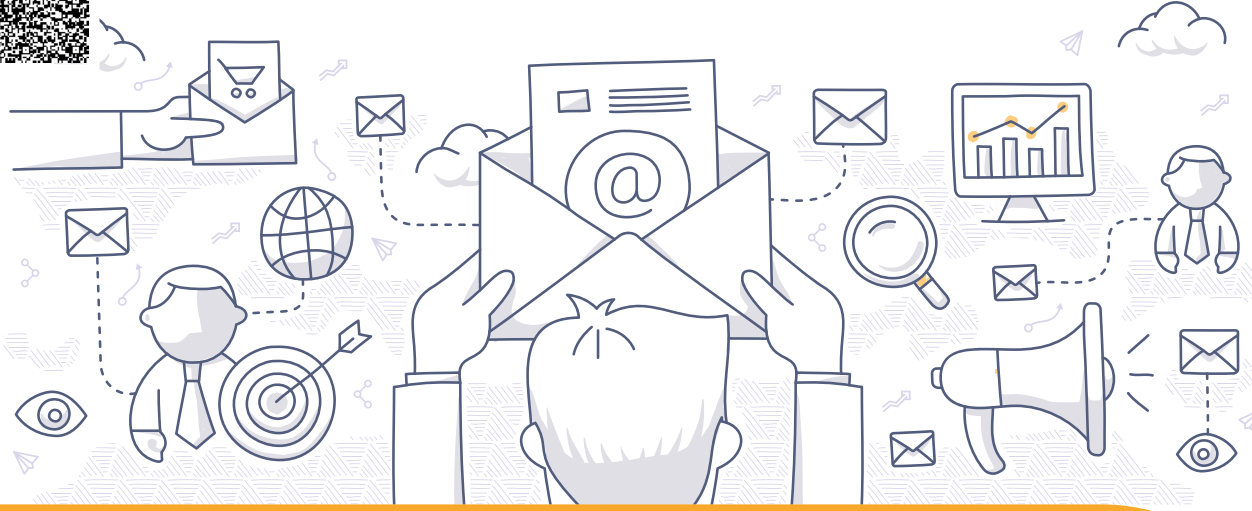
*Yardım talebini reddetmek ne zordur değil mi?
Sonuç ise “Hep Başarı”!
Sonuç olarak çalışanların kendi hataları sonucunda kullanıcı adı ve parolalarının deşifre olması halinde, bu bilgiler kullanılarak yapılan iş ve işlemlerden, şahsen sorumlu tutulabilirler.*



Kurumlarda
Bilgi Güvenliđi Önlemleri
Açısından Personelin
Yükümlölükleri

**Kurumsal eposta
hesabı başka amaçlar //
dođrultusunda
kullanılamaz**





Çalışanların kullanımına sunulan **@aile.gov.tr** uzantılı kurumsal e-posta hesapları, sadece iş ve işleyiş için kullanılır.

Bu e-posta adresleri kişisel amaçlar doğrultusunda kullanılamaz. (sosyal medya hesapları, banka hesapları vb.)

“

Kurum içindeki veya dışındaki kişilere iş ile ilgili olmayan toplu ve/veya kişisel e-posta gönderilmez. Çalışanlar, kurum içine veya kurum dışına göndermiş oldukları tüm e-postalardan kişisel olarak sorumludur.

Spam

Önemsiz postanın elektronik eşiti olarak, istenmeyen ticari e-posta olarak tanımlanabilir. Spam, birçok insana gönderilerek, belli bir yüzdenin buna cevap vermesi ya da belli bir görevi yerine getirmesi beklenir.

Oltalama (Phishing)

Bireylerden kullanıcı adı, şifre, kredi kartı bilgileri, vs. gibi hassas bilgileri almak için e-postaları kullanır. Phishing'i başarılı yapan şey, failerin Google ya da Paypal gibi tanınmış şirketleri, meşru görünür bir şekilde taklit etmeleridir.

Bu e-postalar suç değildir, ama phishing, vs. ile bağlantılı olarak kullanılabilirler. E-posta hizmet sağlayıcılarının çoğunda spamleri tespit etmek için sistemler vardır, ancak tam olarak kullanışlı değildirler ve birçok spam e-posta bu sistemlerden tespit edilemeden geçmeye devam eder.

“

! Spam ve oltalama gibi şüphelendiğiniz mailleri some@aile.gov.tr adresine bildirebilirsiniz.



Kurumlarda
Bilgi Güvenliđi Önlemleri
Açısından Personelin
Yükümlölükleri

İzinsiz
donanım ve
yazılımlara
dikkat!

//





SOCIAL MARKETING

Çalışanlar, kendilerine tahsis edilmiş yazılım, donanım, araç ve gereçlerin üzerinde; kurum bilgisi dışında mekanik (donanım ekleme, kaldırma vb.) ve/veya yazılımsal değişiklik (yeni yazılım yükleme, kurum tarafından koyulan bir kısıtlamayı aşmak üzere bilgisayar ayarlarını değiştirme vb.) yapamaz.

SOCIAL MARKETING

Personeller, kurum tarafından yüklenen işletim sistemi ve uygulama yazılımları haricinde, ilgili birimlerin bilgisi dışında başka yazılımları yükleyemez. Kurum tarafından yüklenmemiş yazılımlardan doğacak sorumluluk, ilgili bilgisayarın sahibine aittir.

Kurumlarda
Bilgi Güvenliđi Önlemleri
Açısından Personelin
Yükümlölükleri

**Kişisel
verileriniz
güvende mi?**

“





“

Çalışanlar, kişisel veri ihlâline ilişkin herhangi bir bilgi alır veya tespitte bulunur ya da bu konuda şüphe duymasını gerektirecek nitelikte bulgularla karşılaşursa,

Bu durumu

**24 saatten geç olmamak üzere
en kısa sürede Bilgi Teknolojileri
Genel Müdürlüğüne ve
some@aile.gov.tr adresine bildirir.**

Bildirimin geç yapılması nedeniyle veri koruma mevzuatında öngörülen 72 saatlik süreye riayet edilememesi durumunda personelin idari sorumluluğu doğabilir.

6698 Sayılı Kişisel Verilerin Korunması Kanunu' nun Amacı Nedir?



Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.

Bu Kanun uygulamasında, Kanun'da belirtilen istisnalar haricinde, kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemeyecek; üçüncü kişilere ve yurtdışına aktarılamayacaktır.



Bunları Biliyor Musunuz?

“

Arıza, yardım ve önerilerinizi
ASHB Yardım Merkezine
jira.aile.gov.tr
bildirebilirsiniz.

**Karantinaya alınan,
sizlere ulaşamayan
mailleriniz için**
karantina@aile.gov.tr
adresi ile iletişime
geçebilirsiniz.

Sosyal mühendislik saldırıları, virüs, zararlı yazılım, sahte ve dolandırıcılık amaçlı e-posta gibi durumlarla karşılaştığınızda

some@aile.gov.tr ve **bg.iletisim@aile.gov.tr**

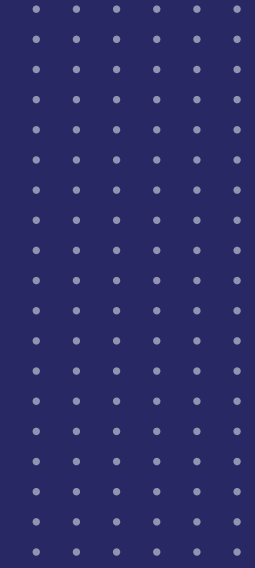
adresleri üzerinden bizlerle iletişime geçerek en kısa zamanda bilgilendiriniz.

Siber Olaylarla Mücadele Ekiplerinin Kuruluş, Görev ve Çalışmalarına dair esaslar kapsamında bakanlığımızda bir SOME ekibi bulunmaktadır. Herhangi bir siber olayla karşılaştığınızda ya da şüphelendiğinizde lütfen genel müdürlüğümüze bildiriniz.

Dosya paylaşım işlerinizi için wetransfer, shareit vb. uygulamaları kullanmayınız.

Bakanlığımıza ait bilgi güvenliği içerikli eğitim, doküman vb. içeriklere e-kilavuz.aile.gov.tr adresinden ulaşabilirsiniz.

Kurumumuzda bilgi işlem faaliyetlerini güvenli ve planlı bir şekilde yürütmek için Bilgi Güvenliği Yönetim Sistemi uygulanmaktadır.



Ekler

“

EK-1

Aile ve Sosyal Hizmetler Bakanlığı Bilgi Güvenliği Politikaları Yönergesi

AİLE VE SOSYAL HİZMETLER BAKANLIĞI BİLGİ GÜVENLİĞİ POLİTİKALARI YÖNERGESİ

BİRİNCİ BÖLÜM Genel Hükümler

Amaç

Madde 1- (1) Bu Yönergenin amacı; Aile ve Sosyal Hizmetler Bakanlığının görevi ve konumu nedeniyle sahip olduğu elektronik ortam ve bilgilerinin paylaşımı ve güvenliği konularında bilgi çağı gereklerine uygun olarak tedbir almak, bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek, içeriden ve/veya dışarıdan gelebilecek kasıtlı veya kazayla oluşabilecek tüm tehditlerden korunmasını sağlamak ve yürütülen faaliyetleri etkin, doğru, hızlı ve güvenli olarak gerçekleştirmektir.

Kapsam

Madde 2- (1) Bu Yönerge, Aile ve Sosyal Hizmetler Bakanlığına bağlı merkez ve taşra teşkilatında bulunan bütün birimlerdeki personelin ve ilgili üçüncü taraf firma/personelin bilgi sistemleri kullanımına yönelik kurumsal ve kişisel bilgi güvenliği ilke ve kurallarını kapsamaktadır.

Hukuki Dayanak

Madde 3- (1) Bu Yönerge, 10/7/2018 tarih ve 30474 sayılı Resmi Gazetede yayımlanan 1 sayılı Cumhurbaşkanlığı Kararnamesinin 65 ve 66 ncı maddelerine, 4/5/2007 tarih ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 6 ncı maddesine, 24/3/2016 tarih ve 6698 sayılı Kişisel Verilen Korunması Kanununa ve 06/07/2019 tarih ve 30823 sayılı Resmi Gazetede yayımlanan 2019/12 numaralı Cumhurbaşkanlığı Genelgesine dayanılarak hazırlanmıştır.

Tanımlar

Madde 4- (1) Bu Yönergede geçen;

Ağ Güvenlik Duvarı	:Aile ve Sosyal Hizmetler Bakanlığı ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında Bakanlığın karşılaşılabileceği sorunları önlemek üzere tasarlanan cihazları,
Aktif Dizin	:Erişim ve yetkilendirme izin sunucusunu,
Bakan	:Aile ve Sosyal Hizmetler Bakanı
Bakanlık	:Aile ve Sosyal Hizmetler Bakanlığının,
Bakanlık Üst Yönetimi	:Bakan ve Bakan Yardımcıları
Genel Müdürlük	:Bilgi Teknolojileri Genel Müdürlüğünü,
Bilgi Güvenliği Yöneticisi	:Bilgi Güvenliği ile ilgili çalışmaların yürütülmesi ve koordinasyonundan sorumlu yöneticiyi,
Bilgi Güvenliği Yönetim Sistemi	: Bir organizasyonun kritik bilgilerini korumak amacıyla sistematik bir yaklaşımla yönetebilme kabiliyeti kazanması için kurulan sistemi,
Bilgi İşleme	:Bilginin oluşturulması, değiştirilmesi, iletilmesi, saklanması ve imha edilme süreçlerini,
Bluetooth	: Kablo bağlantısını ortadan kaldıran kısa mesafe radyo frekansı (RF) teknolojisini,
BTGM	:Bilgi Teknolojileri Genel Müdürlüğünü,
DMZ	:Bakanlık iç ağı ile Bakanlık dış ağı birbirinden ayıran bölgeyi,
E-İmza	:5070 Sayılı Elektronik İmza Kanunu'na göre "Başka bir elektronik veriye eklenen veya başka bir elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi",
Erişim Cihazı (Access Point)	:Dizüstü bilgisayar ve akıllı telefon gibi kablosuz cihazları kablosuz erişim standartları kullanarak kablolu ağa bağlayan aygıtları,
Etki Alanı	:Bakanlık aktif dizin yapısını,
Güvenli Kanal	:Güçlü bir şifrelemeden oluşan iletişim kanalını,



HTTP	:Bir kaynaktan dağıtılan ve ortak kullanıma açık olan bilgi sistemleri için uygulama seviyesindeki iletişim kuralını,
HTTPS	: Bir kaynaktan dağıtılan ve ortak kullanıma açık olan bilgi sistemleri için uygulama seviyesindeki güvenli iletişim kuralını,
IP	:Bilgisayar ağına bağlı cihazların, ağ üzerinden birbirleri ile veri alış veriş yapmak için kullandıkları adresi,
IPSec	:Genel ve özel ağlarda şifreleme ve filtreleme hizmetlerinin bir arada bulunduğu ve bilgilerin güvenliğini sağlayan iletişim kuralı ile uç kullanıcıya güvenli uzaktan erişim sağlamayı,
İstemci	:Sunucuların verdiği hizmeti alan bilgisayar sistemini,
İntranet	:Kuruluş içindeki bilgisayarları, yerel ağları (LAN) ve geniş alan ağlarını (WAN) birbirine bağlayan, çoğunlukla TCP/IP tabanlı bir ağı,
Kızılötesi	: Işık tayfında kırmızı bölümün ötesindeki alanda yayılmış durumda ısı ışınlarının oluşturduğu, gözle görülemeyen ışıması,
Kullanıcı	:Bakanlık Bilgi Sistemlerini kullanan tüm kişileri,
Portal	:Birden çok içeriği bir arada bulunduran alanı,
RADIUS	:Sunucular uzaktan bağlanan kullanıcılar için kullanıcı ismi-şifre doğrulama, raporlama/erişim süresi ve yetkilendirme işlemlerini yapan internet protokolünü,
Risk	:Bakanlığın bilgi sistemlerinin gizliliğini, mevcudiyetini ve bütünlüğünü etkileyen faktörleri,
Sahte E-posta	:Başka bir kişi gibi davranarak ve gerçek göndereni maskeleyerek kişinin güvenliğini kazanmak ve kişisel bilgilerine (tamamen yasa dışı yoldan) erişmeyi,
Siber Olay	:Bilişim sistemleri üzerinde gerçekleşen olayları,
Sistem Yöneticisi	:Bilgi Sistemleri Yöneticisini,
SOME	:Aile ve Sosyal Hizmetler Bakanlığı Siber Olaylara Müdahale Ekibini,
Son Kullanıcı	:Bir yazılım veya donanımın en son halini kullanan kullanıcıları,
Spam	:Yetkisiz ve/veya istenmeyen reklam içerikli e-postaları,
SSH (Secure Shell)	:Ağ üzerinde bulunan bir sunucuya bağlanmaya ve bağlanılan sunucu üzerinde komut çalıştırma, dosya transferi gibi işlemleri gerçekleştirmeye olanak sağlayan uzak sunucu bağlantı protokolünü,
SSL	:Ağ üzerindeki bilgi transferi sırasında güvenlik ve gizliliğin sağlanması amacıyla geliştirilmiş bir güvenlik protokolünü,
Sunucu	:İstemcilerden gelen isteklere hizmet verebilen bilgisayar sistemini,
Şifreleme	:Veriyi, istenmeyen kişilerin anlayamayacakları bir biçime sokan özel bir algoritmayı,
Uygulama Sunucusu	:Dağıtık yapıdaki bir ağda bulunan bir bilgisayarda çalıştırılan sunucu yazılımını,
Uzaktan Erişim	:İnternet, telefon hatları veya kiralık hatlar vasıtası ile Bakanlığın ağına erişilmesini,
Varlık Sahibi	:Varlığın gizliliğinin, bütünlüğünün, erişilebilirliğinin sağlanmasından birinci derecede sorumlu kişi ya da kişileri,
Veri tabanı	:Kolayca erişilebilecek, yönetilebilecek ve güncellenebilecek şekilde düzenlenmiş olan bir veri topluluğunu,
Veri sorumlusu	: 6698 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi
Veritabanı Yöneticisi	:Veritabanı Sistemlerinden Sorumlu Yöneticiyi,
VLAN	:Birçok farklı ağ bölümüne dağılmış olan, ancak aynı kabloya bağlıymışlar gibi birbiri ile iletişim kurnaları sağlanan, bir veya birkaç yerel ağ üzerindeki cihazlar grubunu,
VPN	:Bir ağa güvenli bir şekilde, uzaktan erişimi sağlayan teknolojiyi,
Yedekleme	:Ekipmanın bozulması durumu düşünülerek dosyaların ve/veya



Yetkilendirme	veritabanı'nın başka bir yere kopyalanması işlemini,
Zincir E-posta	:Çok kullanıcıli sistemlerde sistem yöneticisi tarafından, sisteme girebilecek kişilere giriş izni ve kişilere bağlı olarak da sistemde yapabileceği işlemler için belirli izinler verilmesini,
X.509/LDAP	:Bir kullanıcıya gelen şans ve para kazanma yöntemleri gibi bir içeriğe sahip e-postanın art arda diğer kullanıcılara gönderilmesini,
Web	:Aktif izin ve e-posta gibi programlardan bilgi aramak için kullanılan bir internet protokolünü,
	: WWW, Web, ya da W3 (World Wide Web), yazı, resim, ses, film, gibi pek çok farklı yapıdaki verilere kompakt ve etkileşimli bir şekilde ulaşmamızı sağlayan sistemini,
ifade eder.	

İKİNCİ BÖLÜM

Bilgi Güvenliği Politikaları

Bilgi Güvenliği Politikası

Madde 5- (1) İş hedeflerine ulaşmak için kurumun değerli bilgi birikimini oluşturan ve paydaşlara katma değer sağlayan bilgi varlıkları çeşitli ortamlarda üretilmekte, paylaşmakta ve saklanmaktadır. Bakanlık iş süreçleri büyük ölçüde bu bilgilerin işlendiği bilgi ve iletişim sistemlerine bağımlıdır. Bakanlık bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini temin etmek için uyulması gereken temel kurallar iş bu yönergede tanımlanmıştır. Ayrıca Bilgi Güvenliği Yönetim Sistemi kapsamında oluşturulan diğer alt politikalarda ve prosedürlerde de uyulması gereken diğer kurallar tanımlanmıştır.

(2) Bilgi Teknolojileri Genel Müdürlüğü bu yönergenin uygulanması ile ilgili olarak Bilgi Güvenliği Politikaları Kılavuzu hazırlayabilir ve gerek görmesi halinde güncelleyebilir.

Bilgi Sistemleri Genel Kullanım Politikası

Madde 6- (1) Bilgi sistemlerine sahip olma ve bu sistemleri genel kullanım kuralları aşağıda belirtilmiştir.

a) Bakanlığın bilgi sistemleri kişilere makul seviyede mahremiyet sağlasa da, Bakanlığın bünyesinde oluşturulan tüm veriler Bakanlığın mülkiyetindedir.

b) Bakanlık bilgisayarları etki alanına dâhil edilir.

c) Bilgisayarlarda oyun, eğlence, kumar vb. kişisel kullanıma yönelik programlar çalıştırılması ve kopyalanması politikaya aykırıdır.

ç) Bakanlıkta Bilgi Teknolojileri Genel Müdürlüğünün bilgisi ve onayı olmadan Bakanlık ağ sisteminde (web hosting, e-posta servisi vb.) sunucu nitelikli bilgisayar bulundurulamaz.

d) Birimlerde sorumlu bilgi işlem personeli ve ilgili teknik personel haricindeki kullanıcılar tarafından ağa bağlı cihazlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri gibi ayarlar değiştirilemez.

e) Bilgisayarlara lisanssız program yüklenmesi politikaya aykırıdır.

f) Bilgisayar kaynaklarının paylaşımı açılması politikaya aykırıdır.

g) Kullanıcı, bilgi teknolojileri kapsamındaki bilişim kaynaklarına zarar vermemeli, işleyişi aksatma, yavaşlatma veya durdurma eylemlerinde bulunmamalı, kaynakların içeriğini izinsiz olarak değiştirmemelidir.

h) Bakanlık merkez ve taşra teşkilatında bilişim varlığı satın alınacağı zaman, Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Rehberi tedbirleri gereği Bilgi Teknolojileri Genel Müdürlüğü'ne görüş sorulmalı, Bilgi Teknolojileri Genel Müdürlüğü tarafından uygun bulunmayan bilişim varlıkları alınmamalıdır.

ı) Bilgi Güvenliği Yönetim Sistemi, Bakanlığımızda Bilgi Teknolojileri Genel Müdürlüğü kapsamında kurulmuş olup, gerekli durumlarda kapsamın genişletilmesi ve/veya taşra birimlerinde Bilgi Güvenliği Yönetim Sistemi (BGYS) ekiplerinin kurulmasına Genel Müdürlük karar verebilir.

(2) Bilgi sistemleri genel yapılandırması ile ilgili kurallar aşağıda belirtilmiştir.

a) Dizüstü bilgisayarın çalınması/kaybolması durumunda, durum fark edildiğinde en kısa zamanda bağlı olunan birime ve BTGM'ye bilgi verilir.



- b) Bütün cep telefonu, tablet vb. mobil cihazlar Bakanlığın ağı ile senkronize olsun veya olmasın şifreleri aktif halde olmalıdır. Kullanılmadığı durumlarda kablosuz erişim (kızılötesi, bluetooth, vb.) özellikleri aktif halde olmamalıdır ve mümkünse güncel anti-virüs programları ile yeni nesil virüslere karşı korunmalıdır.
- c) Kullanıcılar tarafından kurum dışına gönderilen e-postalarda Aile ve Sosyal Hizmetler Bakanlığı sorumluluk reddini ifade eden açıklayıcı metin yer alır.
- ç) Kullanıcılar ağ kaynaklarının verimli kullanımı konusunda dikkatli olmalıdır.
- d) Doğrudan çalıştırılabilir dosyalar e-posta ile iletilmemelidir.

Son Kullanıcı Güvenliği Politikası

Madde 7- (1) Son Kullanıcı Güvenliği Politikası ile ilgili genel kurallar aşağıda belirtilmiştir.

- a) Bakanlık intranet uygulamalarını kullanan kullanıcılar, sistemlere kendilerine verilmiş kullanıcı adı ve şifreleri ile bağlanırlar.
- b) Her bir son kullanıcının görevleri gereği ihtiyaç duymadıkları sürece yalnızca bir adet kullanıcı hesabı bulunur.
- c) Son kullanıcılar için erişim kuralları görevleri gereği ihtiyaç duydukları kadar yetkilendirilirler.
- ç) Son kullanıcıların aktiviteleri, güvenlik zafiyetlerine ve bilgi sızdırmalarına karşı 5651 sayılı kanuna uygun olarak kayıt altına alınır.
- d) Güvenlik zafiyetlerine karşı, kullanıcılar hesaplarının ve/veya sorumlusu oldukları cihazlara ait kullanıcı adı ve şifre gibi bilgilerin gizliliğini korumalı ve başkaları ile paylaşmamalıdır.
- e) Son kullanıcılar bilgisayarlarındaki ve sorumlusu oldukları cihazlardaki verilerden kendileri sorumludur.
- f) Son kullanıcılar, güvenlik zafiyetlerine sebep olmamak için, bilgisayar başından ayrılırken mutlaka bilgisayar ekranlarını kilitlemelidir.
- g) Son kullanıcılar, bilgisayarlarında ya da sorumlusu oldukları sistemler üzerinde kullandıkları harici cihazları (e-imza ve kart okuyucusu, bellek ve/veya harici hard disk gibi taşınabilir medya araçları) kontrol altında tutmalıdır.
- ğ) Bakanlık, son kullanıcı güvenliğine dair oluşturulmuş grup politikalarını, etki alanı üzerinden kullanıcı onayı olmaksızın uygulama yetkisine sahiptir.
- h) Bakanlık, son kullanıcıların farkında olmadan yapabilecekleri ve sonunda zafiyet yaratabilecek değişiklikleri merkezi grup politikalarıyla engeller.
- ı) Temiz masa, temiz ekran ilkesi benimsenmeli ve hayata geçirilmelidir.
- i) Kullanıcılar, Bakanlık mevcut envanteri haricindeki donanımları kullanırken güvenlik kriterlerine özen göstermelidir.
- j) Bilinmeyen veya şüpheli kaynaklardan dosya indirmemelidir.
- k) Dosya paylaşım alanı ihtiyacı olması durumunda Bakanlık dosya paylaşım sistemleri kullanılır.
- l) Gizli ve kişisel veriler Bakanlık tarafından sağlanan dosya paylaşım ve depolama alanları haricinde depolanamaz/paylaşılamaz.

Parola Politikası

Madde 8- (1) Parola Politikası ile ilgili genel kurallar aşağıda belirtilmiştir.

- a) Yönetici ve kullanıcı yetkisine sahip hesaplara ait parolalar en geç 90 (doksan) günde bir değiştirilir. Parola yenileme işlemi esnasında son 3 parola ile aynı olmayan bir parola girilir.
- b) Sistem yöneticilerinin, sistem ve kullanıcı hesapları farklı olarak tanımlanır.
- c) Parolalar e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir ve kritik sistemlerin bağlantıları için otomatik parola anımsama seçenekleri işaretlenmemelidir.
- ç) Kullanıcı, parolasını başkası ile paylaşmamalı, kâğıtlara ya da elektronik ortamlara yazması durumunda güvenliğini sağlar.
- d) Kullanıcıya ilk verilen veya sıfırlanması istenilen parolalar “geçici parola” olarak verilir ve ilk oturum açılışında değiştirilir.
- e) Kritik sistemlere ve ağ cihazlarına erişim için sistem yöneticileri 'Administrator' ve 'root' gibi genel sistem hesapları kullanmamalıdır. Bunun mümkün olmadığı durumlarda varsayılan parolalar değiştirilir.
- f) Genel kural olarak, parola gibi hassas veri girilen web adresleri HTTPS protokolü kullanılmalıdır. Ayrıca HTTPS site de kullanılan sertifikanın siteyi yayımlayan kurum/şirkete ait olduğu kontrol edilmelidir.



g) Parola kriterleri gerek görüldüğü takdirde Bilgi Teknolojileri Genel Müdürlüğü tarafından sıkılaştırılabilir.

(2) Kullanıcı, güçlü bir parola oluşturmak için, aşağıda belirtilen maddelere uymalıdır.

Parola en az 8 haneli olmak üzere; aşağıdaki kriterlerden (a, b, c) en az 2 tanesine uyulması zorunludur.

a) İçerisinde en az 1 tane küçük ve 1 tane büyük harf bulunmalıdır. (a, b, A, B ..)

b) İçerisinde en az 1 tane rakam bulunmalıdır. (1, 2, 3...)

c) İçerisinde en az 1 tane özel karakter bulunmalıdır. (@, !, ?, ^, +, \$, #, &, /, {, *, -,], =, ...)

Uyulması tavsiye edilenler:

ç) Aynı karakterler peş peşe kullanılmamalıdır. (aaa, 111, XXX, bbbb ...)

d) Sıralı karakterler kullanılmamalıdır. (abcd, qwert, asdf, 1234, zxcvb...)

e) Kullanıcıya ait anlam ifade eden kelimeler içermemelidir. (aileden birisinin, arkadaşının, bir sanatçının, sahip olduğu bir hayvanın ismi, arabanın modeli, doğum tarihi, adres, telefon vb.)

(3) Şifre koruma standartları ile ilgili kurallar aşağıda belirtilmiştir.

a) Bütün parolalar Bakanlığa ait gizli bilgiler olarak düşünülmeli ve kullanıcı, parolalarını hiç kimseyle paylaşmamalıdır.

b) Güvenlik testleri sırasında parola kırma ve tahmin etme operasyonları bilgi güvenliği yetkililerince yapılabilir. Güvenlik taraması sonucunda parolalar tahmin edilirse veya kırılırsa kullanıcıdan parolasını değiştirmesi talep edilir. Tahmin edilen veya kırılan parolalar üçüncü kişilerle paylaşılamaz.

(4) Uygulama Geliştirme Standartları;

a) Bireylerin ve/veya grupların kimlik doğrulaması işlemi desteklemelidir.

b) Parolalar metin olarak veya kolay anlaşılabilir formda saklanmamalıdır.

c) Parolalar, şifrelenmiş olarak saklanmalıdır.

ç) Uygulama geliştirme standartları en az RADIUS ve/veya X.509/LDAP güvenlik protokollerini desteklemelidir.

E-Posta Politikası

Madde 9- (1) E-Posta ile ilgili kullanım kuralları aşağıda belirtilmiştir.

a) Kullanıcı hesaplarına ait parolalar ikinci bir şahsa verilmemelidir.

b) Bakanlığa ait "gizlilik" içeren bilgilerin e-posta ve eklerinde bulunması politikaya aykırıdır.

c) Kullanıcılar, Bakanlığın e-posta sistemini taciz ve suiistimal etmemelidir, küçük düşürücü, hakaret edici veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında Bakanlık Siber Olaylara Müdahale Ekibine (some@aile.gov.tr) adresine iletilmelidir.

ç) Kurumsal iletişim gerektiren durumlarda Kurumsal e-posta adresleri kullanılır. Kullanıcılara tahsis edilen Bakanlık e-posta hesabının güvenliğinden kullanıcılar sorumludur. Bu e-posta hesapları Bakanlık işlerinin gerçekleştirilmesi için kullanılmalı, iş dışı konularda kullanılmamalıdır.

d) Kaynağı bilinmeyen ortalama (phishing), kullanıcı kodu/parolasını girmesini isteyen, zincir mesajlar, ve mesajlara iliştilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında açılmadan, başkalarına iletilmeden, herhangi bir işlem yapmaksızın (some@aile.gov.tr) adresine iletilmelidir.

e) Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.

f) Kullanıcılar, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) gönderemez.

g) Kullanıcılar, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul edip; suç teşkil edebilecek, tehditkâr, yasadışı, hakaret, küfür veya iftira içeren, ahlaka aykırı mesajların gönderilmesinden sorumludur.

ğ) Kullanıcılar e-posta gönderiminde ad, soyad, iletişim bilgisi, kurum, birim adı gibi alanları içeren imza şablonu kullanılır.

h) Bakanlık dışında, güvenliğinden emin olunmayan bir bilgisayar üzerinden kurumsal Web Posta Sistemi kullanılması politikaya aykırıdır.

(2) Kurumsal e-postalar, resmi yazı ile gelen talepler doğrultusunda, hukuki olarak yetkilendirilmiş kişilerce tutanak altında denetlenebilir.

İnternet Erişim ve Kullanım Politikası

Madde 10- (1) İnternet Erişim ve Kullanım Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Kullanıcıların internet erişimlerinde güvenlik kriterleri uygulanır.

b) Bakanlığın politikaları doğrultusunda en az kategori ve uygulama bazlı filtreleme sistemleri kullanılır. İstenilmeyen siteler (terör, pornografi, oyun, kumar, şiddet içeren vs.) yasaklanır.

c) Kullanıcılar internete Bakanlık tarafından sağlanan kullanıcı adı/şifre (LDAP vb.) ile erişim sağlar. Ayrıcalıklı erişim yetkileri ihtiyaç halinde gerekçelendirilerek Genel Müdürlük tarafından belirli bir süre ile sınırlı olarak verilir.

ç) İş ile ilgili olmayan dosyalar (müzik, video vs. dosyaları) gönderilmemeli, paylaşılmamalı ve indirilmemelidir. Dosya paylaşım uygulamaları kullanılmamalıdır. Bu konuda sorumluluk kullanıcıya aittir.

d) Genel Müdürlük tarafından onaylanmamış yazılımlar internet üzerinden indirilmemelidir ve Bakanlık sistemlerine yüklenmemelidir.

e) Bakanlık içerisinde yapılan internet erişimlerinde 5651 sayılı kanun gereği Bakanlık ilgili erişim bilgilerini tutmak ve devletin ilgili mercileri tarafından istenmesi durumunda bu bilgiyi sağlamakla yükümlüdür. Kuruluşlar eğer Bakanlık altyapısı dışında bir internet hizmeti alıyorsa bu hizmetin mevzuata ve 5651 sayılı kanuna uygun olarak kullanılmasından ve iz kayıtlarının tutulmasından sorumludurlar. Bakanlık, kullanıcının internet sisteminde gerçekleştirdiği aktivitelerle ilgili bilgileri hukuki olarak yetkilendirilmiş kişilere verebilir.

f) Bakanlık etki alanına dahil olmayan cihazlar için istisnai durumlarda internete çıkış izni Genel Müdürlük tarafından uygun bulunması halinde verilir.

Uzaktan Erişim Politikası

Madde 11- (1) Uzaktan erişim politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) İnternet üzerinden Bakanlık ağına erişen kişiler ve/veya kurumlar güvenli protokoller kullanmalıdırlar. Web tabanlı uygulama erişimleri sadece yetkili idari yöneticilere bir üst amirinin onayı ile Genel Müdürlük tarafından verilir.

b) Uzaktan erişimler Genel Müdürlük tarafından kayıt altına alınmalıdır.

c) Bakanlık çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.

ç) Bakanlık ağına uzaktan erişecek bilgisayarların işletim sistemi ve anti-virüs yazılımı güncellemeleri yapılmış olmalıdır.

d) Bakanlık personeli haricinde üçüncü şahıslara istisnai durumlar dışında uzak erişim izni verilmemelidir.

Kablosuz İletişim Politikası

Madde 12- (1) Bakanlığın bilgisayar ağına bağlanan bütün cihazların erişim bilgileri Genel Müdürlük tarafından kayıt altına alınır.

(2) Bütün kablosuz erişim cihazları Bilgi Teknolojileri Genel Müdürlüğü tarafından belirlenen güvenlik ayarlarını kullanır.

(3) Kablosuz iletişim ile ilgili gereklilikler aşağıda belirtilmiştir.

a) Kablosuz cihazlar güçlü şifreleme protokolleri kullanmalıdır.

b) Bakanlık kullanıcısı olmayan kişilerin, kablosuz ağa yetkisiz erişimi engellenir.

c) Erişim cihazları üzerinden gelen kullanıcılar ağ güvenlik duvarı üzerinden ağa dâhil olmalıdırlar.

ç) Kullanıcı bilgisayarlarında güncel anti-virüs ve işletim sistemi güvenlik duvarı yazılımları yüklü olmalıdır.

d) Erişim cihazları bir yönetim yazılımı ile devamlı olarak gözlemlenmelidir.

Anti-Virüs Politikası

Madde 13- (1) Anti-virüs Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Bakanlığın tüm istemcileri ve sunucuları güncel anti-virüs yazılımına sahip olmalıdır.

b) İstemcilere ve sunuculara zararlı yazılım bulaştığı fark edildiğinde ağ erişimi sınırlandırılır.

c) Bilgi Teknolojileri Genel Müdürlüğü anti-virüs yazılımının sürekli ve düzenli çalışmasından ve istemcilerin ve sunucuların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur.

ç) Kullanıcı hiç bir sebepten dolayı anti-virüs yazılımını bilgisayarından kaldırmamalıdır.

d) Harici veri depolama cihazları her kullanımda anti-virüs kontrolünden geçirilir.

e) Kullanılan anti-virüs yazılımı üzerinde düzenli taramalar yapılacak şekilde konfigürasyonlar yapılır.



İşletim Sistemleri Güvenliği Politikası

Madde 14- (1) İşletim Sistemleri Güvenliği Politikası ile ilgili genel kurallar aşağıda belirtilmiştir.

- a)Bakanlık, son kullanıcı düzeyinde hangi işletim sistemini kullanacağına karar verir ve bu işletim sistemine uygun yazılım ve donanım sistemlerinin kurulumunu temin eder. Bakanlık tarafından temin edilen kurumsal imaj dosyaları dışında kurulum yapılmamalıdır.
- b)Genel Müdürlük, işletim sistemlerinin güncel ve güvenli olması için yama yönetimi yapar.
- c)Sunucu işletim sistemlerinde kurulumda gelen yönetici hesaplarının (Administrator, root vb.) kaba kuvvet saldırılarıyla ele geçirilmesine karşı, gerekli önlemler alınır.

Fiziksel Güvenlik Politikası

Madde 15- (1) Fiziksel Güvenlik ile ilgili kurallar aşağıda belirtilmiştir.

- a)Bakanlığın binalarının fiziksel olarak korunması, farklı koruma mekanizmaları ile donatılması temin edilir.
- b)Kurumsal bilgi varlıklarının dağılımı ve bulundurulacak bilgilerin kritiklik seviyelerine göre binalarda ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanır ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilir.
- c)Tanımlanan farklı güvenlik bölgelerine erişim yetkileri gözden geçirilir ve güncellenir.
- ç)Bakanlık dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili personel gözetiminde gerçekleştirilir.
- d)Kritik bilgilerin bulunduğu alanlara girişler kontrolü bir şekilde yapılır ve izlenir.
- e)Her ziyaretçi için kayıt tutulur ve her bir ziyaretçiye bir adet ziyaretçi kartı verilir.
- f)Kritik sistemler sistem odalarında barındırılır.
- g)Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunur, yangın ve benzer felaketlere karşı koruma altına alınır ve iklimlendirilmesi sağlanır.
- ğ)Kritik bilgi içeren ofisler ve odalar için işaret, tabela vb. bulunmamasına dikkat edilir.

Personel Güvenliği Politikası

Madde 16- (1) Personel Güvenliği Politikası ile ilgili kurallar aşağıda belirtilmiştir.

- a)Kritik bilgiye erişim hakkı olan çalışanlar ile gizlilik anlaşmaları ilgili Genel Müdürlük/Birim tarafından imzalanır.
- b)Kurumsal bilgi güvenliği bilinçlendirme eğitimleri Genel Müdürlük tarafından düzenlenir.
- c)İş tanımı değişen veya Bakanlıktan ayrılan kullanıcıların erişim haklarının kaldırılması için Genel Müdürlüğe bilgi verilir.
- ç)Bakanlık bilgi sistemlerinin işletmesinden sorumlu personelin konularıyla ilgili teknik bilgi düzeylerini güncel tutmaları çalışma sürekliliği açısından önemli olduğundan, eğitim planlamaları periyodik olarak yapar, bütçe ayırır, eğitimlere katılım sağlanmasını gözetir ve eğitim etkinliği değerlendirir.
- d)Yetkiler, “görevler ayrımı” ve “en az ayrıcalık” esaslı olarak verilir. “Görevler ayrımı”, rollerin ve sorumlulukların paylaşılması ile ilgilidir. Bu paylaşım ile kritik bir sürecin tek kişi tarafından kırılma olasılığı azaltılmalıdır. “En az ayrıcalık” ise kullanıcılara gereğinden fazla yetki verilmemesidir. Sorumlu oldukları işleri yapabilmeleri için yeterli olan asgari erişim yetkisine sahip olmalıdır.
- e)Tüm çalışanlar, yükleniciler ve üçüncü taraflar Bakanlığın politika ve prosedürlerine uymak zorundadır.

Sunucu Güvenlik Politikaları

Madde 17- (1) Sunucuya sahip olma ve sunucu sahiplerinin sorumlulukları ile ilgili kurallar aşağıda belirtilmiştir.

- a)Bakanlıkta bulunan sunucuların yönetiminden, ilgili sunucu üzerinde Genel Müdürlük tarafından yetkilendirilmiş personel sorumludur.
- b)Sunucu kurulumları, konfigürasyonları, yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personel tarafından yapılır.
- c)Sunuculara ait bilgilerin yer aldığı güncel sunucu envanter bilgisi tutulur.
- (2) Genel yapılandırma kuralları aşağıda belirtilmiştir.
- a)Sunucuyu kullanan birim tarafından, kullanılmayan servisler ve uygulamalar kapatılır.



- b)Sunuculara yetkisiz kişilerin erişmesine engel olmak için gerekli önlemler alınmalıdır.
- c)Sunucu üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları ve anti-virüs vb. koruma amaçlı yazılımlar güncel tutulur.
- d)Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
- e)Sunucular üzerine lisanslı yazılımlar kurulur.
- f)Sunucular fiziksel olarak korunmuş sistem odalarında bulundurulur.
- (3) Sunucu işletim kuralları aşağıda belirtilmiştir.
- a)Sunucular elektrik, ağ altyapısı, sıcaklık ve nem değerleri düzenlenmiş, tavan ve taban güçlendirmeleri yapılmış ortamlarda bulundurulur.
- b)Sunucuların yazılım ve donanım bakımları üretici firma tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılır.
- c)Sistem odalarına giriş ve çıkışların erişim kontrollü olması sağlanır ve kayıt edilir.

Ağ Yönetim Politikası

Madde 18- (1) Ağ yönetim politikası ile ilgili kurallar aşağıda belirtilmiştir.

- a)Ağ cihazları yönetim sorumluluğu, sunucu ve istemcilerin yönetiminden ayrı değerlendirilir.
- b)Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için düzenli denetimler yapılır ve güncellemeler uygulanır.
- c)Sınırsız ağ dolaşımı engellenir. Ağ servisleri, varsayılan durumda erişimi engelleyecek şekilde olup, ihtiyaca göre açılır.
- ç)İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden güvenlik duvarı gibi ağ cihazları yoluyla önlemler alınır ve kayıtlar tutulur.
- d)Kullanıcı bilgisayarlarının bulunduğu ağ, iç sunucuların bulunduğu ağ, DMZ ağı birbirlerinden ayrılır ve ağlar arasında geçiş güvenlik sunucuları (firewall) üzerinden sağlanır.
- e)Bilgisayar ağına bağlı bütün cihazlarda kurulum ve yapılandırma parametrelerinin, Bakanlığın güvenlik politika ve standartlarıyla uyumlu olması gerekmektedir.
- f)Ağ trafiği düzenli olarak izlenir ve ölçülür.
- (2)Ağ cihazları güvenlik politikası ile ilgili kurallar aşağıda belirtilmiştir.
- a)Ağ cihazlarının güncel envanter ve topoloji bilgileri tutulur.
- b)Özel durumlar haricinde yerel kullanıcı hesapları kullanılmamalıdır. Ağ cihazları kimlik tanımlama için güvenli protokoller kullanılır.
- c)Cihazlar üzerinde kullanılmayan servisler kapatılır.
- ç)Cihazlara erişim için güçlü bir parola kullanılmalıdır. Erişim parolaları varsayılan ayarlar bırakılmamalıdır.
- d)Yazıcı, fotokopi cihazı, faks cihazı gibi cihazların bulunduğu ağlar kritik sistemlerin bulunduğu ağlardan ayrılır.

Donanım ve Yazılım Envanteri Oluşturma Politikası

Madde 19- (1) Donanım ve yazılım envanteri oluşturma ile ilgili kurallar aşağıda belirtilmiştir.

- a)Oluşturulan envanter tablosunda envantere ait ayırt edici ve önemli bilgiler tutulur.
- b)Envanter bilgileri değişiklik olduğunda güncellenir. Envanter bilgilerinin güncel olmaması nedeniyle yaşanabilecek kayıp ve maliyetlerden, varlık sahipleri sorumlu olacaktır.
- c)Satın alınan, geliştirilen, hibe yoluyla elde edilen, proje kapsamında sağlanan bilişim varlıkları ve yazılımlar Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Rehberi tedbirleri gereği Bilgi Teknolojileri Genel Müdürlüğü tarafından bildirilen envanter yönetim sistemi yazılımına aktarılmalıdır.

Kriz / Acil Durum Politikası

Madde 20- (1) Acil Durum politikası ile ilgili kurallar aşağıda belirtilmiştir.

- a)Oluşturulan acil durum senaryoları çerçevesinde acil durum sorumluları atanır, yetki ve sorumlulukları belirlenir ve yazılı hale getirilir.
- b)Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınır.
- c)Bilişim sistemlerinin kesintisiz çalışmasının sağlanması için sistemler tasarlanırken minimum sürede iş kaybı hedeflenir.
- ç)Acil durumlarda Bakanlık içi işbirliği gereksinimleri tanımlanır.



- d)Acil durumlarda sistem kayıtları incelenmek üzere saklanır.
e)Yaşanan acil durumlar sonrası politikalar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilir.
f)Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulur.
g)Acil durumlarda bilgi güvenliği yöneticisine erişilir, ulaşılamadığı durumlarda koordinasyonu sağlamak üzere önceden tanımlanmış ilgili yöneticiye bilgi verilir ve zararın tespit edilerek süratle önceden tanımlanmış felaket kurtarma faaliyetleri yürütülür.

Kimlik Doğrulama ve Yetkilendirme Politikası

- Madde 21-** (1) Kimlik Doğrulama ve Yetkilendirme Politikası ile ilgili kurallar aşağıda belirtilmiştir.
a)Bakanlık bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama ve sistemler üzerindeki kullanıcı yetkileri belirlenir ve denetim altında tutulur.
b)Erişim hakları tanımlanırken ihtiyacı kadar yetki ilkesi göz önünde bulundurulur. c)Üçüncü tarafların tüm erişimleri kayıt altına alınır. İşi biten firmaların hesapları kapatılır. Bu işlem için Genel Müdürlüğe ve ilgili personele bilgi verilir.
c)Sistemlere başarılı ve başarısız erişim istekleri düzenli olarak tutulur, tekrarlanan başarısız erişim istekleri/girişimleri incelenir.
ç)Kullanıcı hareketlerini doğru bir şekilde kayıt altına almak için her kullanıcıya kendisine ait bir kullanıcı hesabı açılır.

Veri Tabanı Güvenlik Politikası

- Madde 22-** (1) Veri tabanı güvenlik kuralları aşağıda belirtilmiştir.
a)Veri tabanı sistemleri envanteri güvenli şekilde tutulur, saklanır ve bu envanterden sorumlu personel tanımlanır.
b)Veri tabanı işletim prosedürleri belirlenir ve yazılı hale getirilir.
c)Veri tabanı sistem olay kayıtları tutulur ve gerektiğinde Genel Müdürlük tarafından izlenir.
ç)Veri tabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilir.
d)Yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli olarak alınması kontrol altında tutulmalıdır.
e)Veri tabanı yedekleme planları yazılı halde olmalıdır.
f)Veri tabanı erişim politikaları “Kimlik Doğrulama ve Yetkilendirme” politikaları çerçevesinde oluşturulur.
g)Bilgi saklama medyaları kontrolsüz olarak Bakanlık dışına çıkartılamaz.
ğ)İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için temas edilecek kişiler belirlenir.
h)Veri tabanı sunucusuna sadece güvenli erişim protokolleri ile erişim sağlanır.
ı)Veri tabanı sunucusuna ancak zorunlu hallerde ayrıcalıklı erişim (“root” “admin” vb..) yetkisi ile bağlanılır. Ayrıcalıklı erişim yetkili kullanıcılar kişilerin kendi adına özel oluşturulur ve ortak kullanılamaz.
i)Veri tabanına doğrudan bağlanacak kişilerin kendi adına kullanıcı adı verilir ve yetkilendirme yapılır.
j) Veri tabanına doğrudan bağlanan kullanıcıların yaptıkları işlemler kaydedilir.

Değişim Yönetim Politikası

- Madde 23-** (1) Değişim Yönetim Politikası ile ilgili kurallar aşağıda belirtilmiştir.
a)Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri yazılı hale getirilir.
b)Yazılım ve donanım envanteri oluşturularak, yazılım sürümleri kontrol edilir.
c)İş kritik bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek sistem ve uygulamalar ilgili birim(ler) tarafından belirlenir ve yazılı hale getirilir.
ç)Yapılacak değişiklikler öncelikle bir test ortamında denenmelidir.
d)Tüm sistemlere yönelik yapılandırma dokümantasyonu oluşturulur ve güncel tutulması sağlanır.
e)Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanır, geri dönüş planları test edilir ve ilgili yöneticiler tarafından onaylanması sağlanır.



- f)Sistemlerde oluşacak problemlere yönelik bakım, onarım, yama, güncelleme ve değişiklikler ile ilgili çalışmalardan önce varlık sahibine ve proje paydaşlarına bilgi verilir. Sonrasında ilgili uygulama kontrolleri gerçekleştirilir.

Bilgi Sistemleri Yedekleme Politikası

- Madde 24-** (1) Bilgi Sistemleri Yedekleme Politikası ile ilgili kurallar aşağıda belirtilmiştir.
a)Bilgi sistemlerinde oluşabilecek hatalar karşısında; sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigürasyon, sistem bilgileri ve kurumsal veriler düzenli olarak yedeklenir.
b)Veri yedekleme sıklığı, kapsamı, gün içinde ne zaman yapılacağı, ne koşullarda ve hangi aşamalarla yedeklerin yükleneceği ve yükleme sırasında sorunlar çıkarsa nasıl geri döneceğinin kritiklik derecesine göre belirlenmesi ve yazılı hale getirilmesi veri sorumlularının sorumluluğundadır.
c)Yedek medyaları verilerin olduğu fiziksel ortamlardan farklı yerlerde veya binalarda güvenli bir şekilde saklanır.
ç)Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanır.
d)Son kullanıcılar kendi bilgisayarlarındaki verilerin yedeklenmesinden kendileri sorumludurlar.

Bakım Politikası

- Madde 25-** (1) Bakım Politikası ile ilgili kurallar aşağıda belirtilmiştir.
a)Bakanlık sistemlerinin tamamı (donanım, uygulama yazılımları, paket yazılımlar, işletim sistemleri) periyodik bakım güvencesine alınır.
b)Üreticilerden, sistemler ile ilgili bakım prosedürleri sağlanır.
c)Firma teknik destek elemanlarının bakım yaparken bu yönergeye uygun davranmaları sağlanır ve kontrol edilir.
ç)Sistem üzerinde yapılacak değişiklikler ile ilgili olarak “Değişim Yönetimi Politikası” ve ilişkili standartlar uygulanır.
d)Sistem bakımlarından sonra bir güvenlik açığı yaratıldığından şüphelenilmesi durumunda, bu yönerge uyarınca hareket edilir. Güvenlik açıkları Bakanlık Siber Olaylara Müdahale Ekibine (some@aiile.gov.tr adresine) bildirilmelidir.
e)Bakanlık içinde firmalar tarafından bakımı ve onarımı yapılan sistemlerde, bakım işlemi yetkili bir çalışanın gözetiminde yapılır ve sistemden bilgi alınmasına engel olunması sağlanır.
f)Depolama ortamının (örn. sabit disk) bakım, onarım gibi amaçlarla Bakanlık dışına çıkarıldığı durumlar kayıt altına alınır ve firma yetkilisi tarafından imzalanır. Gerekli durumlarda firma ile gizlilik sözleşmesi imzalanır.

Yazılım Geliştirme Politikası

- Madde 26-** (1) Yazılım Geliştirme Politikası ile ilgili kurallar aşağıda belirtilmiştir.
a)Yazılım planlama aşamasında güvenlik ihtiyaçları planlanır.
b)Yazılım Bakanlık Bilgi Güvenliği Politikalarına uygun olarak geliştirilir, yetkisiz kişilerin müdahale etmesi şifreleme işlemleri ile engellenir.
c)Yazılım kodları dışarıdan erişime kapalı olan bir ortamda saklanır.
ç)Yazılım geliştirme, test ve uygulama ortamları ayrılır, her biri için özel olarak tahsis edilmiş ayrı sistemler kullanılır.
d)Yazılım geliştirme süreçleri uluslararası kabul görmüş proje yönetim mantığına uygun şekilde yazılı hale getirilir. (yazılımın veri akışı ve işleme özelliklerini içeren tasarım belgesi, vb.)
e) Bakanlıkta yazılım geliştirileceği ya da temin edileceği durumda Bilgi Teknolojileri Genel Müdürlüğü’ne görüş sorulması, Genel Müdürlük onayı ve bilgisi dışında yazılım geliştirme/temini yapılmaması gerekmektedir.
f) Bakanlık merkez ve taşra kuruluşları Bilgi Teknolojileri Genel Müdürlüğünce sağlanan Bakanlığa ait web portali üzerinden yayın/paylaşım yapmalı, Bakanlık alan adlarından farklı bir web sayfası oluşturmamalı/yayınlamamalıdır.



ÜÇÜNCÜ BÖLÜM Çeşitli Hükümler

Yaptırım

Madde 27-(1) Bu yönergeye uyulmadığının tespit edilmesi halinde, bu ihlalden sorumlu olan çalışan ya da 3. taraf için geçerli olan usul, esas ve sözleşmelerde geçen ilgili maddelerinde belirlenen yaptırımlar uygulanır. Cezaî yaptırımlarda öncelik hukuki, yasal, düzenleyici ya da sözleşmeye tabi yükümlülükler aittir.

Üçüncü Tarafların Yönetimi

Madde 28- (1) Bakanlık çalışanı olmayıp bilgi sistemleri kaynaklarına erişim sağlayan her türlü kişi üçüncü taraf olarak kabul edilir. Üçüncü taraf tanımına uyan her türlü kişi ya da kurumla yapılacak geçici ya da sürekli çalışma sözleşmelerin imzalanması güncel olarak takip edilir. Sözleşme imzalanmadan önce kararlaştırılmış ve onaylanmış güvenlik anlaşmaları hazırlanıp kurumlarla kurumsal, şahıslar ile bireysel gizlilik sözleşmeleri yapılır. Üçüncü taraf çalışanları Bakanlık politikalarına ve yapılan iş ile ilgili Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Rehberi tedbirlerine uymak zorundadır.

Yönetimin Taahhüdü

Madde 29- (1) Bakanlığın, belirlediği hedef ve politikalarını gerçekleştirmek için Bilgi Güvenliği Yönetim Sistemini TS ISO/IEC 27001 standardına uyumlu hale getirecek şekilde kurar ve yürütür.

(2) Bakanlık Üst Yönetimi, tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan Bilgi Güvenliği Yönetim Sistemine uyacağını ve sistemin verimli şekilde çalışması için gerekli olan kaynakları tahsis edeceğini, etkinliğini, sürekli iyileştireceğini ve bunun tüm çalışanlar tarafından anlaşılmasını sağlayacağını taahhüt eder.

(3) Bakanlık Üst Yönetimi, bilgi güvenliği kapsamında yapılan çalışmalar için gerekli bütçeyi temin eder.

Sorumluluk

Madde 30-(1) Bakanlığın bütün çalışanları “Bilgi Güvenliği Politikalarını” bilmek ve uygulamak ile yükümlüdür. Aksi belirtilmedikçe 3. taraflar da bu politikaya uymakla yükümlüdür.

Yürürlükten Kaldırılan Yönerge

Madde 31- (1) Bu yönergenin imzalanmasıyla 09/01/2020 tarihli Aile, Çalışma ve Sosyal Hizmetler Bakanlığı Bilgi Güvenliği Politikaları Yönergesi Bakanlığımızda yürürlükten kalkar.

Yürürlük

Madde 32- (1) Bu Yönerge Aile ve Sosyal Hizmetler Bakanının onayı ile yürürlüğe girer.

Yürütme

Madde 33- (1) Bu Yönerge hükümlerini Aile ve Sosyal Hizmetler Bakanı yürütür.



EK-2

Gizlilik Sözleşmesi (Firma)

	GİZLİLİK SÖZLEŞMESİ	Doküman No	SBLN-001
		Yayın Tarihi	05/01/2022
	Firma	Revizyon No	02
		Revizyon Tarihi	

1 GİZLİLİK SÖZLEŞMESİ

Bir tarafta Eskişehir Yolu Söğütözü Mahallesi 2177.Sokak No:10/A Çankaya/ANKARA adresinde bulunan Aile ve Sosyal Hizmetler Bakanlığı (kısaca "ASHB") ile diğer tarafta **HİZMET ALINAN FİRMANIN ADRESİ** adresinde bulunan **HİZMET ALINAN FİRMANIN ADI** (kısaca "FİRMA" olarak anılacaktır) arasında aşağıdaki şartlarda gizlilik sözleşmesi imzalanmıştır.

1- GİZLİLİK

ASHB projeye ait teknik altyapı, teknik bilgiler, müşteri bilgisi, ticari planlar, ticari stratejiler, müşteri listeleri ve proje ile ilgili olarak yapılacak iş ve işlemlere dair, açıkça ve yazılı olarak gizli olduğu beyan edilen sair her türlü bilgi "Gizli" olarak kabul edilecektir. Bu anlamda ASHB projenin kurulum, geliştirme, bakım, veri aktarma süreçlerinde FİRMA'ya ister sözlü, isterse elektronik ortamda veya yazılı ya da başka bir araçla yapılmış olsun verilen her türlü bilgiler ve FİRMA'nın bu yolla edindiği her türlü bilgi "Gizli Bilgi" olarak kabul edilecektir. ASHB Proje süresince, FİRMA yapacağı açıklamalarda ve vereceği bilgilerde kendisine ait birtakım Gizli Bilgileri FİRMA ile paylaşabilecektir. Tarafların iş bu Sözleşme konusu Gizli Bilgileri paylaşımını ve Gizli Bilgilerin korunması, aşağıda belirtilen şartlar dâhilinde gerçekleşecektir.

2- GİZLİ BİLGİNİN TANIMINA GİRMEYEN BİLGİLER

Kamuoyuna mal olmuş bilgiler, Yürürlükte olan kanun ya da düzenlemeler ya da verilmiş olan bir mahkeme kararı gereğince açıklanması gereken bilgilerdir. FİRMA kendisinden Kanun, mevzuat veya yetkili bir mahkeme emriyle açıklama istendiğinde, bunu derhal ASHB'ye bildirmekle sorumlu sayılacaktır. FİRMA; Bilgi verme yetki ve sorumluluğunun iş bu sözleşme çerçevesinde ASHB'de olduğunu bu makamlara bildirecektir.

3-GİZLİ BİLGİNİN DİĞER TARAFAÇA KORUNMASI

FİRMA; proje ile ilgili kendi Gizli Bilgileri üstündeki haklarını tanımakta ve kabul etmekte olup, işbu Sözleşme altında elde edilen Gizli Bilgiler konusunda aşağıda yazılı olanları sağlamak için gerekli önlemleri almayı kabul ve taahhüt eder:

- a- Büyük bir gizlilik içinde azami dikkat ve özenle korumak,
- b- Herhangi bir 3. kişiye hangi suretle olursa olsun vermemek ve / veya alenileştirmemek,
- c- Doğrudan ya da dolaylı olarak aralarındaki sözleşme gereği yapılan işin gereği dışında kullanmamak.

Taraflar kendi gizli bilgilerini korumakta gösterdikleri dikkat ve özenin aynısını karşı tarafın gizli bilgilerini korumakta da göstermeyi kabul ve taahhüt ederler.

FİRMA; ancak zorunlu hallerde ve işi gereği bu bilgiyi, öğrenmesi gereken işçilerine, alt çalışanlarına ve kendilerine bağlı olarak çalışan diğer kişilere verebilir, ancak bilginin gizliliği hususunda işçilerini, alt çalışanlarını ve kendilerine bağlı olarak çalışan diğer kişilerin iş bu sözleşme yükümlülüklerine aykırı davranmayacaklarını ve böyle davranmaları halinde doğrudan FİRMA sorumlu olacağını peşinen kabul ve taahhüt eder.



	GİZLİLİK SÖZLEŞMESİ		Doküman No	SBLN-001
			Yayın Tarihi	05/01/2022
			Revizyon No	02
	Firma		Revizyon Tarihi	

4- MÜNHASIR HAK SAHİPLİĞİ

Taraflardan her biri kendilerine ilişkin bilgiler üzerinde münhasıran hak sahibidirler. FİRMA; ASHB'nin mülkiyeti altındaki Bilgilere ait tüm fikri mülkiyet haklarının, tasarruf hakkı ve diğer hakların, bilginin sahibi olan ASHB'ye ait olduğunu ve iş bu Sözleşme altında bunların kendisi ile paylaşılmasıyla hiçbir hak, tasarruf hakkı veya avantaj elde etmediğini kabul etmektedir.

5- GİZLİ BİLGİ(LER)'İN KULLANILMASI ŞARTLARI:

İş bu Sözleşme kapsamında ASHB'nin FİRMA ile paylaştığı proje ile ilgili tüm Gizli Bilgiler; FİRMA tarafından, ancak Proje kapsamındaki iş ilişkisini temin edebilmek ve geliştirmek maksadıyla, sözleşme koşulları çerçevesinde ve yapılan işin gereği olarak kullanılabilir.

6- ALINMASI GEREKEN ÖNLEMLER

FİRMA; proje ile ilgili Gizli Bilgiler'in sahibi için değerli ve eşsiz olduğunu ve FİRMA yetkilileri ve/veya çalışanları ve/veya danışmanları ile sözleşme gereği görevlendirdiği sair kişiler tarafından işbu Sözleşme'nin ihlali ve söz konusu bilgilerin açıklanması durumunda, Gizli Bilgiler'in sahibi olan ASHB'nin bundan maddi ve manevi büyük zarar göreceğini kabul etmektedir.

FİRMA; sorumlu olduğu kişilerce projeye ait gizli bilgilerin sözleşmeye aykırı biçimde açıklandığından haberdar olduğunda, derhal ve yazılı olarak ASHB'ye durumu bildirmekle yükümlüdür. Bu durumda; Gizli bilgileri sözleşmeye aykırı olarak açıklanmış olan ASHB, bu bildirim üzerine veya kendiliğinden masrafları FİRMA ait olmak kaydıyla tüm yasal yollara başvurma ve uğradığı zararın giderilmesi diğer taraftan talep etme hakkına sahiptir. Ayrıca FİRMA; ASHB tarafından sözleşmenin ifası gereği kendisine verilen ve/veya sözleşme gereği edindiği Gizli Bilgiler'i kendi ticari ve sair amaçları için kullanması ve 3. kişilere kullandırması, devretmesi durumunda, akde aykırı davranışın karşılığı olarak proje kabul bedelindeki cezai şartı ASHB'ye nakden ve defaten hiçbir ihtar ve ihbara gerek kalmaksızın ödemeyi kabul ve taahhüt etmektedir.

7- GİZLİ BİLGİLERİ İÇEREN MATERYALİN İADESİ

Gizli bilgiler içeren her türlü materyal, taraflar arasındaki ticari ilişkinin ya da iş bu gizlilik sözleşmesinin sona ermesi halinde ve karşı tarafın yazılı ihtar üzerine, derhal bu bilgilerin ait olduğu tarafa iade edilir.

8- GİZLİ BİLGİLERİN AÇIKLANABİLMESİ

FİRMA; ASHB'nin yazılı izni dışında bilgiyi 3. kişilere aktarmaz herhangi bir şekilde ya da herhangi bir yolla dağıtamaz, basın yayın organları ve medya kuruluşları vasıtasıyla açıklayamaz, reklam amacıyla kullanamaz.

9- SÜRE

FİRMA; ASHB'nin "Gizli Bilgilerini", iş bu sözleşmenin konusunu oluşturan iş sona ermiş olsa dahi, süresiz gizli tutmakla yükümlü olduğunu kabul ve beyan etmiştir.



	GİZLİLİK SÖZLEŞMESİ		Doküman No	SBLN-001
			Yayın Tarihi	05/01/2022
			Revizyon No	02
	Firma		Revizyon Tarihi	

10- GENEL HÜKÜMLER

10.1. İşbu Sözleşme'ye yapılacak tüm tadiller yazılı olarak yapılacak ve her iki tarafça imzalanacaktır.

10.2. İşbu Sözleşme hükümlerinden biri veya birkaçının, herhangi bir kanun veya düzenleme altında geçersiz, yasadışı ve uygulanamaz ilan edilmesi durumunda geride kalan hükümlerin geçerliliği, yasalılığı ve uygulanabilirliği bundan hiçbir şekilde etkilenmez veya zarar görmez.

10.3. Taraflardan birinin işbu Sözleşme'nin herhangi bir şekilde karşı tarafça ihlalinden doğan bir hakkını, yetki veya gücünü kullanmaması veya erteleme, iş bu sözleşmedeki herhangi bir haktan vazgeçmesi anlamına gelmez veya bu hakkın daha sonra kullanmasını veya işbu Sözleşme'nin müteakip ihlallerinde diğer hak, yetki ve çözümlerini kullanmasına engel teşkil etmez.

10.4. İşbu Sözleşme hükümlerinden yapılan herhangi bir feragat veya hak sahibinin hiçbir onayı yazılı olarak yapılmadıkça geçerli kabul edilemez.

10.5. İşbu Sözleşme'nin uygulanması veya yorumuyla ilgili uyuşmazlıklarda, haklılığı sabit olan Taraf'ın yaptığı makul harcamalar, ödemeler ve vekâlet ücretini diğer taraftan tahsil etme hakkı saklıdır.

10.6. Taraflar, mahkemelerinin münhasır yargılama yetkisini kabul ederler.

10.7. Tarafların yukarıda belirtilen adresleri yasal ikametgâh adresleri olup; adres değişikliği yazılı olarak karşı tarafa bildirilmediği sürece bu adreslere yapılacak tebligatlar kanunen geçerli bir tebligatın bütün sonuçlarını doğuracaktır.

İşbu sözleşme, bu madde ile birlikte toplam 10 ana maddeden ibaret olup, düzenlenmesine ihtiyaç duyulan diğer koşullar bu sözleşmeyle çelişmeyecek şekilde düzenlenip, sözleşmeye eklenecek ve bu sözleşmenin ayrılmaz bir parçası olacaktır.

Bu sözleşme, taraflarca/...../..... Tarihinde imzalanmış ve aynı gün yürürlüğe girmiştir.

Aile ve Sosyal Hizmetler Bakanlığı

HİZMET ALINAN FİRMA

Bilgi Teknolojileri Genel Müdürlüğü



EK-3

Gizlilik Sözleşmesi (Şahıs)

	GİZLİLİK SÖZLEŞMESİ	Doküman No	SBLN-002
		Yayın Tarihi	05/01/2022
	Şahıs	Revizyon No	02
		Revizyon Tarihi	

GİZLİLİK SÖZLEŞMESİ

Bir tarafta Eskişehir Yolu Söğütözü Mahallesi 2177.Sokak No:10/A Çankaya/ANKARA adresinde bulunan Aile ve Sosyal Hizmetler Bakanlığı (kısaca "ASHB") ile diğer tarafta **HİZMET ALINAN PERSONELİN ADRESİ** adresinde mukim **HİZMET ALINAN PERSONELİN ADI** arasında aşağıdaki şartlarda gizlilik sözleşmesi imzalanmıştır.

1- GİZLİLİK

ASHB projeye ait teknik altyapı, teknik bilgiler, müşteri bilgisi, ticari planlar, mali bilgiler, ticari stratejiler, müşteri listeleri ve proje ile ilgili olarak yapılacak iş ve işlemlere dair, açıkça ve yazılı olarak gizli olduğu beyan edilen sair her türlü bilgi "Gizli" olarak kabul edilecektir. Bu anlamda ASHB projenin kurulum, geliştirme, bakım, veri aktarma süreçlerinde ister sözlü, isterse elektronik ortamda veya yazılı ya da başka bir araçla yapılmış olsun verilen her türlü bilgiler ve bu yolla edinilen her türlü bilgi "Gizli Bilgi" olarak kabul edilecektir. ASHB Proje süresince, yapacağı açıklamalarda ve vereceği bilgilerde kendisine ait birtakım Gizli Bilgiler'i paylaşabilecektir. Taraflar'ın iş bu Sözleşme konusu Gizli Bilgiler'i paylaşımları ve Gizli Bilgiler'in korunması, aşağıda belirtilen şartlar dâhilinde gerçekleşecektir.

2- GİZLİ BİLGİNİN TANIMINA GİRMEYEN BİLGİLER

Kamuoyuna mal olmuş bilgiler, Yürürlükte olan kanun ya da düzenlemeler ya da verilmiş olan bir mahkeme kararı gereğince açıklanması gereken bilgilerdir.

3-GİZLİ BİLGİNİN DİĞER TARAFÇA KORUNMASI

Taraflar, proje ile ilgili kendi Gizli Bilgileri üstündeki haklarını tanımakta ve kabul etmekte olup, işbu Sözleşme altında elde edilen Gizli Bilgiler konusunda aşağıda yazılı olanları sağlamak için gerekli önlemleri almayı kabul ve taahhüt ederler:

a-Büyük bir gizlilik içinde azami dikkat ve özenle korumak,

b-Herhangi bir 3. kişiye hangi suretle olursa olsun vermemek ve / veya alenileştirmemek,

c-Doğrudan ya da dolaylı olarak aralarındaki sözleşme gereği yapılan işin gereği dışında kullanmamak.

Taraflar kendi gizli bilgilerini korumakta gösterdikleri dikkat ve özenin aynısını karşı tarafın gizli bilgilerini korumakta da göstermeyi kabul ve taahhüt ederler.

Taraflar, ancak zorunlu hallerde ve işi gereği bu bilgiyi, öğrenmesi gereken işçilerine, alt çalışanlarına ve kendilerine bağlı olarak çalışan diğer kişilere verebilir, ancak bilginin gizliliği hususunda işçilerini, alt çalışanlarını ve kendilerine bağlı olarak çalışan diğer kişilerin iş bu sözleşme yükümlülüklerine aykırı davranmayacaklarını ve böyle davranmaları halinde doğrudan sorumlu olacaklarını peşinen kabul ve taahhüt eder.

4- MÜNHASIR HAK SAHİPLİĞİ

Taraflardan her biri kendilerine ilişkin bilgiler üzerinde münhasıran hak sahibidirler.



	GİZLİLİK SÖZLEŞMESİ	Doküman No	SBLN-002
		Yayın Tarihi	05/01/2022
	Şahıs	Revizyon No	02
		Revizyon Tarihi	

5- GİZLİ BİLGİ(LER)'İN KULLANILMASI ŞARTLARI:

İş bu Sözleşme kapsamında ASHB'nin paylaştığı proje ile ilgili tüm Gizli Bilgiler ancak Proje kapsamındaki iş ilişkisini temin edebilmek ve geliştirmek maksadıyla, sözleşme koşulları çerçevesinde ve yapılan işin gereği olarak kullanılabilir.

6- ALINMASI GEREKEN ÖNLEMLER

Taraflardan herhangi biri diğer tarafa ait gizli bilgilerin sözleşmeye aykırı biçimde açıklandığından haberdar olduğunda, en kısa sürede, yazılı olarak karşı tarafa durumu bildirmekle yükümlüdür. Gizli bilgileri sözleşmeye aykırı olarak açıklanmış taraf, bu bildirim üzerine masrafları diğer tarafa ait olmak kaydıyla yasal yollara başvurma ve uğradığı her türlü zararın giderilmesini, diğer taraftan talep etme hakkına sahiptir.

7- GİZLİ BİLGİLERİ İÇEREN MATERYALİN İADESİ

Gizli bilgiler içeren her türlü materyal, taraflar arasındaki ticari ilişkinin ya da iş bu gizlilik sözleşmesinin sona ermesi halinde ve karşı tarafın yazılı ihtarı üzerine, derhal bu bilgilerin ait olduğu tarafa iade edilir.

8- GİZLİ BİLGİLERİN AÇIKLANABİLMESİ

Taraflardan hiçbirisi, diğerinin yazılı izni olmaksızın kanunda açıkça belirtilen haller dışında bu bilgiyi 3. kişilere aktarmaz herhangi bir şekilde ya da herhangi bir yolla dağıtamaz, basın yayın organları ve medya kuruluşları vasıtasıyla açıklayamaz, reklam amacıyla kullanamaz.

9- SÜRE

İşbu sözleşme imza tarihinden itibaren yürürlüğe girer ve taraflarca müştereken sona erdirilmedikçe yürürlükte kalır. Taraflar arasındaki ticari ilişki sona erse dahi işbu sözleşmedeki gizlilik yükümlülükleri geçerli olmaya devam eder. Bu sözleşme ya da buradaki herhangi bir hak tamamen ya da kısmen devredilemez.

10- GENEL HÜKÜMLER

10.1. İşbu Sözleşme'ye yapılacak tüm tadiller yazılı olarak yapılacak ve her iki tarafça imzalanacaktır.

10.2. İşbu Sözleşme hükümlerinden biri veya birkaçının, herhangi bir kanun veya düzenleme altında geçersiz, yasadışı ve uygulanamaz ilan edilmesi durumunda geride kalan hükümlerin geçerliliği, yasalılığı ve uygulanabilirliği bundan hiçbir şekilde etkilenmez veya zarar görmez.

10.3. Taraflardan birinin işbu Sözleşme'nin herhangi bir şekilde karşı tarafça ihlalinden doğan bir hakkını, yetki veya gücünü kullanmaması veya erteleme, iş bu sözleşmedeki herhangi bir haktan vazgeçmesi anlamına gelmez veya bu hakkın daha sonra kullanmasını veya işbu Sözleşme'nin müteakip ihlallerinde diğer hak, yetki ve çözümlerini kullanmasına engel teşkil etmez.

10.4. İşbu Sözleşme hükümlerinden yapılan herhangi bir feragat veya hak sahibinin hiçbir onayı yazılı olarak yapılmadıkça geçerli kabul edilemez.



EK-4

Varlık Transfer Formu

	GİZLİLİK SÖZLEŞMESİ	Doküman No	SBLN-002
	Şahıs	Yayın Tarihi	05/01/2022
		Revizyon No	02
		Revizyon Tarihi	

10.5. İşbu Sözleşme'nin uygulanması veya yorumuyla ilgili uyuşmazlıklarda, Ankara Merkez Mahkemeleri ve İcra Daireleri yetkili olup, Türk hukuku uygulanır. Haklılığı sabit olan Taraf'ın yaptığı makul harcamalar, ödemeler ve vekâlet ücretini diğer taraf'tan tahsil etme hakkı saklıdır.

10.6. Taraflar, mahkemelerinin münhasır yargılama yetkisini kabul ederler.

10.7. Tarafların yukarıda belirtilen adresleri yasal ikametgâh adresleri olup; adres değişikliği yazılı olarak karşı tarafa bildirilmediği sürece bu adreslere yapılacak tebligatlar kanunen geçerli bir tebligatın bütün sonuçlarını doğuracaktır.

İşbu sözleşme, bu madde ile birlikte toplam 10 ana maddeden ibaret olup, düzenlenmesine ihtiyaç duyulan diğer koşullar bu sözleşmeyle çelişmeyecek şekilde düzenlenip, sözleşmeye eklenecek ve bu sözleşmenin ayrılmaz bir parçası olacaktır.

Bu sözleşme, taraflarca/...../..... Tarihinde imzalanmış ve aynı gün yürürlüğe girmiştir.

Aile ve Sosyal Hizmetler Bakanlığı

HİZMET ALINAN PERSONEL

Bilgi Teknolojileri Genel Müdürlüğü



Doküman No: FORM-003
Revizyon :01
Yayın Tarihi : 10.10.2021

VARLIK TRANSFER FORMU

TRANSFER BİLGİLERİ

TALEP EDEN

AD SOYAD	
BİRİM/FİRMA	

ALICI BİLGİLERİ

AD SOYAD	
BİRİM/FİRMA	

GÖNDERİCİ BİLGİLERİ

AD SOYAD	
BİRİM	

VARLIK TRANSFER BİLGİLERİ

VARLIK ADI	
MARKA-MODEL	
VARLIK SERİ NO	
TRANSFER YERİ	
TRANSFER TARİHİ	
TALEP NEDENİ ;	
GÖNDERİCİ	ALICI
AD SOYAD	AD SOYAD
İMZA	İMZA



EK-5

Erişim Talep Formu

	FORM		Doküman No: FORM-009
			Yayın Tarihi: 10/11/2021
	Erişim Talep Formu		Revizyon No: 01
			Revizyon Tarihi:

ERİŞİM TALEP EDEN BİLGİLERİ		
Firma/ Kurum Adı:		
Kullanıcı Adı Soyadı/ Sicil No:		
E-Posta Adresi:		
Telefon Numarası:		
İlgili Çalışma/ Proje Adı/ Birimi:		
IP Adresi/ Aktif Dizin Kullanıcı Adı:		
Talep Edilen Erişim Tarihleri:		
Erişim Gerekçesi:		
Erişim Talebi (Erişim İstenen Site, Uygulama, Sunucu Adı, IP ya da IP Bloğu):		
Erişmek İstenen Servis (Port):	☐ RDP ☐ HTTP ☐ Diğer:	☐ SSH ☐ HTTPS
Erişim Yönü	☐ İçeriden içeriye ☐ Dışarıdan içeriye ☐ İçeriden dışarıya	
Dış IP Adresi:		

Talepte Bulunan Kullanıcı ve İlgili Yönetici Taahhüdü

- Talepte bulunan çalışanın işten çıkması durumunda Birim Amiri, Aile ve Sosyal Hizmetler Bakanlığı Bilgi Teknolojileri Genel Müdürlüğüne bildirmek zorundadır. Aksi takdirde yasal her türlü sorumluluk ilgili birime aittir.
- Sistem(ler) üzerinde yapacağım bağlantı için yukarıda belirtmiş olduğum erişim hakkını talep eder ve verilen bu hak sonrası sistemler üzerinde erişim için verilen kimliğim ile oluşacak her türlü problemin sorumluluğunu kabul ettiğimi bildiririm.

Talep Edenin Adı Soyadı / İmza	Birim Amrinin Adı Soyadı / İmza
Bilgi Güvenliği Yöneticisi Adı Soyadı / İmza	Erişim Veren Adı Soyadı / İmza



EK-6

Hizmet Kesintisi Bildirim Formu

	FORM	Doküman No: FORM-015
		Yayın Tarihi: 03/10/2023
	Hizmet Kesintisi Bildirim Formu	Revizyon No: 01
		Revizyon Tarihi:

HİZMET KESİNTİSİ DEĞERLENDİRME FORMU		
1. Bildirimi yapan Birim:		
2. Bildirimi yapan personelin		
Ad, Soyadı	:	
Unvan/Birim	:	
Telefon	:	
E-posta	:	
3. Olay türü:		
☐ Siber Saldırı (Siber Olay Değerlendirme Formu Doldurunuz) ☐ İyileştirme ve Bakım ☐ Planlı Çalıştırma ☐ Anıza ☐ Diğer (Lütfen açıklayınız):		
4. Olay sistem kesintisine sebep oldu mu? ☐ Evet ☐ Hayır		
5. Etkilenen sistemler:		
☐ Uygulama Sunucusu (.....) ☐ Veritabanı Sunucusu ☐ DNS ☐ Posta Sunucusu ☐ Web Sunucusu ☐ Dosya Sunucusu ☐ Güvenlik Duvarı ☐ İnternet Erişimi ☐ Son Kullanıcılar ☐ Diğer (Lütfen açıklayınız):		
6. Olayın kısa tanımı:		



	FORM	Doküman No: FORM-015
		Yayın Tarihi: 03/10/2023
	Hizmet Kesintisi Bildirim Formu	Revizyon No:01
		Revizyon Tarihi:

7. Olayı bildiren kişi/kurum ve tespit edilme yöntemi :

☐ Kurum dışı bildirim ☐ Kurum çalışanı ☐ Bilgi işlem birimi

☐ Kurumsal SOME çalışanı

☐ Diğer (Lütfen açıklayınız):

Tespit edilme yöntemini açıklayınız:

8. Olayın:

Tahmini başlangıç zamanı

Tarih : Saat :

Tespit edildiği zaman

Tarih : Saat :

Yaşanan Toplam Kesinti Süresi

Tarih : Saat :

9. Olaylara ait iz kayıtları tespit edildi mi?

☐ Hayır

☐ Evet

Kaynak IP : _____

Hedef IP : _____

Port : _____

Diğer : _____

10. Alınan Önlemleri Açıklayınız:

EK-7

Log Alma Talep Formu



BİLGİ TEKNOLOJİLERİ GENEL MÜDÜRLÜĞÜ

Doküman No:
FORM-016
Yayın Tarihi:
26/10/2023
Revizyon No:01

Talep Tarihi :/...../.....
Talep Eden Birim:

No	Sistemin Adı/ Sunucu Adı	Source IP (Log'un Oluşturduğu)	Sunucu/Sistem Türü (Web,Veritabanı,Uygulama, FW,Exchange vb.)	Olay Tipi (audit,hata,erişim, performans vb.)	Log Formatı (log, json,txt,csv vb.)	Log Saklama Süresi	Sorumlu Personel	Log Kaybı Tahammül Süresi	Varsa Diğer Açıklamalar
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									

Bilgi Güvenliği Temsilcisi
(Ad Soyad)
İmza

Sorumlu Kişi
(Ad Soyad)
İmza



EK-8

Teknik İnceleme Raporu Formu

	FORM		Doküman No: FORM-013		
	Teknik İnceleme Raporu Formu		Yayın Tarihi: 12/09/2023		
			Revizyon No:01		
Varsa İlgili Yazısı:					
İlgili Birim:					
İnceleme Yeri:					
Refakat Eden Sorumlu Personel:					
NO	Varlık Marka/Model	İncelenen Ürün Tipi (Yazıcı, Tarayıcı, Masaüstü Bilgisayar, Dizüstü Bilgisayar, Diğer. Belirtiniz)	Seri No	Teknik Özellikler	İnceleme Sonucu
1					
2					
3					
4					
5					
6					
İlgili yazıda belirtilen bilişim varlıkları yukarıda belirtilen inceleme yerinde, sorumlu personel refakatinde teknik birimimiz personelince ayrıntılı incelenmiş olup yapılan incelemeler sonucunda;					
Genel Değerlendirme:					

HİZMETE ÖZEL



	FORM		Doküman No: FORM-013		
	Teknik İnceleme Raporu Formu		Yayın Tarihi: 12/09/2023		
			Revizyon No:01		
İlgili Teknik Personel Ad/Soyad:		Unvan:	İmza:	Tarih/Saat:	

HİZMETE ÖZEL





DİJİTAL İÇERİK

Tüm içeriklere alanlarda bulunan
QR kodlardan ulaşabilirsiniz.

www.aile.gov.tr