2020- 2021

KASIM EKENLER MESLEKİ VE TEKNİK ANADOLU LİSESİ

e-GÜVENLİK POLİTİKASI

SCHOOL e-SECURİTY PROTOCOL PREARED

2020- 2021

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1

(1) Bu e-güvenlik politikasının amacı kurumumuz bünyesinde bulunan bilişim kaynaklarının kullanımına yönelik usul ve esasları belirlemektir.

(2) Kasım Ekenler Mesleki ve Teknik Anadolu Lisesi, çevrimiçi güvenliğin (e-Güvenlik), bilgisayarlar, tabletler, cep telefonları veya oyun konsolları gibi teknolojiyi kullanırken, dijital dünyadaki öğrencilerin ve yetişkinlerin korunması için vazgeçilmez bir unsur olduğuna inanmaktadır. Dolayısıyla, riskleri yönetmeleri ve bunlara tepki vermek için stratejiler geliştirmenin yollarını öğrenmeleri için çocuklar desteklenmelidir.

(3) Kasım Ekenler Mesleki ve Teknik Anadolu Lisesi, eğitim standartlarını yükseltmek, başarıyı teşvik etmek, personelin mesleki çalışmalarını desteklemek ve yönetim işlevlerini geliştirmek için toplumun kaliteli İnternet erişimi sunma yükümlülüğüne sahiptir.

Kapsam

MADDE 2-

(1) Bu e-güvenlik politikası kurumumuzdaki tüm personel, öğrenci, veli ile kendilerine herhangi bir nedenle kurumumuz bilişim kaynaklarını kullanma yetkisi verilen paydaş ve konukları kapsar.

(2) Bu e-güvenlik politikası, internet erişimi ve kişisel cihazlar da dahil olmak üzere bilgi iletişim cihazlarının kullanımı için geçerlidir; çocuklar, personel ya da diğer kişilere, çalıştıkları dizüstü bilgisayarlar, tabletler veya mobil cihazlar gibi uzaktan kullanım için okul tarafından verilen cihazlar için de geçerlidir.

Dayanak

MADDE-3

(1) Bu e-güvenlik politikası, 5/12/1951 tarihli ve 5846 sayılı Fikir ve Sanat Eserleri Kanunu, 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu, 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile 25/8/2011 tarihli ve 652 sayılı Millî Eğitim Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname hükümlerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4-

(1) Bu e-güvenlik politikasında geçen;

Bakan: Millî Eğitim Bakanını,

Bakanlık: Millî Eğitim Bakanlığını,

Başkanlık: Bilgi İşlem Dairesi Başkanlığını,

Bilişim Kaynakları: Elektronik ortamda yapılan iş ve işlemlerde kullanılan yazılım, donanım, araç ve gerecini, Doküman Yönetim Sistemi
(DYS): Bakanlık elektronik belge yönetim sistemini,
e-İmza: Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi,
e-Okul: Kurumumuzda öğrenci ve yönetimle ilgili iş ve işlemlerin elektronik ortamda yürütüldüğü ve bilgilerin saklandığı sistemi,
e-Posta: İnternet üzerinden bilgisayarlar aracılığıyla bilgi alışverişini sağlamak için kullanılan elektronik haberleşme sistemini,
Konuk: Kurumumuz bünyesinde kullanmış olduğu bilgisayar, bilgisayar ağı, internet ve benzeri tüm bilişim sistemleri üzerinde yetkilendirilmemiş olan Bakanlık personeli dışındaki kişiler ile görev yeri dışında çalışan Bakanlık personelini,
Kullanıcı: Kurumumuz bünyesinde yer alan bilgisayar, bilgisayar ağı, internet ve benzeri tüm bilişim sistemlerinden yararlanan tüm personeli ile bilişim kaynaklarını kullanma yetkisi verilen paydaş ve konukları,
MEBBİS: Millî Eğitim Bakanlığı Bilişim Sistemlerini,
MEBNET: Kurumumuzda kullanılan intranet ve internet ağlarını, Paydaş: Velilerimizi ve ortak çalışma yapılan kurum veya kuruluşları,
Personel: Kurumumuzdaki tüm çalışanları,
Sistem Odası: Kurumumuzda bulunan bilişim sistemi teçhizatının yer aldığı odayı,
Sistem Yöneticisi: Kurumumuzda görev yapan bilişim personelini, ifade eder.

İKİNCİ BÖLÜM

Sorumluluk ve Genel Kurallar Sorumluluk

MADDE 5-

(1) Kurumumuz, çevrimiçi güvenliğin (e-Güvenlik), bilgi ve iletişim teknolojilerini kullanırken, dijital dünyadaki öğrencilerin ve yetişkinlerin korunması için vazgeçilmez bir unsur olduğuna inanmaktadır. Bu nedenle tüm personel, öğrenci ve velilerin e-güvenlik kapsamında görev ve sorumluluklarını belirler, eğitimi için gerekli çalışmaları yapar,

(2) Kurum personelinin, öğrencilerin cinsel istismarına, müstehcenliğe, şiddet ve intihara yönlendirmeye, uyuşturucu ve uyarıcı madde kullanımını özendirmeye yönelik internet sitelerine girmesi, sohbet oturumları açarak kuruma ait gizli bilgileri paylaşması, oyun oynaması, devlet büyüklerine hakaret etmesi; sosyal medya, gazete, forum ve benzeri sitelerde kurumu küçük düşürücü ve kamuoyunu yanıltmaya yönelik yorumlar yapması, özel hayatına ilişkin suç oluşturabilecek nitelikteki bilgi ve işlemleri kurum internet hattı üzerinden yapması ile ilgili cezai ve hukuki sorumluluğu kendisine aittir. Kurumumuz yukarıda belirtilen davranışları tespit etmeye ve önlemeye yönelik erişim politikalarını uygular.

(3) Bu e-güvenlik politikası kapsamında kurumumuz bilgi ve sistem güvenliğinin planlı, sorunsuz, güvenli ve disiplin içinde gerçekleştirilmesini sağlamakla sorumludur. Bakanlığımızın "Bilgi ve Sistem Güvenliği Politikaları"nı takip etmekle ve bu politikalara uymakla yükümlüdür.

(4) Kurumumuz, yasal hükümler çerçevesinde bilişim kaynaklarını ve bunlarla gerçekleştirilen aktiviteleri izleme, kaydetme ve periyodik olarak inceleme ve denetleme hakkını saklı tutar.

(5) Kurumumuz bilişim kaynaklarında meydana gelen arızalara yetkisiz personel tarafından müdahale edilemez. Edilmesi sonucunda teknik destek verilmez ve ortaya çıkabilecek arızalar, maddi hasarlar ya da kurumsal ağ güvenliğinin ihlaline yol açan uygulamalardan ilgili personel sorumludur.

(6) Kurumumuz demirbaşına kayıtlı olmayan, personelin şahsi bilgisayarlarına arıza bakım ve teknik destek hizmeti sunulmaz.

(7) Kurumumuzda bulunan yetkili kullanıcı hiçbir sebepten ötürü öğretmen, öğrenci ve velilere ait kişisel bilgileri (ad soyad, T.C. kimlik numarası, çalıştığı kurum, okuduğu okul, adres, telefon numarası, e-posta adresi vb.) diğer kamu kurumları ve 3. şahıslar ile paylaşamazlar. Gerekli görüldüğü zaman bu bilgilerin paylaşımı için Başkanlıktan talepte bulunurlar. Başkanlık uygun gördüğü durumlarda bilgileri yasal sınırlar içerisinde ilgili kamu kurum ve kuruluşları ile paylaşır.

(8) Kullanıcı, kurumun kritik bilgisinin ortaya çıkmasına veya kurum servislerinin ulaşılmaz hale gelmesine sebep olabilecek tüm eylemlerden kaçınır.

(9) Kullanıcı, kullanımına tahsis edilen bilişim kaynaklarının güvenliğine yönelik önlemleri alır.

(10) MEBNET ağı ve bu ağı kullanan her kullanıcı ve cihaz ile ilgili her türlü erişim, güvenlik ve yönetim politikaları Başkanlık tarafından belirlenir ve uygulanır. Kurumumuz Başkanlık tarafından belirlenen politikalara uymak ile yükümlüdür.

Genel Kurallar MADDE

6- Okul Personeli İçin:

(1) Kullanıcı, bilgi teknolojileri kapsamındaki bilişim kaynaklarına zarar veremez, işleyişi aksatma, yavaşlatma veya durdurma eylemlerinde bulunamaz, içeriğini izinsiz olarak değiştiremez.

(2) Kullanıcı, bilgi teknolojileri kapsamındaki herhangi bir kaynağı, kendisinden başka hiç kimse adına ve yararına kullanamaz veya bir başkasının kullanımına izin veremez.

(3) Kullanıcı, başka kullanıcıların bilgisayarında yer alan şifrelendirilmiş paylaşım alanlarına çeşitli yöntemleri kullanarak erişemez ve bu türlü girişimlerde bulunamaz.

(4) Kullanıcı, çalışmalarının sonlandırılması ile birlikte kendisinde bulunan bilgisayar, yazıcı, disk ve benzeri tüm donanım ve malzemeleri, tüm yazılım ürünleri ve kodları ile bilişim sistemleri kullanımına yönelik tüm şifreleri içeren kurumumuzun tüm bilişim varlıklarını iade eder. Kullanıcının bilgi ve bilgi işleme olanaklarına erişim hakları kaldırılır.

(5) Kurumumuzda çalışma yapan kurum dışı personelin çalışmaları kayıt altına alır ve herhangi bir olumsuzluk durumunda bu olumsuzluğu açıklayıcı rapor sunar.

(6) Bilgi güvenliğini etkileyen arızalar mümkün olan en kısa sürede uygun yönetim kanalları kullanılarak rapor edilir.

(7) Gizlilik içeren bilgiler ile kişisel veriler, e-devlet kapsamında protokol yapılarak bilgi paylaşımı yapılan veya kanunen yetkili sayılan merciler dışında hiçbir kişi, kurum ya da kuruluş ile paylaşılmaz.

(8) Gizlilik içeren bilgilerin paylaşımı ile ilgili yapılacak protokoller Bakanlık merkez birimlerince veya Bakanlıkça yetkilendirilen taşra teşkilatı birimlerince yapılır.

Öğrenciler İçin:

(1) Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.

(2) Okulun Kabul Edilebilir Kullanım Politikalarını okumak ve onlara bağlı kalmak.

(3) Çevrim içi ve çevrimdışı başkalarının hislerine ve haklarına saygı duymak.

(4) İşler ters giderse, güvenilir bir yetişkinden yardım istemek ve çevrimiçi güvenlik sorunlarıyla karşılaşan diğer kişileri desteklemek.

(5) Kendilerini ve başkalarını çevrimiçi olarak korumak için sorumluluk almak.

(6) Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.

(7) Belli bir teknolojiyi kullanmanın kişisel risklerini değerlendirmek ve bu riskleri sınırlamak için güvenli ve sorumluluk sahibi davranmak.

Velilerimiz İçin:

(1) Okul Kabul Edilebilir Kullanım Politikalarını okumak, öğrencilerını bu politikaya bağlı kalmaya teşvik etmek ve uygun olduğunca kendilerinin de bağlı kalmasını sağlamak.

(2) Çocuklarıyla çevrimiçi güvenlik konularını tartışmak, okulun çevrimiçi güvenlik yaklaşımlarını desteklemek ve evde uygun güvenli çevrimiçi davranışları pekiştirmek.

(3) Teknoloji ve sosyal medyanın güvenli ve uygun kullanımını modellemek.

(4) Davranışlarında, çocuğun çevrimiçi olarak zarar görme tehlikesi altında olduğunu gösteren değişiklikleri belirlemek.

(5) Okul veya diğer uygun kurumlardan, kendileri ve ya çocukları çevrimiçi problem veya sorunlarla karşılaşırsa yardım veya destek istemek.

(6) Okulun çevrimiçi güvenlik politikalarının oluşturulmasına katkıda bulunmak.

(7) Öğrenme platformları ve diğer ağ kaynakları gibi okul sistemlerini güvenli ve uygun bir şekilde kullanmak.

(8) Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.

ÜÇÜNCÜ BÖLÜM

Bilgi ve Sistem Güvenliği Kuralları ve Politikaları

Aktif Dizin Hizmetleri Kuralları

MADDE 7-

(1) Kurumumuz bünyesinde çalışmakta olan veya işe başlayan her personel ile ihtiyaç dahilinde paydaş ve konuklar için aktif dizin kullanıcı hesabı açılır.

(2) Kullanıcı, kendisine verilen "kullanıcı adı" nı ve "şifresi" ni bir başkası ile paylaşmaz ve bir başkasına kullandırmaz. Kullanıcının, "kullanıcı hesabına" ait geçici şifresini derhal değiştirerek, bu Yönergenin 9'uncu maddesinde yer alan şifre politikasına uygun olarak şifresini oluşturur.

(3) Kullanıcının, Başkanlıkça belirlenecek periyodlarla "kullanıcı şifresini" değiştirmesi gerekir. Kullanıcı şifresini yenilemeyen veya kullanıcı şifresini üst üste birkaç kez hatalı giren kullanıcının, kullanıcı hesabı geçersiz kılınır ve iletişim ağına giriş izni otomatik olarak kaldırılır. İlgililerin başvurması halinde ilgili hizmetin bir üst yetkilisi tarafından uygun görülenler tekrar aktif hale getirilir.

(4) Her bir kullanıcı, bilgisayarda kendi "kullanıcı adı" ve "şifresi" ile oturum açarak çalışır. Çalışması biten kullanıcı, oturumu veya bilgisayarını kapatarak bilgisayara başkalarının fiziksel erişimini engeller. Bilgisayar başından kısa süreli ayrılmalarda bilgisayar oturumunu kilitler.

(5) İlgili hesabın amacı dışında kullanılması ve bu hesaptan doğabilecek zararların sorumluluğu, hesabı kullanan kullanıcıya aittir.

e-Posta İşlemleri Kuralları

MADDE 8-

(1) Kullanıcı, tüm resmî yazışmalarında kullanmak üzere e-posta adresini kurumumuza bildirmekle yükümlüdür.

(2) Kullanıcı, kurum saygınlığını zedeleyecek ve/veya başkalarını taciz edecek kurum içi veya kurum dışı eposta gönderemez. e-Posta adresini internet üzerinde herhangi bir siteye kurumsal amaçlar dışında abone olmak için kullanılamaz.

(3) Kullanıcı, kurum tarafından kendisine veya çalıştığı birime tahsis edilen e-posta adresini, sohbet (chat) yapmak için kullanmaz.

(4) Kullanıcı, hesabını ticari ve kar amaçlı olarak kullanamaz. Çok sayıda kullanıcıya toplu halde reklam, tanıtım, duyuru ve benzeri amaçlı e-posta gönderemez ve zincir e-posta, sahte e-posta vb. e-postalara yanıt yazamaz.

(5) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmaz ve derhal silinir.

(6) Kullanıcı, kendisine ait e-posta adresinin şifresinin güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumludur. Şifresinin başkası tarafından tespit edildiğini fark ettiği anda şifresini değiştirip kurumumuzla temasa geçip durumu haber vermekle yükümlüdür.

(7) Güvenlik ve performans açısından e-posta eklentilerinin toplam boyutu hiç bir durumda Başkanlığın belirlediği boyut değerinden fazla olamaz.

(8) e-Posta hesapları için öngörülen kotadan dolayı bir problem yaşamaması için e-posta hesabının kontrolü kullanıcıya aittir.

(9) Usulsüz kullanıldığı tespit edilen veya spam, virüs yayarak sistem ve kullanıcıların güvenliğini tehdit eden e-posta hesapları ilgililere bildirilerek gerekli önlemlerin alınması sağlanır.

Şifre Politikası

MADDE 9-

(1) Kullanıcı, kurumda kullanılan ve belirli bir şifre ile girilmesi zorunlu olan her türlü uygulama için şifre belirler.

(2) Kullanıcının şifrelerini belirlerken dikkat edeceği kurallar şunlardır:

a) Şifreler en az 8 (sekiz) karakter olmalıdır.

b) Şifreler küçük harf, büyük harf, rakam ve simgelerin kullanıldığı karışık yapıda olmalıdır.

c) Şifrelerin Başkanlıkça belirlenecek sayıda hatalı girilmesi sonucu, kullanıcı hesabı Başkanlığın politikalarına bağlı olarak kilitlenebilir. İlgililerin başvurması halinde ilgili hizmetin bir üst yetkilisi tarafından uygun görülenler tekrar aktif hale getirilir.

d) Şifreler en geç altı ayda bir değiştirilir.

e) “Yönetici/Admin” kullanıcı şifreleri sadece sistem yöneticilerinde olur, kesinlikle son kullanıcılarla paylaşılmaz.

f) Şifreler herhangi bir kişi ile paylaşılmaz.

Temiz Masa – Temiz Ekran Politikası

MADDE 10-

(1) Sistemlerde kullanılan şifreler, masaüstü veya ekran üstü gibi herkes tarafından görülebilecek yerlere yazılmaz.

(2) Personel, bilgisayarını belli bir süre kullanmadığı zaman otomatik olarak şifre ile oturum açmasını gerektirecek şekilde ayarlar.

(3) Kullanıcı, gizli bilgi içeren evrakı ağ üzerinden paylaşmaz, gizli bilgi içeren atık evrakı imha eder.

(4) USB bellek, harici disk vb. hafıza ünitelerinin kullanım şartlarını Başkanlık belirler. Başkanlık gerekli gördüğü durumlarda ilgili ünitelerin kullanımının durdurulması, sınırlandırılması veya şifrelenmesi gibi uygulamaları yürürlüğe koyar.

(5) Personel, bilgisayarındaki, USB belleğindeki, harici diskindeki ve benzeri veri depolamanın mümkün olduğu ortamlardaki gizlilik dereceli bilgi içeren her türlü belgenin güvenliğini sağlamakla yükümlüdür. USB veya harici diske gizli/önemli verilerin konulması gerekiyorsa şifrelenerek saklanır.

Ağ ve İnternet Kullanımı

MADDE 11-

(1) Tüm kullanıcılar interneti bilinçli bir şekilde kullanmak, başkalarının hakkını ihlal edici ve bilişim sisteminin işleyişini engelleyici, bozucu faaliyetlerde bulunmamakla yükümlüdür.

(2) Kurumumuzdaki tüm kullanıcılar;

a) Bakanlık sunucuları üzerinde tahsis edilen kullanıcı adı, şifre ve IP adresi kullanılarak gerçekleştirilen her türlü etkinlikten,

b) Kendisine tahsis edilen bilgisayar üzerinde bulundurduğu belge, yazılım gibi her türlü kaynağın içeriğinden,

c) Bilişim sisteminin kullanımı hakkında yetkili makamlar tarafından talep edilen bilgilerin doğru ve eksiksiz verilmesinden,

d) Bakanlık tarafından sağlanan güvenlik programlarının aktif olarak kullanılmasından ve güncellenmesinden,

e) Bilişim sisteminin; kullanım kurallarına, kanun ve yönetmelikler ile Bakanlığın tabi olduğu mevzuata uygun olarak kullanımından sorumludur.

(3) Kurumumuzdaki tüm kullanıcılar, kurumumuz bünyesindeki tüm bilişim kaynaklarını ve MEBNET'i;
a) Bakanlık ağına ve haricindeki bir sisteme, ağ kaynağına veya servisine saldırı niteliğinde girişimlerde bulunmak,

b) Diğer kullanıcılara ait verileri bozmak ya da zarar vermek, gizlilik hakkını ihlal etmek,

c) Yasaklanmış her türlü materyali üretmek ya da dağıtmak,

ç) Gerçek dışı, sıkıntı ve rahatsızlık verici, gereksiz endişe yaratacak materyali üretmek ve dağıtmak,

d) Başka bir kullanıcının e-posta adresini, o kullanıcının izni olmadan kullanmak,

e) Yerel, ulusal, uluslararası bilgisayarları veya hizmetleri kasıtlı olarak yetkisiz kullanmak,

f) Başkalarının telif haklarını ihlal edici konumda olan yazı, makale, kitap, film, müzik eserleri gibi materyali edinmek, yayınlamak, dağıtmak,

g) Özel yazılım, oyun, film, müzik, video vb. materyalleri edinmek, yayınlamak, kullanmak, dağıtmak,

ğ) Canlı televizyon ve radyo yayınlarını izlemek/dinlemek,

h) Resmî işlemler dışındaki interaktif uygulamalara/hizmetlere erişmek,

ı) Bulut ve depolama sistemlerine erişmek,

i) Sosyal medya hesaplarına erişmek,

j) Siyasi ve ideolojik propaganda yapmak için kullanamaz.

(4) Telif hakları ve lisansları ihlal eden, zararlı yazılım bulunduran, MEBNET ağında yoğun ağ trafiğine sebep olan iki veya daha fazla kullanıcı arasında veri paylaşmak için kullanılan noktadan noktaya (Peer-to-peer - P2P) uygulamaları kullanılmaz. Dosya paylaşımı, anlık mesajlaşma programları ve kurum altyapısında soruna yol açacak şekilde yoğun ağ trafiğine sebep olan uygulamalar ile güvenlik tehdidi oluşturan reklam, içerik, site, kullanıcı, yazılım, uygulama, erişim sağlayan cihazların tamamı gerekli görüldüğünde Başkanlık tarafından filtrelenir veya erişime kapatılır.

(5) Zararlı veya güvenlik tehdidi oluşturan yazılım, uygulama, eklenti vb. içerik barındıran bilgisayarlar yeniden kurulum yapılmadan kurumsal ağa dâhil edilemez.

(6) Bilgisayarlara tahsis edilen IP numarası ve ortam erişim kontrolü adresi (MAC adresi) ile BIOS ayarları Bakanlık tarafından yetkilendirilmiş kişiler dışında değiştirilemez.

(7) Kurum ağına sistem yöneticisinin bilgisi dışında herhangi bir aktif ağ cihazı eklenemez.

(8) Kullanıcılar, kişisel bilişim kaynaklarını kurum ağında sistem yöneticisinden izin almadan kullanamaz.

(9) Kurum içinde hizmet veren sunucu, sistem veya kullanıcı bilgisayarlarına uzaktan erişim, zorunlu hallerde Başkanlığın onayı/izni alınarak yapılır.

(10) MEBNET erişimleri ve kaynakları öncelikli olarak resmî ve onaylı kurum işlerinin gerçekleştirilmesi için kullanılır.

(11) Kullanıcı, kendi kullanıcı hesaplarıyla internet üzerinden gerçekleştirdiği tüm işlemlerden sorumludur. Kimlik bilgilerini uygun bir şekilde saklar ve başkalarıyla paylaşmaz.

(12) Kurumsal ağ güvenliği açısından tehlike yaratabilecek nitelikte zararlı olduğu tespit edilen internet adreslerine erişim tüm kullanıcılar için engellenir.

(13) Kurumsal ağ üzerindeki bilgisayarlara erişim hakkı, yetkisi olmayan kişilere verilemez.

(14) Kurumumuzda tanımı Başkanlık tarafından yapılan MEBNET ağı dışında bir ağ kullanılamaz.

(15) Kurumumuzdaki MEBNET ağında Başkanlık tarafından oluşturulan MEB Sertifikası kullanılır. MEB Sertifikası yüklü olmayan cihazların erişimine izin verilmez.

(16) Merkez ve taşra teşkilatında MEBNET ağına izinsiz kablosuz bağlantı alanı cihazı takılamaz.

(17) Kurumumuza ait gizli ya da açık her türlü veri Bakanlık sistemleri üzerinde barındırılır. Herhangi bir bulut depolama sistemine veri aktarılmaz.

(18) Kurumsal ağ üzerindeki bilgisayarlarda güvenlik politikalarının Başkanlık tarafından belirlendiği antivirüs yazılımı kullanılır.

(19) Kurumumuzda kullanılan cihazlarda zararlı yazılım tespit edilen, saldırmaya yönelik teşebbüste bulunan ve kullanılan güvenlik sistemlerini aşmaya, atlatmaya yönelik her türlü tünel, proxy, vpn vb. program kullanan kullanıcıların, internet ve intranet erişimleri kesilir. İlgili durum ortadan kalkınca erişim tekrar sağlanır. Erişim politikalarını ve sistemlerini aşmaya veya bilişim sistemlerine saldırmaya yönelik girişimde bulunan kullanıcılar için rapor tutulur, üst makamlara bildirilir. Başkanlık tarafından belirlenir ve yönetilir.

(20) Kurumumuzca satın alınması düşünülen yazılım ve programlar için Başkanlıktan uygun görüş alınır.

İnternet Sitesi Barındırma Hizmeti Politikası

MADDE 14-

(1) Kurumumuza ait internet sitesinin barındırma hizmeti Bakanlık sunucuları üzerinden yapılır.
(2) Kurum internet sitelerinin hazırlanmasında, güncellenmesinde ve yönetilmesinde dikkat edilecek hususlar şunlardır:
a) Bakanlık tarafından belirlenen internet sitesi standartlarına göre hazırlanır.
b) Her türlü içerikten kurum amiri sorumludur.
c) Uygulamalara yetkisiz kişilerin erişimini engelleyen tedbirler alınır.
ç) Alınan web hizmetine ait şifreler kurum amiri ve görevli personelin sorumluluğu altındadır.
d) Kritik öneme sahip içerikler web hizmeti alan kurum tarafından görevlendirilen yetkili ya da yetkililerce güvenli bir ortamda yedeklenir.
e) Herhangi bir saldırı halinde site üzerinde bir değişiklik yapılmadan Başkanlığa haber verilir.
f) Tahsis edilen web alanında virüs, truva atı vb. zararlı içerik veya bağlantı, oyun, yetkisiz erişime sebep olabilecek uygulamalar bulundurulmaz.
g) Yayınlanacak her türlü içerik telif hakları, fikrî haklar, şeref ve haysiyetin korunması ve gizlilikle uyumlu olur.
ğ) Bakanlığın herhangi bir politikasını, kuralını ya da düzenlemesini ihlal edemez.
h) Web barındırma alanı, internet sitesi yayıncılığı dışında dosya depolama ya da arşiv alanı olarak kullanılamaz.

Nitelikli Elektronik Sertifika (e-İmza) Kullanımı
MADDE 15-

(1) Kurumumuzda Elektronik Belge Yönetimi, Doküman Yönetim Sistemi üzerinden güvenli elektronik imza ile yapılır.
(2) Güvenli elektronik imza sayısal imzadır ve elle atılan imza ile aynı hukukî sonucu doğurur ve aynı ispat gücüne haizdir.
(3) Kullanıcılar elektronik imzalarını ve şifrelerini hiç kimse ile paylaşmaz.
(4) e-İmza veya şifrenin başkasının eline geçmesi sonucu meydana gelecek her türlü durumda yasal sorumluluk e-imza sahibine ait olur.
(5) e-İmzanın çalınması, kaybedilmesi durumunda sorumluluk kullanıcıya aittir ve ESHS'den temin eder.

(6) Kullanıcı sertifika sağlayıcılarından gelen e-imza güncellemelerinin tarihlerini takip eder ve güncellemeleri zamanında, e-imzasını kullanarak yapar. Aksi takdirde ortaya çıkabilecek her türlü maddi ve hukuki sonuçtan sertifika sahibi sorumludur.
(7) Kullanıcı, ESHS'ye tanımlı kişisel bilgi değişikliklerini ESHS' ye bağlı çağrı merkezlerini arayarak günceller.

DÖRDÜNCÜ BÖLÜM

Güvenlik Eğitimleri Politikaları Öğrencilerin eğitimi

MADDE 15 –

(1) Öğrenciler arasında güvenli ve sorumlu internet kullanımının önemi ile ilgili farkındalık yaratmak için bir çevrimiçi güvenlik (e-Güvenlik) müfredatı oluşturulur ve okulun tamamında yer alır.

(2) Güvenli ve sorumlu kullanım ile ilgili eğitim internet erişiminden önce yapılacaktır. (3) Müfredat geliştirme ve uygulama da dahil olmak üzere okul çevrimiçi güvenlik politikaları ve uygulamaları yazarken ve geliştirirken öğrenci katkıları aranacaktır.

(4) Öğrenciler, Kabul Edilebilir Kullanım Politikasını, yaşlarına ve yeteneklerine uygun bir şekilde okumak ve anlamak için desteklenecektir.

(5) Tüm kullanıcılara ağ ve internet kullanımının izleneceği bildirilecektir.

(6) Çevrimiçi güvenlik (e-Güvenlik) PSHE, SRE, Citizenship and Computing / BİT programlarına dahil edilecek ve hem güvenli okul hem de evde kullanımını kapsayacaktır.

(7) Kabul Edilebilir Kullanım beklentileri ve Posterler, Internet erişimi olan tüm odalarda yayınlanacaktır.

(8) İnternetin ve teknolojinin güvenli ve sorumlu kullanımı, müfredatta ve tüm konularda güçlenecektir.

(9) Dışarıdan destek, okulların dahili çevrimiçi güvenlik (e-Güvenlik) eğitim yaklaşımlarını tamamlamak ve desteklemek için kullanılacaktır.

(10) Okul, öğrencilerin teknolojiyi olumlu şekilde kullandıklarını ödüllendirecektir.

(11) Okul, öğrencilerin ihtiyaçlarına uygun olarak çevrimiçi güvenliği geliştirmek için akran eğitimini uygulayacaktır.

(12) Okulda daha güvenli internet gününün (SID) kutlanacak ve yapılacak etkinliklerle güvenli internet hakkında bilgi verilecektir.

Personelin eğitimi

MADDE 16 –

(1) Çevrimiçi güvenlik (e-Güvenlik) politikası, tüm çalışanların katılımı için resmi olarak sağlanacak ve tartışılacak ve korunma sorumluluğumuzun bir parçası olarak güçlendirilecek ve vurgulanacaktır.

(2) Personel, İnternet trafiğinin izlenebileceğini ve tek bir kullanıcıya kadar izlenebileceğinin farkında olacak. Okul sistemlerini ve cihazlarını kullanırken takdir yetkisi ve profesyonel davranış gereklidir.

(3) Personelin tüm üyelerine, profesyonel ve kişisel olarak, güvenli ve sorumlu İnternet kullanımı konusunda güncel ve uygun personel eğitimi, düzenli (en az yıllık) temelde çeşitli şekillerde sağlanacaktır.

(4) Çalışanların tüm üyeleri, çevrimiçi davranışlarının okuldaki rolü ve itibarını etkileyebileceğinin farkına varacaktır. Mesleği veya kurumu çürüme durumuna düşürdüğü veya profesyonel yeteneklerine güvenini kaybetmiş bir şeyin bulunduğu düşünülürse, kamusal, disiplin veya hukuki önlemler alınabilir.

(5) Filtreleme sistemlerini yönetme veya BİT kullanımını izleme sorumluluğu taşıyan personelin üyeleri, Liderlik Ekibi tarafından denetlenecek ve sorunları veya endişeleri bildirmek için açık prosedürlere sahip olacaklar.

(6) Okul, çalışanların öğrencilerin yaşlarına ve yeteneklerine göre kullanması gereken yararlı çevrimiçi araçları vurgulamaktadır

Ebeveynlerin eğitimi

MADDE 17 –

(1) Kasım Ekenler Mesleki ve Teknik Anadolu Lisesi, öğrencilerin internetin ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmesi için ana-babaların oynayacakları önemli bir role sahip olduklarını kabul eder.

(2) Ebeveynlerin dikkatleri, okul açıklamaları ve okul web sitesinde okul çevrimiçi güvenlik (e-Güvenlik) politikasına ve beklentilerine yönelecektir.

(3) Okul Anlaşması´nın bir parçası olarak ebeveynlerin çevrimiçi güvenlik bilgilerini okumaları istenecektir. (4) Ebeveynler, Okula Kabul Edilebilir Kullanım Politikası´nı okumaya ve çocuklarıyla etkilerini tartışmaya teşvik edilecektir.

(5) Çevrimiçi güvenlik konusundaki ebeveynler için bilgi ve rehberlik, ebeveynlere çeşitli biçimlerde sunulacaktır.

(6) Ebeveynlerin, çevrimiçi olarak çocukları için olumlu davranışları rol modellemeleri teşvik edilecektir.