1. AMAÇ

1.1. Bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci Bilgi Güvenliği Yönetim Sistemi Standardında tanımlanmaktadır. Bilgi İşlem Daire Başkanlığı (Başkanlık) ISO 27001 Bilgi Güvenliği Yönetim Sistemi sertifikasyon sürecini 24.12.2018 tarihi itibarı ile tamamlamıştır. Bu standart kapsamında son kullanıcıların dikkat etmesi gereken hususlar aşağıda yer almaktadır.

2. BİLİŞİM VARLIKLARININ KULLANIMINDA DİKKAT EDİLMESİ GEREKEN HUSUSLAR

2.1. Hassas bilgiler içeren evraklar, bilgi ve belgeler masa üzerinde kolayca ulaşılabilir yerlerde ve açıkta bulundurulmaz.

2.2. Çalışma saatleri sonunda ise masaüstünde herhangi bir doküman bulundurulmaz. Bu bilgi ve belgeler kilitli yerlerde muhafaza edilmelidir.

2.3. Ofisten uzun süreli ayrılmalar öncesinde, çalışma masası ve çevre ünitelerinde evrak temizliği yapılır. Önemli dokümanlar dolaplara ve kilitli çekmecelere kaldırılır.

2.4. Personel, Bilgisayara ve/veya işletim sistemine şifre tanımlamamış ise, şifre tanımlamalı bilgisayar başından kalkarken mutlaka oturumu kilitlemeli, bilgisayarını belli bir süre kullanmadığı zaman otomatik olarak şifre ile oturum açmasını gerektirecek şekilde ayarlamalıdır.

2.5. Çalışma saatleri dışında bilgisayar kapalı ve uyku durumunda bırakılır.

2.6. Çalışma saatleri içerisinde bilgisayar başından ayrılırken bilgisayar mutlaka kilitli bırakılır.

2.7. Taşınabilir medya ve mobil cihazlar daima kullanıcısının yanında bulundurulur. Kullanılmadığı durumlarda mutlaka kilitli dolaplarda muhafaza edilir.

2.8. Masaüstlerinde kuruma ait bilgi içeren dokümanlar kilitli ortamda tutulur.

2.9. Kuruma ait antetli kağıtlar kilitli ortamlarda tutulur.

2.10. Yazdırma işlemi yapan kişi yazıcıdaki çıktıyı kendi kontrolüne alır. Hassas ve sınıflandırılmış bilgi uzak ağ yazıcılarından yazdırılamaz. Uzak yazıcılardan yazdırma yapılacak ise parola korumalı yazdırma özelliği kullanılır.

2.11. Şifreler kâğıt, yapışkan kâğıt ve ajanda gibi matbu ortamlarda yazılı olarak bulundurulamaz.

2.12. Sistemlerde kullanılan şifre, telefon numarası ve T.C Kimlik numarası gibi bilgiler ekran üstlerinde veya masaüstünde bulundurulmamalıdır.

2.13. Her türlü haberleşmede kullanılan cihazlar (telefon, faks, fotokopi makineleri) yetkisiz erişimlere bırakılmamalıdır.

2.14. Cihazlar üzerinde belge, doküman bırakılmayacaktır.

2.15. Kullanım ömrü sona eren ve artık ihtiyaç duyulmadığına karar verilen bilgiler kâğıt öğütücü, disk/disket kıyıcı, yalana vb. metotlarla imha edilmeli, bilginin geri dönüşümü ya da yeniden kullanılabilir hale geçmesinin önüne geçilmelidir.

2.16. Her türlü bilgiler şifreler anahtarlar ve bilginin sunulduğu sistemler (sunucu, dizüstü ve masaüstü bilgisayarlar vb. cihazlar) yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde başıboş bırakılmamalıdır.

2.17. Merkezi Kimlik/Etki alanı giriş şifresi hiçbir şekilde başkalarıyla paylaşılmamalı, bu şifrelerin kötü niyetli kişilerin eline geçmesi durumunda ortaya çıkacak olan her türlü hukukî sorumluluğun kullanıcıya ait olacağı bilinmelidir.

2.18. Şifre belirlenirken, yüksek güvenlikli olması için büyük harf, küçük harf, sayılar ve özel karakterlerden (#%&?* vb.) oluşan parolalar tercih edilmeli ve belli aralıklarla değiştirilmelidir. Şifreler yazılı olarak ekran üstlerinde veya masaüstünde bulundurulmamalıdır.

2.19. Kullanıcılar bilgisayarlarını, sadece iş ve akademik çalışma amacıyla kullanmalı, bu amaçlar dışında oyun, bahis, sohbet programları, vb. başta olmak üzere, sistem ve network performansını düşürerek bilgisayarı yavaşlatan, iş ve akademik çalışmalarla ilgisi olmayan program ve/veya dosyalar bilgisayarlara kurulmamalı, akademik ve ders çalışmaları dışında sosyal medya, film, dizi, müzik, vb. içerikli web sayfalar ziyaret edilmemelidir.

2.20. Kullanıcılar, kullandıkları bilişim cihazlarının (masaüstü, dizüstü bilgisayarlar, tablet, telefon vb.) sistem üzerinde kendi adlarına kaydedildiğinden ilgili cihazların amacı dışında kullanımından doğabilecek zararlardan sorumlu oldukları bilinmeli, kısa süreli de olsa cihazın başından ayrılmaları halinde oturumlarını kilitlemeleri (Ctrl+Alt+Del Enter) gerekmekte olup, bilişim cihazları ikinci şahıslarla paylaşılmamalıdır.

2.21. Kullanıcılar, kullandıkları bilişim cihazlarının (masaüstü, dizüstü bilgisayarlar, tablet, telefon vb.) sistem üzerinde kendi adlarına kaydedildiği için olası cihaz/kullanıcı değişikliği durumunda cihazı devreden kullanıcılar **destek.ahievran.edu.tr** web adresinden Başkanlığa bildirmelidir.

2.22. Anti-virüs yazılımları; solucan, truva atı vb. kodların çalıştırılmasını engelleyeceğinden, kullanıcıların bilgisayarlarında bulunan Windows Defender uygulamasını pasif etmemeli veya kaldırılmamalıdır.

2.23. Zorunlu haller dışında USB, CD, DVD vb. ortamlarından bilgisayara herhangi bir dosya yüklenmemeli, zorunlu olması halinde dosyalar Microsoft Defender programı ile taranmalıdır.

2.24. Merkezi sistemden yüklenilen programlar herhangi bir şekilde bilgisayardan kaldırılmamalı, çalışması engellenmemelidir. Güvenlik duvarını aşan (hotspot, ultrasurf vb. genel ismiyle Proxy ve VPN uygulamaları) programların kullanılmaması, kullanılması durumunda ortaya çıkacak olan her türlü hukukî sorumluluğun kullanıcıya ait olacağı bilinmelidir.

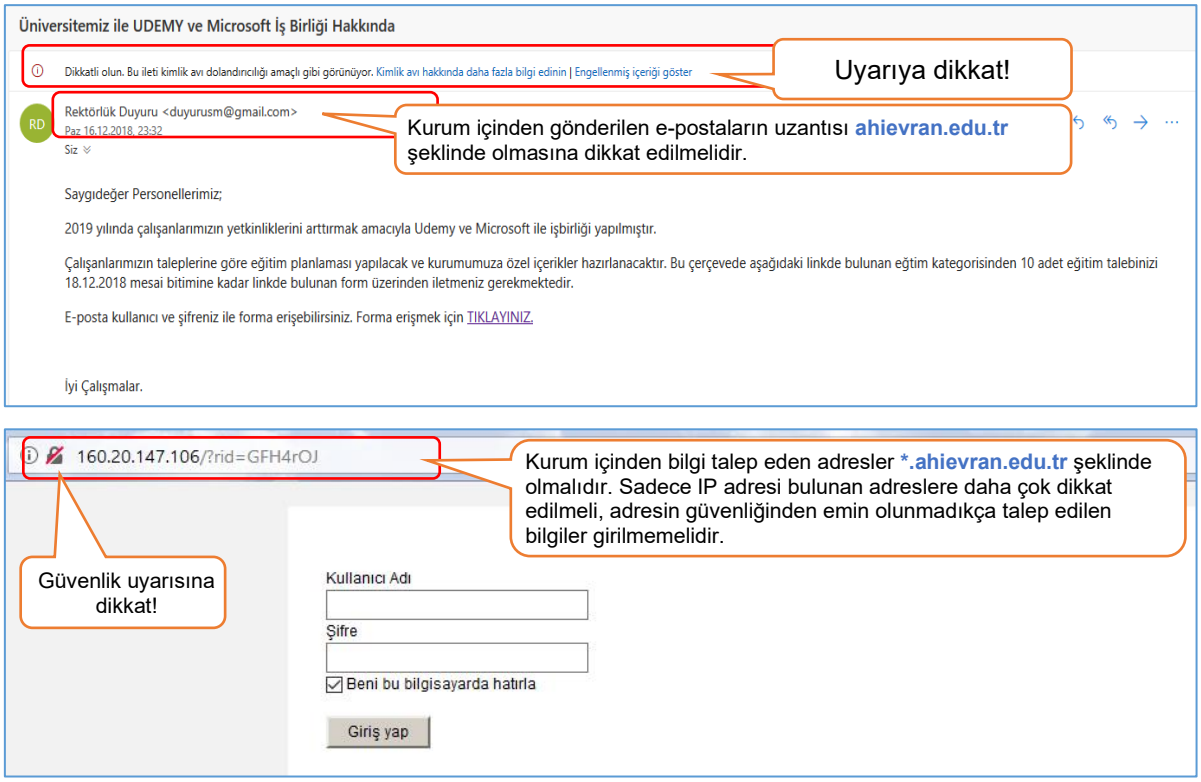
2.25. Peer-to-peer (P2P – noktadan noktaya) dosya paylaşım programları, telif hakları ve lisansları ihlal etmenin yanı sıra, yüksek bant genişliği tüketerek birincil amaçlar için ağ kullanımına kaynak bırakmamaktadır. Bu nedenle, aşağıda sıralanan fakat bunlarla sınırlı olmayan tüm "peer-to-peer" dosya paylaşım araçlarının kullanılması, ağ güvenliğini tehdit edici faaliyetlerde bulunulması (DOS saldırısı, port-network taraması vb.) ve gereksiz dosya indirmeler yapılmaması gerekmektedir. (µTorrent/µTorrent Web, Acquisition, Aimster, Any Send, Ares, Audiogalaxy, BearShare, Bit Che, BitComet, Bitlord, BitTorrent, Cabos, DC++, Deluge, Direct Connect, Dukto, ediaGet, eDonkey2000, eMule, FastTrack, FrostWire, Gnucleus, Gnutella, Halite, iMesh, KaZaA, LimeWire, Mactella, Madster, MFTP, MLDonkey, Morpheus, Napster, NeoModus, OpenNap, Overnet, Phex, PicoTorrent, qBitorrentt, Qtella, RetroShare, Shareaza, Tixati, Tonido Desktop, TorrentRover, Vuze/Azureus, WinMX, XoLoX, vb.)

2.26. Bilgisayar ve yan donanımlarında meydana gelen arızalar öncelikle **destek.ahievran.edu.tr** web adresi üzerinden Başkanlığa bildirilmeli, teknik bilgiye sahip olmayanların bilgisayar kasalarının içini açmak suretiyle müdahalelerde bulunmamaları gerekmektedir.

2.27. Bilgisayar ve yan donanımlarının sıvı maddelerle temas ettirilmemeli, sigara külü, toplu iğne, ataç ve zımba teli gibi yabancı maddelerin masaüstü ve dizüstü bilgisayarların klavyelerine ve özellikle de yazıcı, tarayıcı ve fotokopi cihazlarının içine kaçırılmamalı, cihazların kendi adaptörlerinin dışındaki adaptörler kullanılmamalıdır. Bunlardan doğacak hasarlardan kullanıcılar sorumludur.

2.28. Yazıcı ve fotokopi cihazlarında kullanılacak kâğıtlar 80 gramın altında olmamalı, kâğıtların buruşuk, kenarları yırtık veya kıvrık, zımba teli veya toplu iğne takılı olmamalıdır.
2.29. Kötü niyetli kişilerin bilgisayarları ele geçirmeye çalışabileceği dikkate alınarak, mesai bitiminde (zorunlu haller dışında) kullanıcılar bilgisayarlarını kapatmalıdır.
2.30. Bilgisayarlar, güç/power düğmesinden değil, "***Başlat➔Bilgisayarı Kapat*** veya ***Alt+F4 Bilgisayarı Kapat***" menüsünden kapatılmalıdır.
2.31. Kesintisiz güç kaynağı (UPS) prizlerine bilgisayar, monitör ve dahili telefonlar bağlanmalı, bunların dışında herhangi bir cihaz bağlanmamalıdır. (Elektrikli ısıtıcı ve su ısıtıcısı, lazer yazıcı, elektrikli süpürge vb.)
2.32. Kablo ve kablo kanallarının üzerlerine hiçbir şey konulmamalı, kanallara zarar verebilecek soba, elektrikli ısıtıcı gibi aletler kanallara yaklaştırılmamalı, bina temizliği yapılırken kablo kanallarına su gitmesi önlenmeli, temizlenmeleri gerekiyorsa sadece hafif nemli bezle silinmelidir.
2.33. Microsoft firması ile Windows ve ofis programları için lisans anlaşması yapılmış olup, bilgisayarlara lisanslı Windows işletim sistemi ile ofis programları kurulmalı, lisanssız olan bilgisayarlar destek.ahievran.edu.tr web adresinden Başkanlığa bildirilmelidir. Başkanlığın bilgisi dışında Bilgisayarlara kurulan programlardan kullanıcılarının kendilerinin sorumlu olduğu bilinmeli, lisanslı olmayan programlar bilgisayarlara yüklenmemelidir.
2.34. Ağ ortamında çalışan bilgisayarlar için IP adresleri belirlenerek kayıt altına alınmıştır. Bu nedenle kullanıcılar hiçbir suretle bu IP adreslerini değiştirmemeli, değişmesi gereken veya yeni Ethernet kartı takılması gereken durumlarda Başkanlığa haber verilmelidir.
2.35. Kurumsal ağ ve e-posta kullanılarak, kitlesel e-posta gönderilmesi (mass mailing, mail bombing, spam) ve üçüncü şahısların göndermesine olanak sağlanmamalı, sağlanması durumunda ortaya çıkacak olan her türlü hukukî sorumluluğun kullanıcıya ait olacağı bilinmelidir.
2.36. Kullanıcıların, bilişim cihazlarında (masaüstü, dizüstü bilgisayarlar, tablet, telefon vb.) tutulan kurum bilgilerinin korunmasından sorumlu oldukları bilinmelidir.
2.37. Güvenlik amacıyla yerleştirilen kameralara zarar verilmemeli, açılarıyla oynanmamalı ve görüntüyü engelleyecek şekilde önü kapatılmamalıdır.
2.38. Başkanlık tarafından Üniversitemiz yerleşkelerinde kurulan kablosuz ağ erişim cihazlarının yerleri değiştirilmemeli, Başkanlığın bilgisi ve izni olmadan yeni kablosuz ağ erişim cihazı kurulmamalı, kurulan kablosuz ağ cihazları (Access Point, Router/Yönlendirici, kablolu hattı kablosuz hatta çeviren Wifi cihazları vb.) kaldırılmalıdır.
2.39. Binalara ve özellikle bilgisayar laboratuvarına yerleştirilen network cihazlarının (Switch) enerjileri kesilmemeli, cihazlar kapatılmamalı, kabloları ile oynanmamalı, Başkanlığın izni ve bilgisi olmadan cihazlara hiçbir şekilde müdahale edilmemelidir.
2.40. Uzaktan erişim ancak sınırlı olarak sağlanır ve uzaktan erişimle ilgili kullanıcılar resmi olarak Başkanlığa başvuruda bulunurlar. Kurumun ağına uzaktan bağlantı yetkisi verilen personel, bağlantı esnasında aynı anda başka bir ağa bağlı olmadığını kontrol etmelidir.
2.41. Uzaktan erişim ile kurum ağına bağlanan kullanıcılar, yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahiptir.
2.42. Kurum ağına uzaktan erişecek olan personel, kullandığı bilişim cihazlarının işletim sistemi ve antivirüs yazılımının güncel olmasından sorumludur.
2.43. Kullanıcıların e-posta adresine gelen ve özellikle sosyal mühendislik çalışmaları kapsamında kendilerinden bilgi talep eden e-postalara dikkat edilerek, e-postanın nereden gönderildiğine bakılmalı, şüpheli e-postalar açılmamalı, e-posta içindeki linkler tıklanmamalıdır. Gerekli

görülmesi halinde e-posta açılmadan e-postayı gönderen birim veya şahıstan teyit alınmalı, e-postaların virüslü olabileceği unutulmamalıdır. Şüpheli e-postanın bir örneği aşağıda yer almaktadır.



3. Sosyal Medya Kullanımı

3.1. Sosyal Medya kişisel bloglar, web siteleri, Facebook, Twitter, Instagram, LinkedIn, YouTube ve buna benzer tüm sosyal paylaşım alanlarını kapsar.

3.2. Sosyal medya, paylaşımların hızlı ve kontrolsüz yapılabildiği bir alandır. Özellikle kurumdan hizmet almış tüm özel kişilikleri tüzel kişilikleri ve kurum çalışanlarını ilgilendiren sosyal medya paylaşımları, ilgili kişi ve kurumların bilgisi ve izni olmaksızın yapılamaz.

3.3. Çalışanlar kurum adını içeren ya da kurumla ilişkilendirilebilecek sosyal medya kullanımlarında; kuruma ait hiçbir gizli/özel bilgiyi, onaylanmamış gelişmeyi, müziği, videoyu, yazıları ve fotoğrafları kurumun yazılı izin olmadan üçüncü kişilerle paylaşamaz.

3.4. Sosyal medyada Kırşehir Ahi Evran Üniversitesi adıyla açılan her sayfa/hesap Kırşehir Ahi Evran Üniversitesi resmi alanı gibi düşünebilir ve paylaşılan tüm içerik kurum ile bağdaştırabilir. Yanlış bir marka algısı yaratmamak adına çalışanlar kurum ismi ve logosunu kullanarak sayfa/hesap oluşturulamaz.

3.5. Kurum bünyesindeki kişi, departman toplantı içerik, detay ve mekânları sosyal medyada işaretlenmez; örneğin Instagram, FourSquare, Twitter ve Facebook'ta "Biz VVV otelde, XXXX takımıyla, ZZZ amaçlı toplantı için bulunuyoruz" gibi paylaşımlarda bulunulmaz.

3.6. Sosyal medyada kurumla ilgili gizlilik, güvenlik ve rekabet açısından risk oluşturabilecek uygulamalar kullanılamaz.

3.7. Çalışanlar sosyal medyayı kullanarak öğrencileri, tedarikçileri, çalışanları veya diğer paydaşları aşağılayamaz, rakipler hakkında yanlış veya kanıtlanmamış beyanlarda bulunamaz.

3.8. Çalışanın kurum içindeki görevi özellikle bu tür görüşleri beyan etmek değilse, çevrim içinde ifade edilen görüş ve fikirlerin aynı zamanda kurumun görüşlerini temsil ettiği izlenimini vermediğinden emin olunur.

3.9. Kurum bilişim kaynakları kullanılarak yazılan elektronik yazılar dahi kuruma atfedilebilir. Bu nedenle, kurum tarafından sağlanan bilişim sistemlerini kullanarak iletişim yazıları yazarken özellikle dikkat edilir.

3.10. Sosyal medyada fikirlerin özgürce ifade edilme sürecinde sergilenecek her türlü davranış, temsil edilen kurumun imajını zedeleyebilir. Bu durumdan özellikle kaçınılır.

3.11. Sosyal medyada kullanılan kelimelere ve dile dikkat edilir; ayrımcı, rahatsız edici, ırkçı, cinsel, etnik, dini ya da fiziksel saldırı ve aşağılama niteliğinde ifadeler kullanılmaz, paylaşılmaz ve bu tür durumlara aracı olunmaz.