BAHÇEŞEHİR ÜNİVERSİTESİ SENATOSUNUN 24.11.2022 TARİH VE 2022/26/04 SAYILI KARAR ÖRNEĞİDİR.

KARAR: 2022/26/04

Üniversitemizin Bilgi ve İletişim Güvenliğine ilişkin politikalarının belirlenmesi konusu görüşüldü.

Görüşmeler sonunda; Üniversitemizin kurum vizyonu doğrultusunda, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Uyum Rehberi ve TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standardı çerçevesinde bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamayı amaçlayan ve Üniversitemizde bulunan ve Üniversitenin sağladığı tüm bilgi varlıklarını kapsayan politikaların aşağıda belirtildiği gibi olmasına oy birliği ile karar verildi.

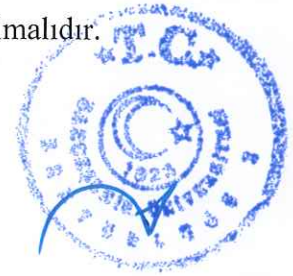
1. Bilgi ve İletişim Güvenliği Politikası

- Bahçeşehir Üniversitesi'nin vizyonu, misyonu ve kurumsal politikaları doğrultusunda eğitim-öğretim, araştırma-geliştirme ve hizmet süreçlerimizin kalitesini sürekli iyileştirerek, öğrencilerimize ve tüm paydaşlarımıza sürekli gelişen değer katmak amacıyla hazırlanan bilgi ve iletişim güvenliği hedeflerini ve faaliyetlerini belirleyerek BGYS (Bilgi Güvenliği Yönetim Sistemi) için yürütülecek çalışmaları planlanması, uygulanması, kontrol edilmesi ve sistemin sürekli olarak iyileştirilmesi sağlanmalıdır.
- Yürütülen faaliyetlerin mevzuat, sözleşme, standart ve iş gereksinimlerini nasıl karşıladığı tanımlanmalıdır.
- Kişisel Verilerin Korunması Kanunu (KVKK) gereksinimlerini nasıl karşıladığı tanımlanmalıdır.
- Bünyesinde kurulu olan diğer yönetim sistemleri ile BGYS çalışmalarının bütünleşik olarak yürütülmesi sağlanmalıdır.
- BGYS kapsamı çerçevesinde görev, rol ve sorumluluklar ile gerekli kaynakların belirlenmesi sağlanmalıdır.
- Bilgi ve iletişim güvenliğini yönetmek için mevcut ve potansiyel risklerin tanımlanması, değerlendirilmesi ve uygun risk işleme seçeneklerinin devreye alınması sağlanmalıdır.
- İş sürekliliği planlamalarının yapılması, bu planların uygulanması ve sürecin sürekli iyileştirilmesi sağlanmalıdır.
- Bilgi ve iletişim güvenliği konusundaki güncel teknolojilerin ve yeniliklerin takip edilmesi, çözümler geliştirilmesi sağlanmalıdır.

- Tüm paydaşların bilgi ve iletişim güvenliği ile ilgili belirlenen hususlara uyması için gerekli önlemlerin alınması sağlanmalıdır.
- İnternet ortamında oluşturulan gezinti verilerine bilimsel amaçlı analiz ve kullanımlar için erişim engellenmemelidir.
- Bu politikanın duyurulması, erişilebilir olması, farkındalığının oluşması ve uygulanması sağlanmalıdır.
- Bu politikanın ihlali durumunda ilgili süreçlerin başlatılması ve takip edilmesi sağlanmalıdır.

2. Ağ Yönetim Politikası

- BAU'nun tahsis ettiği bilgisayarlarda kurumsal antivirüs yazılım programının olması sağlanmalıdır.
- IP adreslerinin denetimi ve uygun olmayanların IP adreslerinin engellenmesi BİDB tarafından sağlanmalıdır.
- Aktif cihazların konum ve güvenliği, gözlenmesi, yönetilmesi ve kontrolü MAM ve MDM kullanılarak sağlanmalıdır.
- Tedarikin yeni yapıldığı veya ağa yeni bağlanacak olan donanımların BİDB tarafından varlık envanterine kaydı yapılmalıdır.
- Kaydı yeni yapılan envanterin zimmet ve takibinden BİDB sorumludur.
- Ağ donanımları BİDB yöneticisi tarafından onaylanmalıdır.
- Güvenilir ağlar arasında kurulan bağlantılarda hassas veriler şifrelenmelidir.
- Kurum iç ağa bağlantı kontrol edilerek yalnızca yetkilendirilmiş cihaz ve kişilerin bağlanması sağlanmalıdır.
- Kullanılan internet tarayıcılarının (Chrome, Firefox, Internet Explorer vb.) güvenlik ayarları yapılarak virüs bulaşma olasılığı engellenmelidir.
- Yetkilendirilmemiş kullanıcının ağ üzerinde erişebileceği servisler VLAN vb. kullanılarak sınırlandırılmalıdır.
- İçerik filtreleme sistemi kullanılmalıdır.
- Ağdaki kullanıcıların BİDB tarafından belirtilen durumlar dışında dış servis sağlayıcı bağlantısı veya dış ağlar ile herhangi bir iletişim kurmaması sağlanmalıdır.
- BİDB tarafından güvenlikle ilgili konuların dağılımı ve raporlaması sağlanmalıdır.
- Ağlarda paylaşım güçlü şifreler kullanılarak ve ağ erişimi düzenlenerek yapılmalıdır.
- İnternet kullanımı ve ağ trafiği BİDB tarafından izlenmelidir.
- Güvenlik duvarı (Firewall) ile içerik denetim ve erişimi yapılmalıdır.



- Kablosuz ağlar parola politikasına uygun olarak şifrelenmelidir.
- Misafir olarak ağa katılım sağlamak isteyen kullanıcılar BAU misafir ağına erişmelidir.
- Kullanılan ve olası bir erişim durumunda kullanılacak olan portların güvenliği sağlanmalıdır.
- Ağ ve sistem sürekliliğinin sağlanması için gerekli kontrol/protokoller uygulanmalıdır.

3. Erişim Kontrol Politikası

- BAU bilgi sistemlerine erişimde, kaynaklara erişim minimum tutularak gerekli yetkilendirmeler yapılmalıdır.
- BAU ile ilişiği kesilen kullanıcıların hesaplarının erişim bilgileri talep edilmesi durumunda silinmesi öncesinde ilgili birim yöneticisi ile paylaşılmalıdır.
- BAU ile ilişiği kesilen ya da işe yeni başlayan kişilerin bilgisi BİDB'ye İKDB tarafından bildirilmelidir. Bu kişilerin yetkilendirilmesinin kaldırılması, hesaplarının silinmesi veya otomatik olarak hesap açılması sağlanmalıdır, bu süreç periyodik olarak kontrol edilmelidir.
- Kullanıcıların yaptıkları işlemlerin ve oturum hareketlerinin kaydı tutulmalı, 6 ay süreyle saklanmalıdır.
- BAU bilgi varlığını korumak amacıyla, tüm kullanıcılara yalnızca ihtiyaç duydukları erişim alanı sağlanmalı ve yetkilendirme düzeyi minimum seviyede tutulmalıdır.
- Kullanıcı hesapları kişiye özel ve tek olmalıdır.
- Tüm kullanıcı hesap parolaları, BAU parola politikasına uygun olmalıdır.
- Kullanıcı hesapları Kullanıcı Hesapları Politikasına (BAU-BİDB-PL-009) uygun olarak oluşturulmalıdır.
- Öğrencilerin, Öğrenci İşlerinde, öğrenci bilgi sistemine kaydı yapıldığı zaman diğer tüm sistemlerde de kaydının otomatik olarak tanımlanması sağlanmalıdır.
- Mezun olmuş, kaydını sildirmiş öğrencinin hesabı tamamen ilişkisi kesildikten 3 ay sonra otomatik kapatılmalıdır.
- Erişim yetkileri rollere göre değişiklik göstermelidir.
- Yetkilendirmeler ve bu yetkilendirme dahilindeki erişim hakları 6 ayda bir kontrol edilmeli ve düzenlenmelidir.
- Uzaktan erişim sağlayacak kullanıcılarda, uygun kimlik doğrulama metotlarının kullanılması sağlanmalıdır.
- Kullanıcılar için BAU standartları çerçevesinde disk kotaları (5TB) belirlenmelidir.

- Kullanıcı rolleri ve erişim yetkilerini açıklayan matrisin güncelliği BİDB tarafından sağlanmalıdır.

4. Ağ Kullanım Politikası

4.1. Genel internet hizmeti kullanım kuralları

- Kar ve şahsi kazanç amaçlarıyla ağ kullanımı yapılmamalıdır.
- BİDB Sistem ve Ağ Yönetimi sorumluları haricinde, BAU dışındaki kişi ve bilgisayarlar tarafından BAU ağ kaynakları kullanılmamalıdır. Bunu sağlayan her türlü faaliyet (DHCP, DNS, Proxy, Relay, NAT vb.) yasaktır.
- Film, lisanssız yazılım gibi dosya paylaşım (peer-to-peer) programları yüksek bant genişliğinde olup ağ trafiğinde yavaşlamaya neden olması ve telif haklarını ihlal etmesi nedeniyle kullanılmamalıdır.
- Kullanıcıların kişisel güvenliğini tehdit edebilecek faaliyetlerde bulunulmamalıdır (ağ trafiğinin dinlenmesi vb.).
- Kullanıcıların kişisel bilgilerinin güvenliğini tehdit eden aktif cihazlar (access point, hub, modem vb.) BİDB yönetim sorumlularının bilgisi dahili dışında yerel ağlarda kullanılmamalıdır.
- Ağ hizmetini sağlayan donanımlara (kablolar, prizler vb.) yalnızca BİDB yönetim sorumluları tarafından müdahale sağlanmalıdır.

4.2. Kablosuz Ağ

- BİDB tarafından BAU genelinde akademik, idari, öğrenci ve misafirlerin kullanımı için kablosuz ağ hizmeti sunulmalıdır.
- Akademik, idari personel göreve başladığında verilmiş olan hesap bilgileriyle bağlanmalıdır.
- Öğrenciler BAU'ya kayıt yaptırdıklarında verilen UMIS hesap bilgileriyle kablosuz ağa bağlanmalıdır.
- Misafirler GUEST ağına bağlantı kurup sistem yönlendirmesi sonrasında hesap açıp ilgili ağa bağlanmalıdır.
- Kablosuz ağ üzerindeki kişisel kullanımlar hiçbir zaman diğer kullanıcıların ağ erişim gereksinimlerini yerine getirmelerine engel olmamalıdır.
- Kablosuz ağ bağlantısı kullanarak servis veren (web hosting servisi, e-posta servisi vb.) sunucu nitelikli bilgisayarlar ve cihazlar bulundurulmamalıdır.

4.3. Kablolu Ağ

- BİDB tarafından BAU genelinde akademik, idari, personel ve öğrencilerin kullanımı için kablolu ağ hizmeti sunulmalıdır. Kablolu ağı kullanacak cihazlar domainde olmalıdır.
- Kampüsler arasındaki bağlantı fiber kablolarla noktadan noktaya metro Ethernet devreleri ile yedeklilik ise radyo link gibi çözümlerle sağlanmalıdır.
- Kablolu ağ üzerindeki kişisel kullanımlar hiçbir zaman diğer kullanıcıların ağ erişim gereksinimlerini yerine getirmelerine engel olmamalıdır.
- Dışarıdan gelen kullanıcılar kablolu ağ bağlantısı kullanarak servis veren (web hosting servisi, e-posta servisi vb.) sunucu nitelikli bilgisayarlar ve cihazlar kullanmamalıdır.
- Öğrenciler UMIS hesap bilgileriyle kablolu ağda bulunan ortak alan ve bilgisayar laboratuvarlarındaki masaüstü bilgisayarları kullanmalıdır.
- Öğrenciler kişisel bilgisayarlarını kablolu ağ kullanımında etki alanı ve port güvenlik kuralları nedeniyle kullanmamalıdır.

5. Uzaktan Erişim Politikası

- BİDB tüm BAU çalışanlarına ve öğrencilerine uzaktan erişim yapabilecekleri bir altyapı hizmeti vermelidir.
- Uzaktan kurum içi kaynaklara erişimin minimum düzeyde yetkilendirmelerle, süre kısıtlamasına tabi tutularak ve parola politikasına uygun bir şekilde olması sağlanmalıdır.
- Kurum içi kaynaklara internet ortamından yetkisiz erişim engellenmelidir.
- Kurum içi kaynaklara internet üzerinden uzaktan erişimin sağlanmasının gerekli olduğu durumlarda, veri bütünlüğünün ve gizliliğinin korunması için VPN teknolojileri ile çok faktörlü kimlik doğrulama kullanılmalıdır.
- Uzaktan erişim yetkisine sahip olan kullanıcılar bağlantı bilgilerini kimse ile paylaşmamalıdır.
- Uzaktan erişim sağlayan kişiler kuruma ait bilgilerin ekran çıktısını almamalıdır.
- Kullanıcıların aynı anda birden fazla oturum açması engellenmelidir.
- Uzaktan erişim için cihazlar antivirüs yazılımı, domain bağlantısı gibi güvenlik önlemlerine sahip olmalıdır.
- İlişiği kesilen yetkili erişim sağlayan kişilerin BİDB'ye İKDB tarafından iletilerek bu kişilerin erişim yetkisinin kaldırılması sağlanmalıdır.
- Uzaktan erişim için kullanılan parolaların 6 ayda bir yenilenmesi sağlanmalıdır.

- Uzaktan erişim yetkileri 3 ayda bir kontrol edilerek gerekli olmayan hesapların erişim yetkisi kaldırılmalıdır.
- Kurum, güvenlik önlemlerini tehdit eden ve gerekli gördüğü durumlarda uzaktan erişim bağlantısını engelleme yetkisine sahip olmalıdır.
- Uzaktan erişim esnasında yapılan işlemler ve oturum açma- oturum kapatma hareketleri kayıt altında tutularak bu hareketlerin gözlem ve takibi yapılmalıdır.

6. Uzaktan Çalışma Politikası

- Uzaktan çalışan kişilerin yaptığı işlerin niteliklerine göre iş sağlığı ve güvenliği önlemlerinin alınması ve çalışanın sağlık gözetimi sağlanmalıdır.
- İş sağlığı ve güvenliği ile ilgili çalışanlar bilgilendirilmelidir ve gerekli eğitim verilmelidir.
- İş ile ilgili sağlanan ekipmanın kullanımıyla ilgili iş sağlığı ve güvenliği tedbirleri alınmalıdır.
- Uzaktan çalışmanın zorunlu olduğu durumlarda kullanılacak malzemeler kurum tarafından sağlanmalıdır.
- Kurum tarafından sağlanan malzemelerin listesi ve veriliş tarihi kayıt altına alınmalıdır.
- İş takibi aktif olarak elektronik posta akışı, internet üzerinden toplantı düzenlenmesi ve telefon görüşmeleri ile yapılmalıdır.
- Uzaktan çalışmada yeni çalışanın oryantasyonu İKDB tarafından sağlanmalıdır.
- Uzaktan çalışmada çalışanın değerlendirilmesi, klavyede yazılanların denetlenmesi, internet aktivitesinin kaydedilmesi, ekran görüntüsünün alınması, cihazlardaki kameraların kullanılması, hangi personelin hangi dosyaya ne zaman girdiğinin belirlenmesi, GPS tekniğiyle çalışanın lokasyonunun tespit edilmesi, bilgisayarın boşta kaldığı zamanın veya bir uygulamanın/programın ne kadar süreyle açık kaldığının ölçümü yoluyla sağlanmalıdır.
- Uzaktan çalışmada kullanılan kablosuz ağlar parola politikasına göre şifrelenmelidir.
- Kablosuz ağ bağlantısı kullanarak servis veren (web hosting servisi, e-posta servisi vb.) sunucu nitelikli bilgisayarlar ve cihazlar uzaktan çalışmada kullanılmamalıdır.
- Uzaktan çalışma ortamında yetkilendirme ve kısıtlama yapılarak, verilerin güvenliği sağlanmalı ve yetkisiz erişim engellenmelidir.
- Uzaktan çalışmanın sona ermesi durumunda yetki ve erişimin iptali ve kullanılan teçhizatın iadesi sağlanmalıdır.

- Uzaktan çalışmada kullanılan cihazlarda güvenlik duvarı ve güncel antivirüs programları kullanılarak güvenlik önlemleri alınmalıdır.
- Uzaktan çalışmada kurum kaynaklarına VPN ve çok faktörlü kimlik doğrulama ile erişilmelidir.
- Kurumun tahsis ettiği cihazın fiziksel güvenliği sağlanmalıdır. Kişi seyahat ediyorsa yanında taşımalı, bavula koymamalıdır. Cihazlar, her zaman şifreli olarak kullanılmalıdır.
- Kurumun tahsis ettiği cihaz yerine kendi kişisel cihazını kullanan kişiler, kurum ile ilgili işlerdeki fikri mülkiyet haklarının tümünün Bahçeşehir Üniversitesi'ne ait olduğu konusunda bilgilendirilmelidir.
- Verilerin korunması için uzaktan çalışma ile ilgili güvenlik önlemleri alınmalı ve tüm çalışanlar bu konuda bilgilendirilmelidir.
- Elektronik posta akışı kurumsal e-posta üzerinden olmalıdır.
- Gönderilen veriler gerekmedikçe cihaza kaydedilmemeli, yazdırılmamalı, kopyalanmamalı ve paylaşılmamalıdır.
- Kişisel online görüşmeler kaydedilmemelidir.
- Oturum hareketleri (login/logout) izlenmelidir.

7. Parola Politikası

7.1. Parola Oluşturma Kuralları (Genel)

- Parolalar en az 8 karakter uzunluğunda olmalıdır.
- En az 1 büyük harf, 1 küçük harf, 1 rakam ve 1 özel karakter (örneğin; !@ #+|~-=\`$%^&>*()_{}[]:";'</) içermelidir.
- İçeriğinde, kişisel bilgiler bulunmamalıdır (örneğin; kullanıcı adı, aile bireylerinin isimleri, doğum tarihleri, telefon numarası veya adres bilgileri gibi).
- Kelime veya rakam dizileri kullanılmamalıdır (örneğin; aaabbb, qwerty, zyxwvuts, 12345678, 123321 vb).

7.2. Parola Oluşturma Kuralları (Sistem)

- Tüm kullanıcı hesaplarına ait bir parola olmalıdır.
- Yeni kullanıcı hesaplarına ait parolalar ilk kez giriş yapılırken kullanıcı tarafından kurallara uygun olarak tanımlanmalıdır.
- Başarısız parola denemeleri üst üste 3 kere ile sınırlandırılmalıdır.
- Kullanıcının aynı parola ile 4'ten fazla cihaz üzerinden sisteme giriş yapmasına izin verilmemelidir.
- Yazılan parolanın ekranda maskelenerek görünmesi sağlanmalıdır.

- Kullanıcı parolaları, saklandıkları ortamlarda, geri dönüşü mümkün olmayan bir şekilde bozularak korunmalı, bu sayede en yetkili kişilerin bile kullanıcı parolasını görmesi engellenmelidir.
- Bilgi kaynaklarına başarılı ve başarısız erişimlerin tarih, zaman ve erişilen kaynağın detayı ile ilgili bilgilerin kaydı 5651 sayılı kanun gereğince tutulmalıdır.
- Kullanıcıların kimlik doğrulaması yaparak oturum açtıkları sistemlerin başından ayrıldıklarında (sisteme parola ile giriş yapıldıktan sonra sistemin açık bırakılması halinde) en geç 10 dakika sonra otomatik olarak kapanması (sistemin kilitlenmesi) sağlanmalıdır.
- Halka açık veya paylaşılan ağlardan iletilen kimlik bilgileri güçlü şifreleme metotları ile (SSL) korunmalıdır.
- Başkaları tarafından öğrenildiğinden şüphelenilen parolalar hemen değiştirilmelidir.
- Kullanıcıların parolalarını 6 ay içinde kullanmamaları durumunda ilgili hesap dondurulmalıdır.
- Kritik kaynaklara 2 faktörlü şifre ile erişilebilmeli, bu sayede sistemde güvenlik ihlali oluşturulmasına izin verilmemelidir.

7.3. Parola Kullanım Kuralları

- Kullanıcı parolaları en geç 6 ayda bir değiştirilmelidir.
- Yönetici parolaları 3 ayda bir değiştirilmelidir.
- Her yeni parola için, son kullanılan 3 paroladan farklı bir parola kullanılmalıdır.
- Parola değiştirme işlemi sırasında parola onayı (tekrarı) istenerek parolanın bilinmeyen bir değer ile değiştirilmesi engellenmelidir.
- Parolalar hiç kimse ile paylaşılmamalıdır.
- Parolaların klavyeden girilmesi sırasında dikkatli olunmalı ve çevredeki kişilerin göremeyeceği şekilde girilmelidir.
- Aynı parola ve SSO servisi ile tüm hizmetlere erişim sağlanmalıdır.
- Parolalar, ilave bir şifreleme metodu kullanılmadan hatırlamak amacıyla kaydedilmemelidir (kağıt, bilgisayardaki bir dosya, cep telefonu gibi ortamlarda saklanmamalıdır).
- İnternet tarayıcılarında (Internet Explorer, Chrome, Firefox vb.) "Parolayı hatırla" seçeneği kişisel bilgisayarlar dışında kullanılmamalıdır ve kişisel bilgisayarlarda bir güvenlik açığı olduğu göz önünde bulundurulmalıdır.

7.4. Parolanın Unutulması

- Bütün sistemler üzerinde, kullanıcıların parolasını unutma ihtimaline karşı öğrenciler için UMIS üzerinden SMS doğrulaması ile şifre güncellenmelidir. İdari ve akademik çalışanlar için e-posta hesabı ve GSM numarası kurtarma hesabı olarak kullanılmalıdır.
- UMIS'de parola unutulması durumunda çalışanlar için; kullanıcı adı ve T.C. kimlik numarası ile, öğrenciler için; okul numarası, doğum tarihi ve kullanıcı adı ile şifre BSVA tarafından güncellenmelidir.
- EBYS'de parola unutulması durumunda kullanıcı adı ve e-posta hesabı ile Yönetim Destek ve Bilgi Sistemleri Direktörlüğü tarafından şifre güncellenmelidir. Bu çözüm, kullanıcıların kişisel doğrulamasını yapmak amacıyla kişilerin gizli soruları ve özlük bilgilerinden oluşan en az iki soru içermelidir.
- Hiçbir kullanıcının parolası güvenlik yöneticisinin onayı olmadan diğer yetkili kişiler tarafından değiştirilmemelidir.
- Bütün parola değiştirme ve güncelleme işlemleri, kullanıcı eski ve yeni parolanın bozulmuş hali, değiştiren kişi (kullanıcıdan farklıysa), değiştirme saati ve tarihi kayıt altına alınmalı ve 2 faktörlü şifre ile korunmalıdır.
- Parola güvenliği adına Parola Politikası (BAU/BİDB/PL-007) tüm personele duyurulmalı, gerekli destek sağlanmalıdır.

8. E-Posta Kullanım Politikası

- Her kullanıcının BAU'ya ait Microsoft 365 altyapısında çalışan @bahcesehir.edu.tr ve @bau.edu.tr alan adlarında sadece bir adet e-posta hesabı bulunmalıdır.
- Aynı ad soyada sahip kişilere verilecek e-posta hesapları ilk kullanıcıya "ad.soyad" olarak, sonrakilere "ad.soyad#" (#=1,2,3,…,n) şeklinde sıralanarak verilmelidir.
- Öğrencilerin kaydı yapıldıktan sonra tüm hesapları otomatik olarak açılır, akademisyen ve çalışanların tüm hesapları BİDB tarafından açılmalıdır.
- Kurum personeline ad.soyad@bau.edu.tr (varsa ikinci adı ve soyadı dahil) e-posta adresi tahsis edilmelidir.
- BAU öğrencilerine ad.soyad@bahcesehir.edu.tr (varsa ikinci adı ve soyadı dahil) e-posta adresi tahsis edilmelidir.
- E-posta kullanıcı adı ve parolalar aynı zamanda kablosuz ağ altyapısında kullanılmalıdır.
- Sadece kurum tarafından onaylı e-posta istemcisi eklentileri kullanılmalıdır.

- Kullanıcılar parolalarını Parola Politikası (BAU/BİDB/PL-007) doğrultusunda belirlemeli ve kullanmalıdır.
- Kullanıcılar bilerek veya bilmeyerek (zararlı yazılımların bulaşması neticesinde) istenmeyen iletiler (SPAM) göndermemelidir.
- E-posta hesaplarının güvenliğinden öncelikle kullanıcıların kendileri sorumludur.
- BAU e-posta hizmeti bünyesinde, BAU kullanıcılarının e-posta grupları oluşturulmasını isteme ve e-posta gruplarını kullanma olanağı bulunmalıdır.
- BAU ile ilişiği kesilen öğrencilerin e-posta adresleri mezuniyet tarihini takip eden eğitim yılında sistemden silinmelidir.
- İKDB biriminden alınan liste doğrultusunda, emeklilik haricinde BAU ile ilişiği kesilmiş (istifa, nakil tayin, görev süresi sona erme vb.) kullanıcıların e-posta adresleri 1 ay sonra sistemden silinmelidir.
- Toplu e-posta gönderimi için genel duyuru istekleri Genel Sekreterlik, akademik duyuru istekleri Rektörlük ve hem genel hem de akademik duyuru istekleri Kurumsal İletişim tarafından yapılmalıdır.
- E-posta yoluyla dağıtılması gereken içeriklerin, kurum dışı dağıtımı amacıyla servis sağlayıcı portalları kullanılmalıdır.

9. Kullanıcı Hesapları Politikası

9.1. Etki Alanı Hesapları

- İKDB'den gelen atama bilgisine istinaden göreve başlayan akademik, idari personelin domain hesabı "ad.soyad" (varsa ikinci adı ve soyadı dahil) olarak açılmalıdır.
- Aynı ad soyada sahip kişilere verilecek domain hesapları ilk kullanıcıya "ad.soyad" olarak, sonrakilere "ad.soyad#" (#=1,2,3,…,n) şeklinde sıralanarak verilmelidir.
- Hesap adı ve geçici şifre bilgisi, bağlı olduğu akademik veya idari birim sekreterliğine e-posta olarak gönderilmelidir.
- ÖİDB tarafından öğrencilere kayıt sırasında hesapları "ad.soyad" (varsa ikinci adı ve soyadı dahil) olarak açılmalı ve geçici şifre bilgisi belge olarak verilmelidir.
- Akademik ve idari personeller domain hesaplarıyla kablolu ağdaki bilgisayarını açabilmeli, kablosuz ağa bağlanabilmeli ve kampüs dışından elektronik kaynakları kullanabilmelidir.
- Öğrenciler domain hesaplarıyla bilgisayar sınıflarındaki ve ortak alanlardaki bilgisayarları açabilmeli, kablosuz ağa bağlanabilmeli ve kampüs dışından elektronik kaynakları kullanabilmelidir.

- Adı veya soyadı değişen akademik ve idari personelin hesap değişikliği işlemleri İKDB'den gelen bilgiye istinaden yapılmalıdır.
- Adı veya soyadı değişen öğrencilerin hesap değişiklik işlemleri ÖİDB tarafından gönderilen bilgiye göre BİDB tarafından yapılmalıdır.
- Akademik, idari personel ve öğrenciler geçici şifrelerini BİDB'nin parola politikasında belirtildiği gibi değiştirmeli ve kimseyle paylaşmamalıdır.
- Akademik ve idari personel görevden ayrıldığında domain hesabı kapatılmalıdır.
- Öğrencilerin kaydının silinmesi veya mezuniyet işlemlerinin yapılması sonrasında domain hesabı kapatılmalıdır.

9.2. E-posta Hesapları

- İKDB'den gelen atama bilgisine istinaden göreve başlayan akademik, idari personelin e-posta hesabı "ad.soyad" (varsa ikinci adı ve soyadı dahil) olarak Microsoft Office 365 sisteminde açılmalıdır. Örnek: ad.soyad @bau.edu.tr
- İKDB'den gelen atama bilgisine göre akademik ve idari personelin hesap adı ve geçici şifre bilgisi bağlı olduğu akademik ve idari birim sekreterliğine e-posta olarak gönderilmelidir.
- ÖİDB tarafından öğrencilere kayıt sırasında e-posta hesapları "ad.soyad" (varsa ikinci adı ve soyadı dahil) olarak açılmalı ve geçici şifre bilgisi belge olarak verilmelidir.
- Adı ve soyadı değişen akademik ve idari personelin hesap değişiklik işlemleri İKDB'den gelen bilgiye istinaden yapılmalıdır.
- Adı veya soyadı değişen öğrencilerin hesap değişiklik işlemleri ÖİDB tarafından gönderilen bilgiye göre BİDB tarafından yapılmalıdır.
- Bölüm veya birim adı ile açılması istenilen e-posta hesapları isteği, isteği yapan akademik veya idari birimin amir onayıyla açılmalıdır.
- Akademik, idari personel ve öğrenciler geçici şifrelerini BİDB'nin parola politikasında belirtildiği gibi değiştirmeli ve kimseyle paylaşmamalıdır.
- Akademik, idari personel görevden ayrıldıktan 1 ay sonra e-posta hesabı kapatılmalıdır.
- Öğrencilerin kaydının silinmesi veya mezuniyet işlemlerinin yapılması sonrasında e-posta hesabı kapatılmalıdır.
- Öğrenciler mezuniyet işlemi sonrasında Mezunlarla İletişim ve İş Birliği Koordinatörlüğü'ne başvurarak mezun e-posta hesap bilgilerini temin edebilmelidir.
- Sadece mezuniyetin iptal edilmesi durumunda, mezun e-posta hesabı kapatılmalıdır.

9.3. UMIS Hesapları

- UMIS platformu akademik, idari personelin ve mezunların erişimine açık olmalıdır.
- Öğrencinin kesin kayıt işlemi sonrasında kullanıcı hesapları UMIS sisteminde oluşturulmalı ve kullanıcı bilgileri ÖİDB personeli tarafından "Hoş Geldin Mektubu" adı altında bir çıktıyla öğrenciye verilmelidir.
- Akademik personelin işe başlangıcıyla birlikte, UMIS kullanıcı hesabı Akademik Planlama Müdürlüğü tarafından oluşturulmalı ve hesaba ilişkin erişim bilgileri UMIS tarafından kullanıcının kurum e-posta adresine gönderilmelidir.
- İdari personelin işe başlangıcıyla birlikte, UMIS kullanıcı hesabı BSVA birimi tarafından oluşturulmalı ve hesaba ilişkin erişim bilgileri UMIS tarafından kullanıcının kurum e-posta adresine gönderilmelidir.
- Akademik personelin kullanıcı hesabına, başlamış olduğu görev ve birime uygun yetki tanımlaması Akademik Planlama Müdürlüğü tarafından yapılmalıdır. İlgili personelin görev/ birim değişikliği takip edilerek yetkilendirme düzeyi güncellenmelidir.
- İdari personelin kullanıcı hesabına, başlamış olduğu görev ve birime uygun yetki tanımlaması BSVA birimi tarafından yapılmalıdır. İlgili personelin görev/ birim değişikliği takip edilerek yetkilendirme düzeyi güncellenmelidir.
- Akademik personelin işten ayrılmasıyla birlikte kullanıcı hesabı Akademik Planlama Müdürlüğü tarafından kapatılarak sistem erişimi engellenmelidir.
- İdari personelin işten ayrılmasıyla birlikte kullanıcı hesabı BSVA birimi tarafından kapatılarak sistem erişimi engellenmelidir.
- ÖİDB personeli tarafından, öğrencinin kaydının silinmesi veya mezuniyet işlemlerinin yapılması sonrasında sistem erişimi otomatik olarak kapatılmalıdır.
- AKTS Bilgi Paketi, SMS, Apply BAU, Revir, Mezun uygulamalarının tümü UMIS üzerinden yürütülmelidir.
- Mezun olan öğrencilerimiz için kullanıcı hesabı mezuniyet işlemi sonrasında otomatik olarak oluşturulmalıdır. Öğrenciyken kullanılan kullanıcı adı ve şifre, UMIS mezun modülü için de geçerli olmalıdır. Sadece mezuniyetin iptal edilmesi durumunda kullanıcı hesabı erişime kapatılmalıdır.

9.4. EBYS Hesapları

- Kurum içi/dışı yazışma ve form süreçleri web tabanlı elektronik belge yönetim sistemi EBYS tarafından yönetilmelidir.

- Akademik ve idari personelin işe başlangıcıyla birlikte, EBYS kullanıcı hesabı Yönetim Destek ve Bilgi Sistemleri Direktörlüğü tarafından oluşturulmalı ve hesaba ilişkin erişim bilgileri kullanıcının e-posta adresine gönderilmelidir.
- Akademik ve idari personelin kullanıcı hesabına, başlamış olduğu görev ve birime uygun yetki tanımlaması Yönetim Destek ve Bilgi Sistemleri Direktörlüğü tarafından yapılmalıdır. İlgili personelin görev/birim değişikliği takip edilerek yetkilendirme düzeyi güncellenmelidir.
- Akademik ve idari personelin işten ayrılmasıyla birlikte kullanıcı hesabı Yönetim Destek ve Bilgi Sistemleri Direktörlüğü tarafından kapatılarak sistem erişimi engellenmelidir.
- Akademik ve idari personel izin süreci de yine EBYS üzerinden yönetilmelidir.
- E-İmza, EBYS yazışma ve form süreçlerinde kullanılmalıdır. Belirlenmiş görev ve unvanlar doğrultusunda Yönetim Destek ve Bilgi Sistemleri Direktörlüğü tarafından e-imza talep süreci başlatılmalı, kullanıcıya elektronik olarak iletilen form doldurulduktan sonra kargo ile e-imza ilgili kullanıcıya teslim edilmeli ve teslim edilen e-imzanın kurulumu BİDB tarafından yapılmalıdır.

9.5. PARS Hesapları

- Satın alma ve tedarik süreçleri PARS web tabanlı envanter ve kayıt sisteminde yönetilmelidir. Kullanıcıların oluşturulması EBYS üzerinden entegrasyon ile sağlanmalıdır. EBYS'de oluşmuş bir hesap PARS üzerinden otomatik olarak oluşturulabilmeli, güncellenebilmeli ve iptal edilebilmelidir. Kullanıcılar UMIS erişim bilgileri ile PARS sistemine erişebilmelidir.

10. Kimlik Doğrulama ve Yetkilendirme Politikası

- BAU bilgi sistemlerine erişim sağlayacak kullanıcıların, erişim ve yetkileri belirlenmeli ve güncel olarak takibi yapılmalıdır.
- Kullanıcıların hangi sistemleri hangi kimlik doğrulama yöntemi ile kullanacağı belirlenmelidir.
- Kullanıcılara yönelik profiller ve kimlik doğrulama yöntemleri BİDB tarafından tanımlanmalıdır.
- Kullanıcılar parola politikasına uygun olarak şifre oluşturmalı ve şifrelerini kimseyle paylaşmamalıdır.
- BAU'nun sağladığı cihazlara iki faktörlü kimlik doğrulama ile giriş yapılmalıdır.

- İki faktörlü doğrulamada BAU e-postası veya BAU'nun onayladığı mobil cihaz kullanılmalıdır.
- Uzaktan çalışmada iki faktörlü kimlik doğrulama ve VPN kullanılarak uçtan uca veri güvenliği sağlanmalıdır.
- Sistemlere girişlerin kaydı tutulmalı ve olağan dışı bir durum ile karşılaşılırsa gerekli incelemeler yapılmalıdır.
- BAU verilerine erişen tüm sistemler denetlenmeli ve kayıt altına alınmalıdır.
- İKDB tarafından bildirilen, ilişiği kesilen personelin erişim yetkileri kaldırılmalıdır.
- BAU verilerine erişim yetkileri 6 ayda bir güncellenmeli ve denetlenmelidir.

11. Veri Tabanı Denetim Politikası

- Kurum içi veri tabanı yönetiminde, gizlilik, bütünlük ve erişilebilirlik unsurlarına göre muhtemel risklerin tespiti yapılmalıdır.
- Veri tabanının denetiminden BİDB sorumludur.
- Veri tabanı denetimleri periyodik olarak yapılmalı, normal işleyişin dışında bir durum tespit edilirse gerekli incelemeler ve müdahaleler yapılmalıdır.
- Veri tabanı denetimi, Kişisel Verileri Saklama ve İmha Politikasına (BAU/BİDB/PL-013) uygun olmalıdır.
- Veri tabanı yönetim sürecinde personel bazlı görevlendirme yapılarak bu görevlendirmenin denetimi sağlanmalıdır.
- Veri tabanına erişim yetkisi olan kişilere gerekli bilgilendirmeler yapılmalıdır.
- Yetkili kişiler veri tabanına erişirken iki aşamalı doğrulama kullanmalıdır.
- Verilere erişim yetkisi verilen kişilerin oturum hareketleri ve yaptığı işlemler kayıt altına alınmalı ve olağan dışı bir durum tespit edildiğinde gerekli incelemeler yapılmalıdır.
- Veri tabanı üzerinde yapılan değişiklikler (yetkilendirme değişiklikleri, erişim kısıtlamaları, mimari değişiklikler) ve silinen veriler Kişisel Verileri Saklama ve İmha Politikasına (BAU/BİDB/PL-013) uygun olmalıdır.
- Veri tabanlarının sunucu tarafındaki değişiklikler kayıt altına alınıp saklanmalıdır.
- Gerçek izleme yapılarak sistemlerin sürekliliği sağlanmalıdır.
- Veri tabanlarının depolama bölümü için referans değerlerin olduğu bir referans dokümanı hazırlanmalıdır. Bu değerlerin farklılık gösterdiği durumlar için uyarı oluşturulmalı ve bunun düzenli takibi yapılmalıdır.
- Genele açık hale getirilen veri tabanı, uygulama ve simülasyonlarından araştırma ve geliştirme faaliyetleri için faydalanma olanağı sağlanmalıdır.

12. Güvenli Veri Depolama Politikası

- Güvenli veri depolama verinin, yetkisiz erişim, ifşa ve imhadan korunmasını sağlamalıdır.
- Hassas veriler, şifreleme yazılımları ile korunmalıdır.
- Verilerin dijital olarak depolanmasında güncel bir antivirüs programı ve güvenlik duvarı kullanılmalıdır.
- Dijital ortamda depolanan verilerin fiziksel ortamda da yedeklemesi yapılmalıdır.
- Yedeklemeler için bulut ve harici disk kullanılmalıdır.
- Kişisel veriler ile araştırma verileri ayrı depolama alanlarında saklanmalıdır.
- Depolamada şifrelerin oluşturulması ve kullanımı Parola Politikasına (BAU/BİDB/PL-007) uygun olarak yapılmalıdır.

13. Kişisel Veri Saklama ve İmha Politikası

13.1. Kişisel Verilerin Saklanması

- BAU, kişisel verileri hukuka uygun bir şekilde elektronik veya elektronik olmayan ortamlarda saklamalıdır.
- Kişisel verilerin saklandığı elektronik ortamlar; sunucular (etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım vb.), yazılımlar, bilgi ve iletişim güvenliği cihazları, kişisel bilgisayarlar, mobil cihazlar, optik diskler, çıkartılabilir bellekler, yazıcı, tarayıcı ve fotokopi makinesidir.
- Kişisel verilerin saklandığı elektronik olmayan ortamlar; kağıt, manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş rehberi vb.) ve görsel (yazılı, basılı) ortamlardır.
- Kişisel verilerin güvenli bir şekilde saklanması ve gerektiğinde imha edilmesinde gerekli idari ve teknik tedbirler alınarak hukuka aykırı bir durum oluşması önlenmelidir.

13.2. İdari Tedbirler

- Kişisel verilerin bulunduğu ortamlara sadece yetkili kişilerin erişimi sağlanmalıdır.
- Erişim sınırlandırılması, verinin niteliği ve önem derecesine göre BİDB tarafından yapılmalıdır.
- Veri erişimi olan kişilere, 657 sayılı kanun uyarınca, kişisel verilerin hukuka aykırı şekilde erişilmesi ve işlenmesinin engellenmesini sağlamak adına gerekli bilgilendirmeler yapılmalıdır.

- BAU tarafından yürütülen faaliyetlerin gizliliğini korumak adına, çalışanlara gizlilik sözleşmesi imzalatılmalıdır.
- Çalışanlara yönelik bilgi ve iletişim güvenliği eğitimi verilmelidir.
- Kişisel verileri içeren evraklar, elektronik olmayan ortamlarda (kağıt) aktarılıyorsa gizlilik dereceli belge formatında gönderilmelidir.
- Periyodik olarak kurum içi denetimler yapılmalıdır. Bunun sonucunda ortaya çıkan güvenlik açıkları giderilmelidir.
- İlgili çalışana kişisel verilerin güvenliği ve veri gizliliği ile ilgili gerekli bilgilendirme ve eğitim yapılmalıdır.
- Kişisel veri işleme envanteri hazırlanmalıdır.

13.3. Teknik Tedbirler

- Ağ ve uygulama güvenliği sağlanmalıdır.
- BAU bilişim sistemlerinin güvenliğine yönelik zafiyet açıklarının tespiti için yılda 1 defa sızma (penetrasyon) testi yapılmalıdır.
- Özel nitelikli kişisel verilerin aktarılmasında şifreleme yapılmalıdır.
- Açık rıza metni kişi tarafından onaylanmadan, kişinin kişisel verileri işlenmemelidir.
- Bilişim sistemlerinin sürekliliğini engelleyecek riskler ve tehditlerin takibi BİDB tarafından yapılmalıdır.
- Gerekli durumlarda veri maskeleme kullanılmalıdır.
- Kişisel verilerin işlendiği elektronik ortamlarda loglama kullanılmalıdır.
- Erişim loglarının düzenli olarak tutulması sağlanmalıdır.
- Kişisel verilerin yedeklemeleri yapılmalıdır.
- Kişisel verilerin işlendiği ortamlarda parola politikasına (BAU-BİDB-PL-007) uygun güçlü şifrelemeler yapılmalıdır.
- Risk belirlemesi yapılarak kişisel verilerin hukuka aykırı bir şekilde işlenmesine engel olacak tedbirler alınmalıdır.
- Kişisel verilerin bulunduğu alanlara erişimler kısıtlanmalı ve kayıt altına alınmalıdır.
- Yazılımsal ve donanımsal tedbirler alınarak bilgi sistemlerinin ve kişisel verilerin korunması sağlanmalıdır.
- Kurum, imha edilen kişisel verilere tekrar ulaşılmasını engelleyecek tedbirleri almalı ve yetkili kişileri bu konuda uyarmalıdır.
- Kurum internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 256 bit RSA algoritmasıyla şifrelenmelidir.

- Kişisel verinin elektronik ortamda e-posta yolu ile yapılacak her işlemi için kurumsal e-posta hesabı kullanılmalıdır.
- Kişisel veriler, Kanun'a ve ilgili mevzuata uygun bir biçimde amacı dahilinde öngörülen süre kadar saklanmalı ve işlenmelidir.

13.4. Kişisel Verilerin Saklanmasını Gerektiren İşleme Amaçları

- İnsan kaynakları süreçlerinin işletilebilmesi.
- Yasal raporlamaların yapılabilmesi.
- Öğrenci/Mezun işlem süreçlerinin yürütülebilmesi.
- Akademik faaliyet, araştırma geliştirme süreçlerinin yönetilebilmesi.
- Akademik yayın ve bilişim kaynaklarının yönetilebilmesi.
- Yemek, etkinlik süreçlerinin yönetilebilmesi.
- Satın alma süreçlerinin yönetilebilmesi.
- İletişim süreçlerinin yürütülmesi.
- Kurumsal iletişimin sağlanması.
- Üniversite güvenliğinin sağlanması.
- İstatistiksel çalışmaların yapılabilmesi.
- İmzalanan süreç ve protokoller sonucunda iş ve işlemlerin ifa edilebilmesi.
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesinin sağlanabilmesi.
- Telefon/Çağrı merkezi süreçlerinin yönetilebilmesi.
- İleride doğabilecek hukuki anlaşmazlıklarda delil olarak ispat yükümlülüğünün olması.

13.5. Kişisel Veri Saklama ve İmha Süreleri

- Kurul İşlemleri- 10 yıl,
- Kurumu ilgilendiren uyuşmazlık, dava/icra takibi, adli ve idari mercilerle yapılan iletişimlere ilişkin kayıtların saklanması- 10 yıl,
- Sözleşmelerin Hazırlanması- Sözleşmenin bitimine takiben 10 yıl,
- Kurum İletişim Faaliyetlerinin İcrası- Faaliyet bitimini takiben 10 yıl,
- İnsan Kaynakları Süreçlerinin Yürütülmesi- İş ilişkisinin sona ermesinden itibaren 10 yıl,
- Çalışan adayı başvurularının alınması- 1 yıl,
- Masraf ve avans takibinin yapılması- İş ilişkisinin sona ermesinden itibaren 10 yıl,
- İlgili kişi başvurularına ilişkin kayıtların saklanması- 3 yıl,

- Log Kayıt Takip Sistemleri- 10 yıl,
- Donanım ve Yazılım Erişim Süreçlerinin Yürütülmesi- 2 yıl,
- Ziyaretçi ve Toplantı Katılımcılarının Kaydı- Etkinliğin bitmesini takiben 2 yıl,
- Kamera Kayıtları- 3 ay
- Biyometrik veri- çalışma süresince
- Kişisel veri periyodik imha süresi 6 aydır.

13.6. Kişisel Verilerin İmhasını Gerektiren Sebepler

- Kişisel verilerin işlenmesine ilişkin mevzuatın ilgili hükümlerinin değiştirilmesi ve ortadan kaldırılması durumunda imha edilmelidir.
- Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması durumunda imha edilmelidir.
- İlgili kişinin, Kanun'un 11.maddesinde yer alan hakkına göre BAU'ya başvuru yapması durumunda imha edilmelidir.
- Kişinin yaptığı başvuruya gelen ret yanıtının yeterince açıklanmamış olması veya belirtilen süre içinde kişiye bir yanıt verilmemiş olması koşullarında, kişinin başvuruda bulunarak kişisel verilerinin imhasını, anonim hale getirilmesini istemesi ve bu talebin uygun bulunması durumunda imha edilmelidir.
- Kişisel verileri saklamanın amacının bitmiş olup saklama süresini uzatacak haklı herhangi bir gerekçe olmaması durumunda imha edilmelidir.
- Kişisel veriler Kanun'un 5. ve 6. maddesinde belirtilen veri işleme şartlarına dayalı olarak işlenmiş olmasına rağmen, veri işlemenin Kanun'un 4. maddesinde belirtilen genel ilkelere aykırılık teşkil etmesi durumunda imha edilmelidir.
- Kişisel veri işlemenin dayandığı hukuki sebeplerin tümünün ortadan kalkması durumunda imha edilmelidir.
- Kişisel verileri işlemenin ilgili kişinin açık rızasına dayalı olarak gerçekleştirildiği hallerde, ilgili kişinin açık rızasını geri alması ve söz konusu kişisel verileri işlemek için başkaca bir hukuki sebep bulunmaması durumunda imha edilmelidir.
- Kişisel verileri saklama ve işleme amaçları ortadan kalmışsa, kişinin talebiyle 30 gün içinde veriler imha edilmelidir.
- Elektronik ortamda olmayan kağıt üzerindeki veri karartma yoluyla imha edilmelidir.
- Kişisel verileri saklama ve inceleme amaçları ortadan kalkmamışsa imha talebi reddedilebilir. Böyle bir talep ile karşılaşıldığında 30 gün içinde cevap kişiye iletilmelidir.

- İmha talebine konu kişisel veriler üçüncü kişilere aktarılmış ise, üçüncü kişiler de verilerin imhası hakkında bilgilendirilmeli ve en geç otuz gün içerisinde bu kişiler nezdindeki verilerin imhasına ilişkin tüm işlemlerin yerine getirilmesi sağlanmalıdır.
- Kişisel verilerin imhası yetkili kişiler tarafından politika ve prosedürlere uygun olarak yapılmalı ve imha kayıtları en az 3 yıl süre ile saklanmalıdır.

13.7. Kişisel Veri İmha Teknikleri

- Fiziksel ortamda (kağıt) yer alan kişisel verileri karartma ve kağıt kırpma makinesi ile imha edilmelidir.
- Optik/Manyetik medyada yer alan kişisel veriler fiziksel olarak ya da yüksek manyetik alan altında verilerin okunmasını olanaksız hale getirerek imha edilmelidir.
- Elektronik ortamlardaki kişisel veriler üstüne yazarak (wiper yöntemi) imha edilmelidir.

13.8. Kişisel Verileri Anonim Hale Getirme

- Kişisel veriler kime ait olduğu bilinemeyeceği hale dönüştürülerek anonim hale getirilmelidir. Kişisel verilerin anonim hale getirilmesi için kullanılabilecek yöntemler:
  - Genelleştirme
  - Değişkenleri Çıkartma
  - Örnekleme
  - Bölgesel Gizleme
  - Global Kodlama
  - Alt ve üst sınır kodlama
  - Maskeleme

14. Sistem Odası ve Veri Merkezi Güvenliği Politikası

- Sistem odaları kurumun ihtiyaçlarına uygun ve kurumun içinde olmalıdır.
- Isı, nem, su, yangın gibi risk teşkil eden değişkenlerin kontrollü olduğu bir ortam sağlanmalıdır.
- Yedekli bir güç kaynağı sistemi ve haberleşme bağlantılarına sahip olmalıdır.
- Fiziksel erişim kontrol edilmeli ve kamera sistemi ile erişim denetlenmelidir.
- Sistem odası için risk analizi yapılmalı ve raporlanmalıdır.
- Risk değerlendirmesi sonucu veri akışındaki güvenlik ve bütünlüğün sağlanması için riskli görülen veri akışlarında uygun ve güncel kriptografik mekanizmalar (IPSec, SSL/TLS, link seviyesinde şifreleme, HMAC, vb.) kullanılmalıdır.

- Sistem odasının kontrollü olarak bakım ve onarımı yapılmalıdır.
- Sistem odasının kendi sistem bileşenlerini ve başka sistemlerle olan bağlantılarını içeren sistem odası dokümanı hazırlanmalıdır.
- Veri merkezinde bulunan cihaz ve yazılımların ideal çalışması konusunda referans dokümanı hazırlanmalıdır.
- Veri merkezindeki fiziksel cihaz ve sistemlerin envanteri tutulmalıdır.
- Veri merkezi bilgi sistemi potansiyel saldırılara karşı izlenip korunmalıdır.
- Sistem odasında 7/24 kayıt yapan güvenlik kameraları bulundurulmalı, kamera kayıtları 2 ay süre ile saklanmalıdır.
- Veri merkezindeki veriler yedeklenmelidir, bu amaçla veri yedekleme mekanizması oluşturulmalıdır.
- Herhangi bir güvenlik ihlali tespit edildiğinde ilgili taraflara bilgilendirmeler yapılmalıdır.
- Veri merkezinde bulunan işletmecinin kontrolü dışına çıkacak (devretmek, satmak, devre dışı bırakmak) veriler imha edilmelidir. Elektronik/manyetik ortamda verilerin imha edilmesi, Kişisel Verileri Saklama ve İmha Politikasına (BAU-BİDB-PL-013) uygun bir şekilde yapılmalıdır.
- Veri merkezine yetkisiz giriş, yetkili bir personelin eşlik etmesi ile yalnızca gerekli durumlarda gerçekleştirilmelidir.
- Veri merkezine erişim yetkisi BİDB tarafından kısıtlı olarak verilmelidir.
- Erişim yetkisi olan kişilerin oturum hareketleri ve işlemleri kayıt altına alınmalı ve izlenmelidir.
- Yetkilendirme yapılırken Kimlik Doğrulama ve Yetkilendirme Protokol'ü uygulanmalıdır.
- Sanal makineler silinmeden önce, sanal makineye ait disk dosyalarına sıfır yazılmalı ve daha sonrasında kalıcı silme işlemi uygulanmalıdır.

15. Cihaz Kullanım Politikası

- BAU tarafından kişiye tahsis edilen cihazların kaydı tutulmalı ve cihazlar kişiye zimmetli olmalıdır.
- Bu cihazların teknolojik yeterliliği kontrol edilmelidir.
- Cihazlar parola politikasına uygun şekilde şifrelenmelidir.
- Cihazlara antivirüs yazılımları kurularak uzaktan erişimde yaşanabilecek olan olası güvenlik problemleri engellenmelidir.

- Kampüs ağlarının aktif cihaz sayısının fazla olması nedeniyle uygun yazılımlar kurularak cihazların uzaktan yönetimi ve sorun giderimi sağlanmalıdır.
- BAU'ya ait ağa internet üzerinden bağlanacak olan kişi ve kurumlar VPN kullanmalıdır.
- Uzaktan erişim izni standart dışı erişimlerde BİDB tarafından geçici olarak verilmelidir.
- BAU tarafından tahsis edilen taşınabilir bilgisayarların fiziksel olarak korunmasına önem gösterilmelidir.
- Tahsis edilen cihazlar BAU tarafından belirlenen alanlarda bulundurulmalıdır, bilginin korunması amacıyla cihazlar belirtilen alanların dışına çıkarılmamalıdır.
- BAU'ya ait verileri içeren tüm işlemler, BAU tarafından tahsis edilen cihazlarda yapılmalıdır, kişisel cihazlar kullanılmamalıdır.
- BAU verilerine uzaktan erişim sınırlandırılmalı, yetkili erişim minimum düzeyde tutularak ve kısıtlanarak verilerin güvenliği sağlanmalıdır.
- Bilgisayarların ekran süresi sınırlandırılarak işlem yapılmayan bilgisayarlarda otomatik kilitleme yapılmalı, uzun süre kullanılmayan hesaplarda oturumun kapatılması sağlanmalıdır.
- Bilgisayarlarda yapılan işlemler devam ederken, bilgisayar başından ayrılmayı gerektiren durumlarda ekran kilitlenmelidir.
- Taşınabilir bilgisayarlar, kurum dışına çıkarıldığında el çantası/bagajı ile dikkatli bir şekilde kullanılmalıdır.
- BAU tarafından tahsis edilen cihazların kaybolması/bozulması durumunda cihaz BİDB'ye kişinin beyanı ile teslim edilmelidir.
- Ofislerde kullanılan ortak yazıcılar arıza konumuna geçtiğinde üzerindeki bilgiler silinmesi sağlanacak şekilde kurulumu yapılmalıdır ve yazıcılara erişim kullanıcı bazlı olmalıdır.
- BAU'nun tahsis ettiği mobil cihazlar MDM (Mobil Cihaz Yönetimi) ile yönetilmelidir.
- Mobil cihazın kaybolması durumunda IMEI'leri üzerinden bağlantı kurularak cihaz fabrika ayarlarına döndürülmeli ve veri güvenliği sağlanmalıdır.
- Cihazlara kimliği belirsiz kişiler tarafından gönderilen dosya ve mesajlar dikkate alınmamalıdır.
- Cihazlar el değiştirecekse, tüm veriler geri dönüştürülemeyecek şekilde sıfırlanarak yeni kullanıcıya teslim edilmelidir.
- Cihazlarda kuruma zarar verebilecek gizli belgeler bulundurulmamalıdır.
- MDM yüklenen tüm cihazlar kayıt altına alınarak takipleri yapılmalıdır.

- Mobil cihazların kontrolü için bir yönetim arayüzü oluşturulmalı ve kullanılan cihazların kaydı burada tutulmalıdır.
- Mobil cihazlar en az 4 rakamdan oluşan ekran parolası ile şifrelenmelidir.
- Cihazların kablolu (USB ile medya bağlantısı, vb.) ve kablosuz (bluetooth bağlantısı ve hotspot, vb.) kullanımı kısıtlanmalıdır.
- SMS içeriğindeki linklerin kullanımı ve kopyala/yapıştır fonksiyonunun kullanımının sakıncalarıyla ilgili farkındalık oluşturulmalıdır.
- Ekran görüntüsü alınmasının engellenmesi, ayarlar kısmına erişimin engellenmesi, MDM'in cihaz adminlerinden kaldırılmasının engellenmesi, cihazın fabrika ayarlarına dönülmesinin engellenmesi sağlanmalıdır.
- Mobil cihazlarda kurulu uygulamaların verileri toplanmalıdır.
- Kuruma ait web sayfaları gibi erişimin sağlanması istenilen web sayfaları MDM'e ait browser üzerinden yer imi (bookmark) olarak eklenmelidir.
- Uygulama bazlı tünelleme yapılarak bu uygulamalara kurum ağındaymış gibi erişim sağlanmalıdır.
- Veri güvenliğinin sağlanması için ActiveSync konfigürasyonu uygulanmalıdır.
- Yurt dışı seyahati sırasında kullanılacak olan cihazlar kişiye zimmetli olmalıdır.
- Mobil cihazların yurt dışı kullanımı açılmalı ve gerekli yurtdışı paket kurum tarafından sağlanmalıdır.
- Seyahat dönüşü cihazlar incelemeye alınmalı ve seyahat başlangıcıyla farklar değerlendirilmelidir. Şüpheli bir durum oluştuğunda detaylı inceleme ve takip yapılmalıdır.

16. Temiz Masa Temiz Ekran Politikası

- Çalışma alanlarının temiz ve düzenli tutulması sağlanmalıdır.
- Kuruma ait önemli bilgiler içeren bir evrak (sözleşme, resmi yazı vb.) masanın üzerinde bırakılmamalıdır.
- Yazıcılardan çıkarılan evraklar hemen alınmalı, veri güvenliğini sağlamak amacıyla ihtiyaç dışında çıktı alınmamalıdır.
- Kuruma ait veriler dosya, klasör ve kısayollar ile masaüstüne kaydedilmemelidir.
- Personel şifresini kimseyle paylaşmamalı, çalışma alanında ve elektronik ortamda yazılı olarak tutmamalıdır.
- Veri güvenliğini sağlamak için çalışma saatleri dışında ve odada kimse yokken ofis kapıları kilitli tutulmalıdır.

- Bilgisayarlar parola ile korunmalı, kısa süreliğine de olsa bilgisayar başından uzaklaşılacağı zaman ekran koruyucusu aktifleştirilmelidir (Windows+L).
- Çalışma saatleri dışında bilgisayarlar kapalı tutulmalıdır.
- Kuruma ait antetli kağıtlara kilitli dolaplarda tutulmalıdır.
- Kuruma ait verileri içeren dosyalar gizlilik derecesine göre sınıflandırılarak kullanılmalıdır.
- Kullanılmayacak belgeler kağıt öğütme makinesinde imha edilmelidir.
- Sistem odası gibi verinin depolandığı yerlere yiyecek, içecek ile girilmemelidir.
- Taşınabilir disk, cep telefonu vb. cihazlar masanın üstündeyken çalışma ortamı terk edilmemelidir.
- Kurum ile ilgili haberleşmelerde kurum e-posta hesabı kullanılmalıdır.

17. Teknik Çalışma Politikası

- BAU lokasyonlarında yapılacak tüm kurulum çalışmalar öncesinde çalışma yapacak şirketlerin ve onlara bağlı tüm taşeronların kurulum ekip listelerini BAU'ya Kurulum Ekip Listeleri Formu ile iletmelidir.
- BAU lokasyonlarında yapılacak tüm acil çalışmalar öncesinde çalışma yapacak şirketlerin ve onlara bağlı tüm taşeronların acil durum ekip listelerini BAU'ya Acil Durum Ekip Listeleri Formu ile iletmelidir.
- BAU lokasyonlarında yapılacak tüm planlı çalışmalar için öncesinde çalışma yapacak şirketlerin ve onlara bağlı tüm taşeronların Planlı Çalışma İzin Talep Formu ile BAU'dan uygunluk talep edilmelidir.
- Acil girişler için formlarda ismi olan personellerden giriş sırasında izin talep formu istenmeyecektir. Müdahaleye gelmeden önce ve lokasyondan ayrılırken BİDB'ye telefonla bilgi verilmesi ve müdahale sonrasında arıza müdahale ile ilgili detay bilginin Arıza Çalışması Sonuç Raporu doldurularak elektronik posta ile paylaşılmalıdır.
- Planlı çalışma için, kuruma dışarıdan gelen teknik personelin kuruma girişte kimlik kontrolü sağlanmalı ve kurum içindeki erişimi bir refakatçi eşliğinde sınırlanmalıdır.
- Kuruma dışarıdan giren personel, BAU lokasyonlarında bulunduğu müddetçe kurumun kurallarına uygun şekilde davranmalıdır. Bu durumun sağlanmasından çalışma yapan personelin işvereni sorumludur.
- Çalışma yapan personel çalıştığı lokasyondaki tüm varlıkları temiz ve teslim aldığı şekilde bırakmakla sorumludur.

- Çalışmanın sona ermesinin ardından çalışan personelin, çıkış kayıtları alınarak kurum dışına çıkışı sağlanmalıdır.
- Yapılan çalışmayla ilgili Teknik Çalışma Raporu, çalışma sona erdikten sonra 2 (iki) iş günü içinde kuruma iletilmelidir.

18. Yazılım Kullanım Politikası

- BAU tarafından tahsis edilen tüm cihazların yazılım ve donanım bilgileri güncel, geriye dönük ve tümleşik olarak PARS üzerinde tutulmalıdır.
- Zararlı yazılımlardan korunmak için gerekli kurulumlar BİDB tarafından yapılmalıdır.
- BAU tarafından tahsis edilen tüm cihazlarda Uzaktan Erişim Protokolü uygulanarak, beyaz listede bulunan uygulamalar haricinde uygulamalar yüklenmemelidir.
- Beyaz liste BİDB tarafından erişilebilirlik sınırlaması ile oluşturulmalı ve denetimi yapılmalıdır.
- Cihazlara yazılım BİDB tarafından yüklenir. Kullanıcı, mobil, bilgisayar, tablet ve benzeri hiçbir cihaza yazılım yüklememelidir. Gerekli olduğu durumlarda BİDB'den onay alınarak kurulum talebi yapılmalıdır.
- Bilgi sistemlerinin sürekliliği ve gizliliğini korumak için kurum cihazlarında güncel anti-virüs programları yüklü olmalıdır.
- BAU bilgi sistemleri altyapı bileşenlerinde gerekli önlemler (Firewall gibi) alınmalıdır.
- Office 365 global güvenlik kuralları ile e-postalardan yayılabilecek zararlı yazılımlar engellenmelidir.
- BAU tarafından tahsis edilen tüm bilgisayarları taşınabilir cihazlardan geçebilecek virüs gibi tehditlerden korunmak için, taşınabilir cihazlarda otomatik zararlı yazılım taraması yapılmalıdır.
- DNS sorguları kaydedilerek zararlı IP adreslerine erişim denetlenmelidir.

19. Sosyal Medya Kullanım Politikası

- Sosyal medya kullanımının daha bilinçli ve aktif yapılmasını sağlamak için bir sosyal medya uzmanı KİB tarafından belirlenmelidir.
- Hesapların kullanıcı adı ve şifreleri sadece sosyal medya uzmanları tarafından bilinmeli ve KİB tarafından şifrelenerek saklanmalıdır. Hesap ve oturum hareketleri izlenerek denetlenmeli, olağan dışı gözlenen bir durumda gerekli işlemler yapılmalıdır.
- Sosyal medya uzmanları, uyulması gereken politikalar ile ilgili bilgilendirilmelidir.
- Sosyal medya kullanıcılarına hızlı ve kolay erişim sağlanmalıdır.

- Kurum ile ilgili hiçbir gizli ve hassas veri paylaşımı yapılmamalıdır.
- İtibar zedeleyici, ayrımcı, ırkçı, saldırgan, politik ve rahatsız edici etkileşimlerden uzak durulmalıdır.
- Yazım kuralları ve noktalama işaretlerine dikkat ederek yanlış anlaşılmalar önlenmelidir.
- Tasarımı veya telifi kuruma ait olmayan görseller izinsiz kullanılmamalıdır.
- Kişisel veri barındıran içerikler için Kişisel Verilerin Korunması Kanunu uyarınca aydınlatma ve gerekli ise rıza yükümlülükleri yerine getirilmelidir.
- Resmi sosyal medya hesapları BAU'nun web sitesinde belirtilmelidir.
- Sosyal medya hesaplarında reklam içerikli paylaşımlar yapılmamalıdır.
- Sosyal medya hesaplarının altında üçüncü kişilerce yapılan yorumlar incelenmeli ve uygunsuz yorumlar silinmelidir.
- BAU'nun sosyal medya hesapları Parola Politikasına (BAU-BİDB-PL-007) uygun bir şekilde şifrelenerek iki aşamalı şifreleme yöntemi ile korunmalıdır.
- Kurumun sosyal medya hesaplarından üçüncü kişiler ile tartışılmamalıdır.
- Bir sosyal medya uzmanı veya yetkili personel, politikada belirtilen maddelere aykırı hareket etmesi durumunda İKDB tarafından disiplin süreci başlatılmalı ve hesaplara erişimi engellenmelidir.

20. Kabul Testi Politikası

- Yazılım test sürecinin son aşamasıdır. Kabul Testlerinde, ürünün farklı koşullarda nasıl davranması gerektiğine dair senaryolar oluşturulmalı, oluşturulan senaryolarda belirtilen durumlarda kabul kriterlerini hangi seviyede sağlandığı test edilmelidir.
- Tedarik edilen ürünün hedeflenen amaçları karşılayıp karşılamadığını kontrol etmek için İş Kabul Testi (BAT) uygulanmalıdır.
- Yazılımın iş gereksinimlerini karşılayıp karşılamadığı son kullanıcı tarafından Kullanıcı Kabul Testine (UAT) tabii tutulmalıdır. Kullanıcı Kabul Testi sadece işlevseldir, gerçek zamanlı veriler ile yapılmamalıdır.
- Sözleşme/Yönetmelik Kabul Testleri ile tedarik edilen ürünün kural ve düzenlemelerinin ülkenin ve kurumun kurallarına uygun olma durumunun tespiti yapılmalıdır.

21. Tedarikçi Politikası

- Tedarikçilerin BAU'ya ait fikri mülkiyet hakları, ticari sırlar, hassas ve gizli bilgiler dahil erişimleri olan tüm bilgi varlıklarını korunması için gerekli güvenlik tedbirleri alınmalıdır.

- BAU, Tedarikçileri ile iş ilişkisi sürecinde gerekli olduğunda birtakım gerçek kişilere ait veri aktarımında bulunabilecektir. Dolayısıyla, tüm Tedarikçilerin iş ilişkisi sebebiyle BAU tarafından paylaşılan kişisel verilerin hukuka uygun olarak işlenmesini ve muhafaza edilmesini, gerekli güvenlik tedbirlerinin alınması sağlanmalıdır.
- Tedarikçiler, kişisel verilerin korunmasının garanti edilmesi için BAU ile akdedilecek sözleşmelerde bu hususa ilişkin belirli sözleşmesel yükümlülükleri kabul ve taahhüt etmelidir.
- Tedarikçilerin erişimi olan tüm bilgi varlıklarının BAU'nun önceden verilmiş yazılı izni olmaksızın kesinlikle kullanılmamalı veya ifşa edilmemelidir.
- Tedarikçiler, BAU'nun gizli bilgilerini kendi kuruluşları dışındaki kimseye ifşa etmemeli, kendi kurumları içerisinde ise yalnızca işin ifası için bilmesi gerekenler ile sınırlı olmak üzere ifşa edilmelidir.
- Tedarikçiler, BAU'ya ait gizli bilgileri kendi çıkarları ya da BAU haricindeki kişi ve kurumların çıkarları için kullanmamalıdır.
- Tedarikçi ve/veya (alt) yükleniciler ile mal/hizmet tedarik sözleşmesi imzalanması öncesinde BAU Gizlilik Sözleşmesi yapılmalıdır.
- Tedarikçi ve/veya (alt) yüklenici tarafından temin edilen yazılımların BAU bünyesinde bulunan sistemlerine her türlü bakım, onarım, güncelleme vb. ihtiyaçlar için uzaktan erişim ihtiyacı bulunması durumunda yapılan iş ve işlemlerin kayıt altına alınabildiği BAU tarafından onaylı uzaktan bağlantı programları kullanılmalıdır. Bağlantı programı için lisans ihtiyacı olması halinde ilgili firma lisansı sağlamayı kabul ve taahhüt etmelidir.
- Tedarikçi ve/veya (alt) yüklenici iş sürekliliğinin sağlanması amacıyla Acil Durum Planı oluşturmayı kabul ve taahhüt etmelidir.
- BAU, Tedarikçi ve/veya (alt) yüklenicinin BAU lokasyonlarında görevlendireceği teknik personel için Servis Sağlayıcı kimliği sağlamalı ve yetki tanımlamasını yapmalıdır.
- Tedarikçi ve/veya (alt) yüklenici BAU lokasyonlarında görevlendirdiği ve özel yetki atanmış teknik personelin ilgili firma ile ilişiğinin kesilmesi veya görevinin değişmesi durumunda, yetki iptali için kimlik bilgileri ile yeni görevlendireceği teknik personelin bilgileri ve verilecek özel yetki kapsamının BAU'ya derhal bildirilmesini kabul ve taahhüt etmelidir.
- Tedarikçi ve/veya (alt) yüklenici ile imzalanan sözleşmenin süresinin dolması ya da feshedilmesi durumunda ilgili firmaya atanmış tüm yetkilerin kaldırılması için BİDB'ye BAU sözleşme sahibi tarafından bilgi verilmelidir.

- Tedarikçi ve/veya (alt) yüklenicinin kendisi ya da üçüncü partiler tarafından bilgi ve iletişim güvenliği ihlali gerçekleştiğinde, ihlal durumunu BAU Yönetimine yazılı olarak bildirmeyi kabul ve taahhüt etmelidir.

22. Kurum Verileri Politikası

- BAU tarafından üretilen tüm bilgi varlıklarından BAU veri kütüphanesi oluşturulmalıdır.
- Tüm BAU bilgi varlıklarına, BAU içerisinde varlık sahibi tanımlanmalıdır.
- BAU veri kütüphanesindeki tüm bilgi varlıkları sınıflandırılmalıdır.
- BAU veri kütüphanesindeki tüm bilgi varlıklarının gizliliği garanti altına alınmalıdır.
- BAU veri kütüphanesindeki tüm bilgi varlıklarının güncelliği, bütünlüğü ve erişilebilirliği sağlanmalıdır.
- BAU bilgi varlıklarının paylaşılacağı tüm kurum ve kuruluşlarla paylaşım öncesi BAU Gizlilik Sözleşmesi yapılmalıdır.
- BAU kütüphanesindeki tüm bilgi varlıklarının periyodik olarak yedeklenmesi sağlanmalıdır.
- BAU kütüphanesindeki tüm bilgi varlıklarının dış tehditlere karşı en üst seviyede korunması için gerekli teknolojik gereklilikler sağlanmalı ve tüm değişimlere dirençli hale getirilmelidir.
- BAU veri kütüphanesindeki tüm bilgi varlıklarının güncelliği, bütünlüğü ve erişilebilirliği sağlamak için kullanılması gereken teknolojik altyapı BİDB sağlanmalıdır.

23. Sanal Sunucu İmha Politikası

- BAU'nun verilerinin depolandığı sanal sunucuların güvenliğinin garanti altına alınması yükleniciler ile yapılan sözleşmelerle sağlanmalıdır.
- BAU'nun verilerinin depolandığı sanal sunuculardaki BAU bilgi varlıklarının yedeklemesi sağlanmalıdır.
- BAU'nun verilerinin depolandığı sanal sunucularda loglama kullanılmalıdır ve bu kayıtların 10 yıl saklanmalıdır.
- BAU'nun verileri depoladığı sanal sunuculardaki silinmesi gereken bilgi varlıkları üstüne yazarak (wiper yöntemi) yok edilmelidir.
- Sanal sunucu kullanım dışı kaldığında makineye ait diske üstüne yazarak (wiper yöntemi) kalıcı silme işlemi uygulanmasının sağlanması sözleşme ile garanti altına alınmalıdır.

19./12./2022
ASLI GİBİDİR

Yönetim Destek ve Bilgi Sistemleri Direktörlüğü