BAYÜ	VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI POLİTİKASI UZAKTAN ERİŞİM VE MOBİL CİHAZ KULLANIMI POLİTİKASI TAŞINABİLİR VE ORTAM YÖNETİM VE İMHA POLİTİKASI GİZLİLİK SINIFI VE BİLGİ ETİKETLEME POLİTİKASI	Kod No:	EYS.PL.06
		İlk Yayın Tarihi:	01.10.2022
		Revizyon Tarihi:	30.10.2023
		Revizyon No:	0.1
Birim / Bölüm:	Bilgi İşlem Daire Başkanlığı		

İÇİNDEKİLER

Bayburt Üniversitesi'nin, KVKK, DDO ve BGYS ile ilgili uyması gereken bazı kurallar aşağıda belirtilmiştir.

1. AMAÇ

Bilgi varlıklarının envanter listesinin dokümante edilmesi, bilgi varlıklarının kullanım kuralları, bilgilerin yedeklendiği, taşındığı, uzaktan çalışma ve varlıkların dolaşıma sunulduğu ortamlara, ortamlarda taşınan verilere yetkisiz kişilerin erişimini engellemek ve hassas bilgi içeren bilgiye izinsiz kişilerin sızmasını engellemek için gerekli önlemleri almak.

2. KAPSAM

Kişisel veri ve özel nitelikli veriler dâhil olmak üzere BAYÜ'ye ait basılı, yazılı her tür bilgi varlığının korunması, varlıkların taşınması, erişilmesi, uzak bağlantı ve mobil cihazlara ilişkin kuralların yanı sıra varlıkların imhası, elden çıkarılması, değiştirilmesi veya dönüştürülmesi süreçlerini kapsamaktadır.

3. SORUMLULAR

Kapsam dâhilinde tüm çalışanların bu politikaya ve erişim haklarına uygun hareket etmesi Bayburt Üniversitesi Rektörlüğü'nün sorumluluğundadır.

4. TANIMLAR

BAYÜ: Bayburt Üniversitesi

KVKK: Kişisel Verileri Koruma Kanunu

ÖNKV: Özel Nitelikli Kişisel Veri

CB: Cumhurbaşkanlığı

DDO: Dijital Dönüşüm Ofisi

BGYS: Bilgi Güvenliği Yönetim Sistemi

KVYS: Kişisel Verileri Yönetim Sistemi

İMHA: Saklama süresi dolan tüm kişisel ve kurumsal kayıtların imhası

5. UYGULAMA

5.1. VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI POLİTİKASI

Bu doküman, Bayburt Üniversitesi tüm kullanıcıları ve 3. tarafların kurum varlıklarını kullanırken uyması gereken kuralları tanımlamak amacıyla oluşturulmuştur.

Bayburt Üniversitesi Kişisel Verilerin Korunması Kanunu, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ve Bilgi Güvenliği Kapsamı dokümanında belirtilen tüm kullanıcıları, geçici görevliler ve kurumun bilgi varlıklarına erişimine izin verilmiş olan diğer kurum/şirket çalışanları (üçüncü taraf) bu politika ile belirtilen kurallara uymak zorundadır.

5.1.1. VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI POLİTİKASI

GENEL KURALLAR

1. Kurum bilgi ve haberleşme sistemleri ile donanımların (İnternet, e-posta, telefon, çağrı cihazları, telsiz, faks, bilgisayarlar, tabletler, mobil cihazlar ve cep telefonları vb. dahil olmak üzere) kullanımı sadece kurum hizmet alanı ve ilgili amaçlar doğrultusunda olmalıdır. Bilişim kaynakları sadece kurum için yapılan çalışmalar ve kurumun onayladığı alanlarda kullanılabilir. Bu sistemlerin yasa dışı, rahatsız edici, kurumun diğer politika, standart ve rehberlerine aykırı veya kuruma zarar verecek herhangi bir şekilde kullanımı bu politikanın ihlal edildiği anlamına gelir.
2. İş süreçlerini engellemeyecek düzeyde ve Bilgi Güvenliği Politikasını ve BGYS prosedürlerini ihlal etmeyen kişisel kullanımlar kabul edilebilir kapsamda değerlendirilir.
3. Kullanıcılar bilişim kaynaklarını aşağıdaki durumlar için kullanamaz:
    a. Yetkisiz erişim
    b. Kişisel veriler ve özel nitelikli verilerin ifşası
    c. Diğer kullanıcılara ait varlıklara kasıtlı yetkisiz erişim ve ziyan
    d. Diğer kullanıcılara ait varlıkları yetkisiz kullanmak
    e. Bilişim kaynaklarında yer alan varlıkların izinsiz (yetkisiz) kopyalamak ve kullanmak

f. Bilgisayar iletişim imkânlarını kasten gereksiz olarak kullanarak, diğer kullanıcıların bilişim faaliyetlerini engellemek. (Rastgele etkileşimli elektronik iletişim veya e-posta değişimi başlatmak, etkileşimli ağ olanaklarının aşırı kullanımı vb.)

g. Kuruma ait kişisel verilerin ve kritik bilgisinin ortaya çıkarmak veya kurum servislerinin ulaşılamaz hale getirmek

h. Kurum faaliyetleri ile ilişkisi olmayan, özel iş veya eğlence amacıyla kullanmak

i. Kuruma ait bilgi işlem sistemlerine şifreleme ve parola mekanizmalarını kırmaya yönelik program ve araçları yüklemek ve kullanmak

j. Kuruma ait bilgi sistemleri üzerinde, kurumun bilgisi ve izni olmadan değişiklik, yükseltme, genişletme yapmak

k. Kurum gizli varlıklarına yetkisiz erişim yapmak

l. İşle ilgili olmayan veya telif hakları ile korunan dosyaları (örneğin müzik, film, kitap dosyaları, vb.) kurum bilgisayarlarına ve bilgi sistemlerine indirmek, depolamak, çoğaltmak ve paylaşıma açmak

4. Üst yönetim tarafından yazılı veya mail yolu ile yetki verilmedikçe ağ izleme, port taraması veya güvenlik taraması yapılamaz.

5. Kullanıcılar kurum tarafından kendilerine sağlanmış olan program lisans bilgilerini sadece kurum faaliyetleri doğrultusunda kullanabilir.

6. USB Disk, CD-ROM gibi taşınabilir cihazlarda kuruma özel veya gizli bilgi yedeklenmesi ve bulundurulması esas olarak kabul edilmemektedir. Zorunlu durumlarda uyulması gereken esaslar "Uzaktan Erişim ve Mobil Cihaz Politikası"nda belirtilmiştir. Diğer taşınabilir ortamlar için "Uzaktan Erişim ve Mobil Cihaz Politikası"nda belirtilen kurallara uyulmalıdır.

7. Herkese açık sistemler (örneğin genel internet sayfaları) hariç tüm bilişim sistemlerine erişim parola korumalı olmalıdır. Parolalar "Parola Politikası''na uygun şekilde tanımlanmalı ve kullanılmalıdır.

8. Kullanıcılar kurum kaynaklarına erişimi için kullandığı hesap bilgilerini kimseyle paylaşamaz. Yetkisiz kişilerin ele geçirmesine imkân verecek şekilde söylememeli, yazmamalı, kaydetmemeli ve elektronik ortamda depolamamalıdır. İlgili kullanıcı hesabı ile yapılan tüm işlemlerin sorumluluğu hesap sahibi kullanıcıya aittir.

9. Kurum varlıklarına her türlü erişim için "Erişim Kontrol Politikası"'na uygun hareket edilmelidir.

10. Kuruma ait bilgi sistemleri üzerindeki kaynaklara erişecek tüm bilgisayarlar etki alanına dâhil edilerek kullanılmalıdır. Kurumun üretim sahasında kullanmış olduğu ortak bilgisayarlar etki alanı dışında tutulmuştur. Ortak hesaplarla yönetilmektedir.

11. Bilgisayarlar, aktif kullanım dışında iken şifreli ekran koruyucular devreye alınmalıdır.

12. Mesai zamanları dışında bilgisayar sistemleri mecbur olmadıkça kapalı tutulmalıdır.

13. Kullanıcılar sorumlu oldukları kurum varlıklarını yetkisiz kişilerle paylaşamaz. Gerekli özenin gösterilmesi ve yetkisiz erişime karşı dikkatli olunması kullanıcı sorumluluğundadır.

14. Kurum bu sistemleri ve bu sistemlerle gerçekleştirilen aktiviteleri izleme, kaydetme ve periyodik olarak denetleme hakkını saklı tutar.

15. Çalışma alanlarında, "Temiz Masa ve Temiz Ekran Politikası" prensiplerine uygun olarak, GENEL olarak sınıflandırılmış bilgiler dışında bilgilerin başkalarınca görülmesine imkân verilmeyecek şekilde önlemler alınmalıdır;

   a. GENEL olmayan belgeler, masalarda bırakılmamalıdır.

   b. GENEL olmayan dosyalar üzerinde çalışılırken bilgisayar ekranları herkesin görebileceği konumda bırakılmamalıdır.

   c. GENEL olmayan dokümanlar diğer kişilerce görülmesini engellemek amacıyla, kullanılmadığı zamanlarda masa üstlerinden kaldırılıp gerekli korumaları alınmış çekmece ve dolaplarda saklanmalıdır.

16. GENEL olmayan belgeler dışında doğrudan işle ilgili olarak kendisine ulaştırılmayan ya da teslim edilmeyen kurum belgelerini incelememeli, değiştirmemeli, saklamamalı, kopyalamamalı, silmemeli ve paylaşmamalıdır.

17. Gizlilik dereceli bilgilerin posta, faks, telefon, e-posta ve benzeri elektronik yöntemlerle iletiminde politikaya uygun davranılmalıdır.

18. Herkese açık bilgiler dışındaki bilgileri internet üzerinde, haber gruplarında, posta listelerinde ve forumlarda paylaşmamalıdır.

19. Gizlilik dereceli bilgi içeren belgeler, elektronik ortamları ve bilgi işlem sistemlerini korumak için gerekli fiziksel önlemleri uygun şekilde yerine getirmelidir.
20. Gizlilik dereceli bilgiler elektronik ortamda işlenirken, depolanırken, aktarılırken bilgi güvenliğine uygun şekilde davranılmalıdır.
21. Gizlilik dereceli bilgilerin ve bilgi içeren ortamların imhasında "Taşınabilir Ortam Yönetimi ve İmhası Politikası"'na uygun şekilde davranılmalıdır.
22. Kurum tarafından açıkça belirtilen durum ve yöntemler dışında 3. taraflar ile kurum bilgileri paylaşmamalı, satmamalı, aktarmamalı, yayınlamamalı ve internet ortamında paylaşmamalıdır.
23. 3. Taraflar ile gizlilik sözleşmesi imzalanmadan, yetkili kurum çalışanınca nezaret edilmeden kurum bilgi işlem sistemlerine ve donanımlarına bağlanmamalı ve çalışmalarına izin verilmemelidir.
24. Çalışanlar, çalıştıkları ortamdaki masa ve dolap çekmecelerini kilitli tutmalı ve anahtarları sorumlu kişiler haricinde kimseyle paylaşmamalıdır.
25. Başta kullanıcı bilgisayarları ve sunucular olmak üzere mümkün olan tüm sistemler, zararlı yazılımlara karşı korunması için uygun şekilde kullanılmalıdır.
26. Kuruma ait bilgi sistemleri izinsiz olarak kullanım dışı bırakılmamalı, yeri değiştirilmemeli ve kurum dışına çıkartılmamalıdır.
27. İş süreçleri için gerekmeyen ve kullanılmasına izin verilmeyen sunucu hizmetleri bilgi işlem sistemleri üzerinde çalıştırılmamalıdır.
28. Kurum tarafından sağlanan ve kullanım amaç ve biçimleri yazılı olarak bildirilen kurum ağ bağlantı yöntemleri dışında bir yöntemle (örneğin ADSL modem, 3G modem, GPRS, HUB vb.) internete veya başka ağlara bağlanmak için kullanılmamalıdır.
29. Kabul edilebilir internet ve e-posta erişim kuralları için "İnternet Kullanım ve E-Posta Politikası"na uygun hareket etmelidir.

GENEL DONANIM KULLANIM ESASLARI

1. Bilgisayar donanımlarının kullanıcılara verilmesi ile ilgili kullanım esaslarının tanımlanması Bilgi İşlem Daire başkanlığı tarafından yönetilir.
2. Kullanıcılar donanımlara yeni bileşenler ekleyemez veya çıkartamazlar. Ek bir gereksinimin oluşması durumunda kurum yardım masası üzerinden talepte bulunmalıdır.
3. Kullanıcılar kullandıkları bilgisayarların işletim sistemlerinde değişiklik yapamazlar.
4. Bilgisayar donanımları üzerindeki tüm bilgilerin kurumsal nitelikte olduğu kabul edilir.
5. Kurum bilgisayarları üzerinde tutulan tüm bilgiler kurum tarafından denetlenebilir.
6. Kullanıcılar bu esasa uymakla yükümlüdürler.
7. Kullanıcılar donanım güvenliğini tehdit edecek eylemlerden sakınmakla yükümlüdürler. Kullanıcılara teslim edilen donanımlar üzerinde ayarların değiştirilmemesi, anti virüs programı gibi makine güvenliği ile ilgili ayarlara müdahale edilmemesi ve ilgili programlarda bir sorun gözlemlendiğinde bağlı olduğu sorumluya bildirmesi gerekmektedir.
8. Kullanım gerekliliği kurum tarafından yazılı olarak belirtilen güvenlik yazılımlarını (Örneğin anti-virüs, kişisel güvenlik duvarı, vb.) bilgi işlem sistemlerden kaldırmamalı veya devre dışı bırakmamalıdır.
9. İstemciden istemciye dosya paylaşım programlarını (P2P) kurum bilgisayarlarına yüklememeli ve kullanmamalıdır.
10. Donanımlar üzerinde kurum tarafından izin verilmeyen bir programın yüklenmemesi, güvenlik riski oluşturabilecek internet sitelerine girilmemesi kullanıcı sorumluluğundadır.
11. Kullanıcılar kurumdan ayrılmadan önce kendilerine zimmetli olan tüm donanımları teslim etmekle yükümlüdürler.
12. Kullanıcılar, kullanım hatası (makine üzerine bir sıvının dökülmesi, makinenin düşürülmesi, yetkisiz donanım eklenmesi/çıkarılması vb.) nedeniyle oluşan donanım sorunlarından sorumludurlar.
13. Yükleme yetkisi verilmemiş kullanıcılar program yükleme isteklerini Kurumsal Yardım Masası üzerinden bildirmelidirler ve Bilgi İşlem Dairesi Başkanlığı'ndan onayını almalıdırlar.

OFİS EKİPMANLARI KULLANIM ESASLARI

1. Kullanıcılar ofis ortamında çalışırken temiz masa politikasına göre önemli dokümanların kullanılmadığı zamanlarda masa üstlerinden kaldırılıp gerekli korumaları alınmış çekmecelerde saklanmalıdır. Bu şekilde masa üstlerinde hassas bilgilerin bulunmayacağı garanti altına alınmaktadır.
2. Kullanıcılar ofis ortamında çalışırken "Temiz Masa ve Temiz Ekran Politikası"'na göre bilgisayarlar oturumlarını ekran kilidi ile korumalıdır.
3. Faks ve Ses cihazlarını kullanıcılar sadece kurum işleri için kullanmalı, işle alakasız şahsi işleri için meşgul etmemelidirler.
4. Kullanıcılar çıktı alma işlemi için kendi katlarında bulunan ağ yazıcılarını kullanmalıdırlar. Çok gizli gizlilik derecesindeki çıktılar masaüstü ve genel kullanıma açık olmayan yazıcılardan alınmalıdır.
5. Kurum işi ile alakalı olmayan çıktılar kesinlikle kurum yazıcılarından çıkarılmamalıdır.
6. Çıktı alınan kritik dokümanlar yazıcıya gönderildikten sonra, yazıcı yanında beklenmeli, tüm dokümanın çıktı işlemi bittikten sonra yazıcının yanından ayrılmak gerekmektedir.
7. Yazıcıya gönderilen ve daha sonra iptal edilen tüm dokümanlar mutlaka kontrol edilmelidir.
8. Kullanılmayan ve yok edilmesi gereken bilgiler ilgili prosedüre göre yok edilmelidir.
9. Kurum mühürleri kullanımında aşağıdaki kurallara uyulmalıdır.
    a. Mühür, kullanma yetkisi verilen kişi tarafından muhafaza edilmelidir.
    b. Mühür, kullanma yetkisi verilen kişilerden habersiz şekilde kullanılmamalıdır.
10. İnternet ve E-posta kullanımları "İnternet Kullanım ve E-Posta Politikası"'na göre yapılır.

5.1.2. UYGULAMA ve CEZA

Varlıkların Kabul Edilebilir Kullanımı Politikasına ve burada belirtilen diğer politika ve prosedürlere uymayanlar hakkında disiplin süreci başlatılır ve ilgili kanunlar çerçevesinde yasal işlem uygulanır.

5.2. UZAKTAN ERİŞİM VE MOBİL CİHAZ POLİTİKASI

Politikanın amacı; herhangi bir yerden kurumun bilgisayar ağına erişilmesine ve mobil cihaz kullanımına ilişkin standartları belirlemektir. Bu standartlar kaynaklarının yetkisiz kullanımından dolayı kuruma gelebilecek potansiyel zararları minimize etmek için tasarlanmıştır.

5.2.1. GENEL

- Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir.
- Cep telefonu üzerinde ilgili personellerin e-postaları kullanıldığında, şahsi cep telefonları parmak izi veya şifre ile korunmalıdır. Cep telefonlarının kayıp olması veya çalınmasına karşın bilgilerin ifşasını engellemek için şifre koruma zorunluluğu bulunmaktadır.

5.2.2. UZAK MASAÜSTÜ BAĞLANTILARI

- Kurum çalışanları hiç bir şekilde kendilerinin login ve e-posta şifrelerini, aile bireyleri dâhil olmak üzere, hiç kimseye veremezler.
- Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmadıklarından emin olmalıdır.
- Uzaktan erişim yöntemi ile kuruma erişen bütün bilgisayarlarda, en son güncellenmiş anti-virüs yazılımına sahip olmalıdır.
- Kurum ağına standart dışı erişim isteğinde bulunan organizasyon veya kişilere Bilgi İşlem Daire Başkanlığı'nın izni ile geçici olarak izin verilebilecektir.
- Her türlü uzaktan erişim hakkı Bilgi İşlem Daire Başkanlığı'nın izni ile yapılmaktadır.

5.2.3. MOBİL CİHAZLAR

Mobil cihazlar iş akış süreçlerinde sağladıkları birçok faydanın yanı sıra güvenlik zaafiyeti oluşturmaktadır. Mobil cihaz içerisinde kuruma ait herhangi bir bilgi; kurum dışında bulundurulmamalıdır. Olası kurum dışındaki mobil cihazlarda oluşan veri zaafiyeti nedeniyle kurum itibarı zarar görebilecektir.

Mobil cihazlar kurum bünyesi dışarısında kullanıldığında oluşabilecek tüm risklerden personel sorumludur.

5.3. TAŞINABİLİR ORTAM YÖNETİMİ

İş ihtiyaçlarının karşılanması amacıyla taşınabilir ortamların kullanılması gerektiği durumlarda, yalnızca kurum tarafından yetkilendirilmiş ve kurum envanterine kayıt edilmiş taşınabilir ortamların kullanılmasına izin verecek şekilde gerekli önlemler alınmalıdır.

5.3.1. ELEKTRONİK ORTAM

Özel veri/Gizli veri bulunduran bilişim teknolojisi cihazları içindeki veriler tekrar okunmayacak şekilde silindikten sonra cihaz tekrar kullanılabilir.

CD, DVD, HDD, Cep Telefonu gibi taşınabilir ortamlar aşağıdaki seçeneklerine göre elden çıkarılırlar. Elden çıkarma sırasında "Taşınabilir Ortam İmha Tutanağı" imzalanarak dosyalanır. Kayıtların Kontrolü Prosedürü ve Doküman Listesinde belirtilen saklama sürelerine göre saklanır.

Kurum tarafından sağlanan telefon ve tabletler üzerinde kırma (jailbreak veya rootlama) işlemi yapılmamalıdır.

5.3.2. TAŞINABİLİR ORTAM YÖNETİMİ

Bilgi içeren verinin bir yerden bir yere transfer işlemlerinde aşağıdaki yöntemler kullanılmaktadır.

İlgili taraf ile veri transferi gerçekleşmesi durumunda kurumun belirlemiş olduğu (FTP, Posta, WEB Servis, vb.) sistemler üzerinden karşılıklı olarak veri transferleri gerçekleşmektedir. Her veri transfer yöntem ve metodu ilgili tarafın kullanmış olduğu sistemlere göre değişiklik gösterebilir.

İlgili tarafın belirlemiş olduğu yöntem, metod ilgili tarafın sorumluluğunda olup Bayburt Üniversitesi'ni bağlayıcılığı bulunmamaktadır.

Taşınabilir ortamlar üzerinde yer alan kritik bilgi/veri şifreli olarak saklanmalıdır.

Kurum bünyesinde geliştirilen uygulamalar rootlanmış / jailbreak yapılmış cihazlarda çalışmayı reddetmelidir.

Bilgi transferi, izin verilen bölüm yöneticisi tarafından gerçekleşmektedir.

Bilgi transferinde 3.taraflar ile gizlilik sözleşmesi imzalanmaktadır.

Bilginin transferi işlemi sırasında bozulma kaybolma gibi durumlara karşı yedekleme yapılır.

Bilgi transferi işlemlerinde kurumumuzun politika ve prosedürlerine uygun olarak hareket edilmelidir.

5.4. KVKK, DDO VE BGYS İMHA POLİTİKASI

Kişisel Verilerin ve Bilgi güvenliği verilerin imhası, verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi şeklinde üç farklı şekilde sağlanabilir. İmha işlemindeki amaç, kalan veriler ile gerçek kişiye veya gizli bilgiye ulaşabilmenin mümkün olmamasıdır. BAYÜ, Kişisel Verilerin 6698 sayılı Kanuna ve ISO 27001 bilgi güvenliği standartlarına uygun olarak Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi ile ilgili gerekli her türlü teknik ve idari tedbirleri alır.

5.4.1. KİŞİSEL VERİLERİN ve BİLGİ GÜVENLİĞİ VERİLERİNİN SİLİNMESİ

ISO 27001 Bilgi güvenliği standartları dikkate alınarak tamamen veya kısmen otomatik yollarla işlenen Kişisel verilerin veya bilgi güvenliği verilerinin silinmesi; söz konusu kişisel verilerin İlgili kullanıcılar tarafından hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

BAYÜ bilgi güvenliği verileri ve kişisel verilerin silindiği durumlarda ilgili kullanıcılar için verileri hiçbir şekilde erişilemez veya tekrar kullanılamaz hale getirir.

5.4.2. KİŞİSEL VERİLERİN ve BİLGİ GÜVENLİĞİ VERİLERİNİN YOK EDİLMESİ

Yok etme işlemi, BAYÜ'nün verileri fiziksel kayıt ortamlarında işlediği durumlarda yapılabilecektir. BAYÜ bu durumda ilgili kişisel verilerin yanı sıra kurumun gizli verilerine erişilememesini, tekrar kullanılamamasını ve geri getirilememesini sağlayacaktır.

Yok etme işlemleri sırasında BAYÜ çalışanları ve ilgili departmanlar, BGYS yönetim temsilcisi'ne yok edilecek ilgili verileri bildirmekle yükümlüdür sonrasında BAYÜ BT hizmet sağlayıcı gerekli her türlü teknik ve idari tedbiri alacaktır.

5.4.3. KİŞİSEL VERİLERİN ANONİMLEŞTİRİLMESİ

Anonim Hale Getirme işlemi, BAYÜ'nün Kişisel Verileri tamamen veya otomatik yollarla işlediği durumlarda, bu verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Kişisel Verilerin Anonim Hale Getirilmesi BGYS Yönetim Temsilcisi'nin görevidir. BGYS Yönetim Temsilcisi gerekli durumlarda Veri sahibi ilgili birimden destek alabilir fakat her hâlükârda ilgili birimin bilgilendirme yükümlülüğü vardır.

Kişisel Verilerin Anonim Hale Getirilmesi sırasında BAYÜ, işbu Politika kapsamında belirtilen yöntemleri kullanabilir. Uygulanacak yöntemin doğruluğundan emin olunamadığı durumlarda BGYS Yönetim Temsilcisi'ne danışılmaktadır.

5.4.4. PERİYODİK İMHA

BAYÜ, Kişisel Veri Saklama Süre Tablosu ve Kişisel Veri İşleme Envanterine paralel olarak, dijital ve fiziksel ortamlarında tuttuğu kişisel verileri, periyodik olarak altı (6) ayda bir kontrol edeceğini ve işlendikleri amaç sona erdiğinde söz konusu verileri tekrar eden aralıklarla sileceğini, yok edeceğini veya anonim hale getireceğini taahhüt eder.

- Harddiskler'in imhası esnasında notebook veya desktop bilgisayardan sökülen disk, matkap aracılığı ile delinerek elektronik atığa atılır.
- CD, DVD gibi taşınabilir ortamların imhası esnasında CD ve DVD'nin yazılı olan kısmı maket bıçağıyla çizilir, yakılarak imha edilir.
- Ekonomik ömrünü tamamlayan bilgisayarlar, harddiskler, usb bellekler prosedüre uygun olarak imha edilir, elektronik atığa atılır.

- Kurum içinde tekrar kullanılması durumunda ise veri kurtarmaya imkân sağlamayacak şekilde güvenli silme işlemine tabi tutulduktan sonra kullanıma alınmalıdır.
- Kurum tarafından satın alınan kullanıcı bilgisayarlarına ait sabit diskler, veri kurtarmaya imkân sağlamayacak şekilde güvenli silme işlemine tabi tutulduktan sonra sistemlere dâhil edilmelidir.
- Kurum tarafından düzenli olarak erişilmeyen kritik veri veya sistemler ağdan çıkarılmalıdır. Bu sistemler ihtiyaç duyulmadığı durumlarda ağ bağlantısı kesilmiş olarak tutulmalıdır.
- Saklama gereksinimi sona eren kritik veri geri getirilemeyecek şekilde silinmelidir.
- Kullanım süresi dolmuş taşınabilir ortamlar veri sızıntılarını önlemek amacıyla güvenli olarak imha edilmelidir.
- Bilgi güvenliği gereksinimleri göz önünde bulundurularak, kullanımına ihtiyaç kalmayan veya farklı alanlarda kullanılacak cihazlar üzerindeki kritik veri geri döndürülemeyecek şekilde silinmelidir.
- Sanal makineler silinmeden önce, sanal makineye ait disk dosyalarına sıfır yazılmalı ve daha sonrasında kalıcı silme işlemi yapılmalıdır.
- Paylaşımlı/bulut ortamdan hizmet sağlayan servis sağlayıcılar hizmetin sonlanması durumunda hizmet alan tarafa ait profil ayarları, hizmet raporları vb. hizmete ilişkin tanımları silmelidir.
- Bulut sistemlerde barındırılan veriler, kullanımının sonlandırılması durumunda sistemlerden geri getirilemeyecek şekilde silinmelidir.

5.5. GİZLİLİK SINIFI VE BİLGİ ETİKETLEME POLİTİKASI

Üniversitemizin gizlilik ile ilgili uyması gereken bazı kurallar aşağıda belirtilmiştir. Resmi yazışmalara ilişkin usul ve esaslar kapsamında tüm bilgiler ve bu bilgileri ifade eden yazışmalar sınıflandırılmıştır.

Bilgi varlıklarına ilişkin etiketleme Kurumumuzda elektronik ortamda EBYS üzerinden yapılmakta olup; fiziksel varlıklar için dosya kodu ile etiketlemeler takip edilmektedir.

5.5.1. GİZLİLİK KURALLARI

- **Çok Gizli**: Bu verilere ilgili personel ulaşabilmektedir.

- **Gizli**: Departmanına göre müdürler ve müdürlerin görevlendirdiği sorumlular ulaşabilmektedir.
- **Hizmete Özel**: Tüm kurum personeli ulaşabilmektedir.
- **Varlık**: Varlığın önem derecesi gizlilik sınıfıyla eş değer olduğundan yaşanabilecek olası durumlarda varlıkların önem dercesine göre kurtarma işlemi yapılır.
- **Özel**: Kişisel bilgiler.

İLGİLİ DOKÜMANLAR

Devlet Kurumları Arşiv Hizmetleri Yönetmeliği