# AMAÇ

Bu prosedürün amacı, Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı içinde farklı koruma gerektiren varlıkların saptanmasını ve her aşamadaki işaretleme, koruma ve imha yöntemlerini tanımlamaktır.

Prosedür; gizlilik, önem ve ivedilik açısından farklılık gösteren varlıkların değişik aşamalarda ne şekilde ele alınacağını belirler.

# KAPSAM

Tekirdağ Namık Kemal Üniversitesi bünyesinde işlenen tüm bilgi varlıkları bu prosedür kapsamındadır.

# TANIMLAR VE KISALTMALAR

Birim: Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı

Kurum: Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı

# SORUMLULAR

Bu prosedürün hazırlanmasından BGYS Yönetim Temsilcisi sorumludur. Prosedürün uygulanması tüm Tekirdağ Namık Kemal Üniversitesi çalışanlarının sorumluluğundadır.

# UYGULAMA

## BİLGİ SINIFLARI

Kurumda Gizli, Hizmete Özel Birime Özel ve Genel olmak üzere 4 adet gizlilik sınıfı kullanılır. Bu sınıfların detayları aşağıda açıklanmaktadır:

* **Gizli:** Bilgi İşlem Daire Başkanlığı’na özel kritik ve hassas bilgi içeren veya işleyen varlıkları ifade eder. Bunlara kurum içinde ayrıca erişim denetimi uygulaması gereklidir.
* **Hizmete Özel:** Bilgi İşlem Daire Başkanlığı içinde hizmetlere özel bilgi içeren veya işleyen varlıkları ifade eder. Bunlara kurum içinde ayrıca erişim denetimi uygulaması gereklidir.
* **Birime Özel:** Bilgi İşlem Daire Başkanlığı bünyesi içinde kullanıma açık ancak kamuya (genele) açık olmayan varlıkları ifade eder. Bu varlıklar için kurum içinde doğrudan bir erişim denetimi uygulanmasına gerek yoktur. Bununla beraber, varlığın sorumlusu tarafından korunması gerekir.
* **Genel:** Kamuya (genele) açık olan bilgi ve varlıkları ifade eder. Erişim denetimi uygulanmasına gerek yoktur.

Basılı veya elektronik ortamdaki bilgilerin sınıflaması gizlilik derecesinin tanımları dikkate alınarak, varlık sahipleri tarafından yapılmalıdır.

## BİLGİLERİN ETİKETLENMESİ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Gizli | Hizmete Özel | Birime Özel | Tasnif Dışı |
| Elektronik Dokümanlar | Header kısmına işaret konur. | Doküman ve kayıt listesinde “HIZMETE ÖZEL” bilgisi belirtilir. | Doküman ve kayıt listesinde “HIZMETE ÖZEL” bilgisi belirtilir. | İşaret yok. |
| Basılı Dokümanlar | Elle Header kısmına işaret konur. | Doküman ve kayıt listesinde “HIZMETE ÖZEL” bilgisi belirtilir. | Doküman ve kayıt listesinde “HIZMETE ÖZEL” bilgisi belirtilir. | İşaret yok. |
| Taşınabilir depolama aygıtları | Aygıt üzerine işaret yazılır. | Doküman ve kayıt listesinde “HIZMETE ÖZEL” bilgisi belirtilir. | Doküman ve kayıt listesinde “HIZMETE ÖZEL” bilgisi belirtilir. | İşaret yok. |
| Mailler | Mail etiketinde işaret yazılır. | Mail etiketinde işaret yazılır. | Mail etiketinde işaret yazılır. | İşaret yok. |
| Bilgi Sistemleri | Bilgi içeren sistemler açılırken giriş işleminden sonra kullanıcılara uyarı verilir. | Bilgi içeren sistemler açılırken giriş işleminden sonra kullanıcılara uyarı verilir. | İşaret yok | İşaret yok. |

## BİLGİLERE ERİŞİM KISITLARI

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Gizli | Hizmete Özel | Birime Özel | Tasnif Dışı |
| Elektronik Dokümanlar | Kullanıcı Adı ve Parola korumalı ortamlarda tutulur.  Ek koruma önlemleri tercih edilir. | Kurum içinde kullanıcı adı ve parolaya dayalı önlem alınır. Bilmesi gereken prensibi esas alınır. | Kurum dışı ile paylaşılamaz. Kurum içinde Bilmesi gereken prensibi esas alınır. | Erişim kısıtı uygulanmaz. |
| Basılı Dokümanlar | Sorumluların kontrolünde kilitli dolaplarda tutulur. | Kurum içinde sorumluların kontrolündeki dolap ve çekmecelerde tutulur. | Kurum dışı ile paylaşılamaz. Kurum içinde Bilmesi gereken prensibi esas alınır. | Erişim kısıtı uygulanmaz. |
| Taşınabilir depolama aygıtları | Sorumluların kontrolünde kilitli dolaplarda tutulur. | Kurum içinde sorumluların kontrolündeki dolap ve çekmecelerde tutulur. | Kurum dışı ile paylaşılamaz. Kurum içinde Bilmesi gereken prensibi esas alınır. | Erişim kısıtı uygulanmaz. |
| Mailler | Gizli bilgi içeren mailler veya hesaplar kullanıcı adı ve parola ile korunur. | Kullanıcı adı ve parola ile korunur. | Kurum dışı ile paylaşılamaz. Kurum içinde Bilmesi gereken prensibi esas alınır. | Erişim kısıtı uygulanmaz. |
| Bilgi Sistemleri | Gizli bilgi içeren bilgi sistemleri, kullanıcı adı ve parola ile koruma altına alınır.  Kurum içindeki güvenli bölge içinde ikinci bir fiziksel erişim katmanı ile korunuz.  Eğer kurum dışına çıkarılacaksa, gizli verilerin şifreli olması gerekir. | Kullanıcı adı ve parola ile koruma altına alınır. | Kurum dışı ile paylaşılamaz. Kurum içinde Bilmesi gereken prensibi esas alınır. | Erişim kısıtı uygulanmaz. |

## BİLGİLERİN İLETİLMESİ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Gizli | Hizmete Özel | Birime Özel | Tasnif Dışı |
| Elektronik Veriler | Şifreli veya parola korumalı olarak iletilir. Şifre veya parola koruması sağlandıktan sonra iletim mail, depolama aygıtları gibi ortamlar üzerinden gerçeklenebilir. | Açık olarak iletilebilir. Ancak alıcıya özel ortamlarda gönderilmelidir. | Alıcıya özel olmak kaydıyla açık iletilebilir. | Bilmesi gereken prensibi esas alınır. |
| Basılı Dokümanlar | Bilgi sahibi veya güvenilir kişi tarafından elden iletilir. İletim ofis ortamında anlık yapılmayacaksa kapalı zarf içinde iletim yapılır. | Bilgi sahibi veya güvenili kişi tarafından elden iletilir. İletim ofis ortamında anlık yapılmayacaksa kapalı zarf içinde iletim yapılır. | Birim içinde genel yollarla iletilebilir. Birim dışına çıkacaksa kişiye özel iletilmelidir. | Bilmesi gereken prensibi esas alınır. |

## BİLGİLERİN DEPOLANMASI

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Gizli | Hizmete Özel | Birime Özel | Tasnif Dışı |
| Elektronik Veriler | Kullanıcı Adı ve Parola korumalı ortamlarda şifreli olarak tutulur. | Kullanıcı Adı ve Parola korumalı ortamlarda tutulur. | Kurum içinde bir güvenlik mekanizması şart değildir. Bilmesi gereken prensibi esas alınır. | Özel bir kısıt uygulanmaz. |
| Basılı Dokümanlar | Sorumluların kontrolünde kilitli dolaplarda tutulur. | Sorumluya ait dolap ve çekmecelerde tutulur. | Kurum içinde bir güvenlik mekanizması şart değildir. Bilmesi gereken prensibi esas alınır. | Özel bir kısıt uygulanmaz. |
| Taşınabilir depolama aygıtları | Sorumluların kontrolünde kilitli dolaplarda tutulur. | Sorumluya ait dolap ve çekmecelerde tutulur. | Kurum içinde bir güvenlik mekanizması şart değildir. Bilmesi gereken prensibi esas alınır. | Özel bir kısıt uygulanmaz. |
| Mailler | Kullanıcı Adı ve Parola korumalı ortamlarda şifreli olarak tutulur. | Kullanıcı Adı ve Parola korumalı ortamlarda olarak tutulur. | Kurum içinde bir güvenlik mekanizması şart değildir. Bilmesi gereken prensibi esas alınır. | Özel bir kısıt uygulanmaz. |
| Bilgi Sistemleri | Kurum içindeki güvenli bölge içinde ikinci bir fiziksel erişim katmanı ile korunuz. | Kullanıcı Adı ve Parola korumalı ortamlarda olarak tutulur | Kurum içinde bir güvenlik mekanizması şart değildir. Bilmesi gereken prensibi esas alınır. | Özel bir kısıt uygulanmaz. |

## İMHA

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Gizli | Hizmete Özel | Birime Özel | Tasnif Dışı |
| Elektronik Veriler | Üstüne yazarak silme yöntemi ile imha edilir. | Silme yöntemi ile imha edilir. | Silme yöntemi ile imha edilir. | Silme yöntemi ile imha edilir. |
| Basılı Dokümanlar | Kırpma ile imha edilir. | Elle parçalayarak imha edilir. Çöpler kurum dışına çıkacaksa kırpma ile imha edilir. | Elle parçalayarak imha edilir. Çöpler kurum dışına çıkacaksa kırpma ile imha edilir. | Elle parçalayarak imha edilir. |
| Taşınabilir depolama aygıtları | Elektronik veriler güvenle silindikten sonra tekrar kullanılabilir veya atılabilir.  Eğer verileri silmek mümkün değilse Kırpma makinası vb yöntemlerle geri dönüşüm olmayacak şekilde imha edilir. | Elektronik veriler güvenle silindikten sonra tekrar kullanılabilir veya atılabilir.  Eğer verileri silmek mümkün değilse Kırpma makinası vb yöntemlerle geri dönüşüm olmayacak şekilde imha edilir. | Elektronik veriler güvenle silindikten sonra tekrar kullanılabilir veya atılabilir.  Eğer verileri silmek mümkün değilse Kırpma makinası vb yöntemlerle geri dönüşüm olmayacak şekilde imha edilir. | Elektronik veriler güvenle silindikten sonra tekrar kullanılabilir veya atılabilir. |

# İLGİLİ DOKÜMANLAR

İlgili doküman yoktur.