1.AMAÇ

Bu politikanın amacı, Hakkari Üniversitesi çalışanlarının mesai saatleri içi veya dışında bilgisayar ekranlarını ve çalışma ortamlarını düzenli, güvenli ve gizli bilgi içermeyecek şekilde tutması ve kendilerine görevleri gereği paylaşılmış olan bilgilerin yetkisiz kullanımını engellemesi için gerekli kuralları belirlemektir.

2.KAPSAM

Bilgi İşlem Daire Başkanlığı TS EN ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi kapsamında çalışma masaları, ekranları, basılı dokümanları, belgeleri, kayıtları ve bunlardan sorumlu tüm kullanıcıları kapsamaktadır.

3.TANIMLAR VE KISALTMALAR

3.1.Bilgi Güvenliği Yönetim Sistemi (BGYS): Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, risk yaklaşımına dayalı yönetim sistemidir.

3.2.Bilgi: Hakkari Üniversitesi süreçlerinin devamlılığı için gerekli olan ve bu nedenle değeri olan, dolayısı ile uygun şekilde korunması gereken bir veridir.

3.3.Bilgi varlıkları: TS EN ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi dâhilinde Üniversitede bulunan ve bilgi güvenliği için anlam taşıyan tüm varlıklar.

3.4.Üniversite: Hakkari Üniversitesi.

3.5.Rektör: Hakkari Üniversitesi Rektörü

3.6. Kalite Yönetim Temsilcisi: Kalite Yönetim Sistemi şartlarını, gerekli proseslerin oluşturulmasını, uygulanmasını ve sürekliliğini sağlayarak, Hakkari Üniversitesi Kalite Yönetim Sisteminin performansı ve iyileştirme için fırsatlar ile ilgili üst yönetime rapor sunan, Üniversitemizde, müşteri şartlarının bilincinde olunmasını tüm çalışanlarda sağlayan, Hakkari Üniversitesi Kalite Yönetim Sistemindeki değişiklikler planlayan ve uygulayan, kalite yönetim sisteminin bütünlüğünü güvence altına alan Üniversite çalışanı

3.7.Daire Başkanı: Hakkari Üniversitesi Bilgi İşlem Daire Başkanı.

3.8.Temiz Masa: Çalışma saatleri sonunda ve kullanıcının masadan ayrılması durumunda, masaüstünde hiçbir gizli veya hassas bilginin açıkta bırakılmamasını ifade eder.

3.9.Temiz Ekran: Bilgisayar ekranlarının, kullanılmadığı zamanlarda kilitlenmesi veya kapatılması suretiyle gizli bilgilerin görüntülenmemesini ifade eder.

4.SORUMLULAR

4.1.Bilgi Güvenliği Yönetim Sistemi Komisyonu: Bu politikanın hazırlanmasından ve güncellenmesinden sorumludur.

4.2.Rektör: Politikanın onaylanması ve yürürlüğe konulmasından sorumludur.

4.3.Kalite Yönetim Temsilcisi: Politikanın Dokümanların Kontrolü Prosedürü'ne göre kontrol edilmesinden, prosedüre doküman kodu verilmesinden, prosedür revizyona uğrarsa takibinden ve revizyon numarasının verilmesinden, prosedürün güncel doküman listesine eklenmesinden ve listenin takibinden sorumludur.

4.4.Daire Başkanı: Politikanın kontrolü ve uygulanabilirliğinin sağlanmasından sorumludur.

4.5.Kullanıcı: Politikanın içinde belirtilen faaliyetlerin uygulanmasından sorumludur.

5.UYGULAMA

5.1. Temiz Masa

5.1.1.Tüm kullanıcılar kendi masalarının temizliği ve düzeninden sorumludur.

5.1.2. Kullanımı biten not kağıtları, fotokopiler, personel özlük bilgileri gibi basılı evraklar müsvedde amaçlı kullanılamaz. Bu tür dokümanların müsvedde olarak kullanılması halinde doğacak bilgi açıklıklarından kullanıcı sorumludur.

5.1.3. Kullanıcı, çalışma masasından ayrılmadan önce masa üzerini kontrol etmeli ve masaya yaklaşıldığı takdirde görülebilecek hiçbir doküman; taşınabilir bellek, CD, DVD, mobil telefon gibi veri taşıma ve depolama araçlarını ortada bırakmamalıdır.

5.1.4. Telefon, Fotokopi Makinesi, Yazıcı, Tarayıcı gibi ortak kullanılan cihazlar üzerinde bilgi, belge bırakılmamalıdır.

5.1.5. Kişisel kullanım adları ve parolalar kesinlikle kâğıt vb. ortamlara yazılı bir şekilde personel masalarında bırakılmamalıdır.

5.1.6. Personeller çalışma masalarından ayrıldığında basılı doküman ya da taşınabilir depolama aygıtları

üzerinde tutulan bilgileri güvenlikli ortamlarda (çelik kasa, kilitli dolap ve çekmeceler vb.) saklamalıdır.

5.1.7. Gizli olarak tanımlanan (sözleşme, fatura, kişisel veri içeren, şartnameler, veri dokümanları vb.) dokümanlar ve kopyaları, müsvedde olarak kullanılmayacak ve kâğıt öğütücü veya elle imha edilmelidir.

5.1.8. Kullanımı biten basılı evraklar "Veri İşleme, Kaydetme, Paylaşma, Değiştirme, Anonimleştirme ve İmha Politikası" na uygun olarak imha edilmelidir.

5.2. Temiz Ekran

5.2.1. Daire Başkanlığının tüm personeli, kendisine teslim edilen masaüstü/taşınabilir bilgisayarların amaca uygun kullanılması ve güvenliğinin sağlanmasından sorumludur.

5.2.2. Personelin çalışma saatleri dışında bilgisayarlar kapalı ya da kilitli şekilde bırakılmalıdır. Çalışma saatleri içerisinde başından ayrıldığında mutlaka bilgisayar kilitli bırakılmalıdır.(Ekran koruyucu 5-10 dk arasında devreye girmelidir ve şifre koruması olmalıdır.)

5.2.3. Bilgisayarların masaüstü ekranlarında üniversiteye ait gizlilik derecesi yüksek bilgiler, kişisel veri içeren dosyalar ve bunlara ait kısa yollar bulundurulmamalıdır.

5.2.4. Bilgisayar, telefon, yazıcı/tarayıcı, fotokopi makineleri vb. üniversite bilgi varlıklarına sadece bu cihazlardan sorumlu kişiler erişmelidir.

5.2.5. Bilginin sunulduğu sistemler, ana makineler (sunucu), bilgisayarlar vb. cihazlar yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde başıboş bırakılmamalıdır.

5.2.6. Personel bilgisayar ekranları, yetkisiz kişilerin ekranları izlemesine izin verilmeyecek şekilde konumlandırılmalıdır. Bilgisayarların masaüstündeki klasör ve dosyalar iş sürekliliği açısından düzenli tutulmalıdır.

5.2.7. Yazıcı, fotokopi makinesi, faks vb. cihazların üzerinde veya yakınındaki çöp kutularında kişisel veri bulundurulmayacaktır. Bu alanlarda kurumsal gizlilik derecesi içeren bilgi, belge, çıktı vb. bırakılmayacaktır.

5.2.8. Fotokopi cihazlarının yetkisiz kullanımı önlenmeli ve belleğinde bulunan kritik ve hassas bilgiler

silinmelidir.

6.İLGİLİ DOKÜMANLAR

6.1. Veri İşleme, Kaydetme, Paylaşma, Değiştirme, Anonimleştirme ve İmha Politikası
6.2. Dokümanların Kontrolü Prosedürü