1. AMAÇ

Bu politika, **HEKİMOĞLU DOKUM SANAYİ NAK. VE TİC. AŞ**(Şirket) tarafından yürütülen her türlü faaliyette 6698 Sayılı Kişisel Verilerin Korunması Kanunu'na (KVKK) uygun olarak Şirket ağ ve veri tabanlarına, aktif cihazların konfigürasyon ara yüzlerine, uygulamalara, elektronik ortamdaki yönetim sistem dokümanlarına, tekliflere, sözleşmelere, ihale dosyalarına, kurumsal yazışmalara, personel özlük bilgilerine ve diğer kişisel veri barındıran fiziksel ortamlara erişimi kontrol altında tutmak ve etkin biçimde korumak amacıyla hazırlanmıştır.

2. KAPSAM

Politika, Şirketin tüm çalışanlarını, dış kullanıcıları, tedarikçilerini ve ziyaretçileri kapsar.

3. POLİTİKA

3.1. Fiziksel Erişim Kontrolü

- Kişisel veri içeren ortamların güvenliği sağlanır.
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınır.
- Kritik tüm sistemler, sunucular mutlaka fiziksel olarak korumalı sistem odasında muhafaza edilir.
- Sistem odasının kapıları mutlaka kapalı tutulmalı ve erişimler biyometrik/kartlı/şifreli giriş ile yetkilendirilmiş çalışanlar tarafından yapılır.
- Erişim kontrol mekanizmasına ait günlük kayıtlar (log ve kamera vb.) saklanır ve değiştirilmeye karşı korunur.
- Sistem odasına giriş yetkisi olmayan ama bakım/onarım, danışmanlık vb. gibi amaçlarla sistem odasında çalışma ihtiyacı olan kişilere yetkili bir personel içeride bulunduğu sürece refakat eder ve giriş çıkış kayıtları tutulur.
- "Gizli" ve üzeri gizlilik derecesine sahip bilgilerin bulunduğu ofis ve odalara erişimler biyometrik/kartlı/şifreli kapı girişi ile sınırlandırılmıştır.
- "Hizmete Özel" ve üzeri gizlilik derecesine sahip bilgilerin bulunduğu ofis ve odalar yetkili bir personel içeride olmadığı zaman kilitli tutulur.
- "Gizli" ve üzeri gizlilik derecesine sahip bilgiler kilitli dolaplarda muhafaza edilir.
- Kablo bağlantıları, sistem odası sıcaklığı, sistemlerin çalışma durumları ve yedekleme sistemlerinin kontrollerinden Bilgi İşlem Birimi sorumludur.
- Son kullanıcılar kendilerine tahsis edilen bilgisayarlara fiziksel ya da yazılımsal olarak müdahale edemez.
- Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanır.

3.2. Sistem Erişim Kontrolü

- Sistem erişimlerinde mutlaka erişimlerin kısıtlanması için kullanıcı adı ve parola kontrolü kullanılmalıdır.
- Şifresiz erişilebilen sunucu, servis veya sistem bulunamaz.
- Sistemlere erişimlerde ortak hesap kullanılamaz.
- Sistemlere yapılan tüm erişimlerin günlük kayıtları (log) tutulur ve bozulmaya karşı korunur.
- Sistem yöneticisi "Administrator" ve/veya "root" gibi genel sistem hesapları kullanamaz.
- Erişim yetkileri verilirken "bilmesi gerektiği kadar prensibi" ne göre hareket edilir.
- Bilgi Sistemleri Yöneticisi rolündeki personel sistem, sunucu ve servisler üzerinde her türlü işlem için tam yetkilidir.
- Sistemlere erişim için kullanılan şifreler, **Kriptografik Kontroller ve Anahtar Yönetim Politikasın**a göre belirlenir.

3.3. Ağ Erişimi Kontrolü

- Kablosuz ağlar için güçlü parolalar belirlenir ve 6 aylık periyotlar ile güncellenir.
- Kablosuz ağlarda varsayılan ve tahmin edilen SSID isimleri kullanılmaz.
- Kablosuz ağ parolaları SSID ismini içermez.
- Kullanıcıların erişim cihazları üzerinden ağa bağlanabilmeleri Firewall üzerinden kontrol edilir.
- Kurum kullanıcısı olmayan kişiler için misafir ağı bulunmaktadır ve kurum kullanıcısı olmayanlar kurum ağına dahil edilmez. Misafir ağı kurum ağının bulunduğu ortamdan VLAN'ler kullanılarak ayrılır. Misafir erişim kayıtları (log) tutulur.
- Kablosuz ağ cihazlarına erişim sadece yetkili kişiler tarafından HTTPS, SSH ile ya da cihaz başında konsol ile yapılır, HTTP ve Telnet gibi düz metin bağlantıları olabildiğince kullanılmaz.
- Ağ cihazları erişimlerinde mutlaka tüm erişimlerin kısıtlanması için şifre kontrolü kullanılır.
- Şifresiz ya da varsayılan şifre ile erişilebilen ağ cihazı bulunmaz.
- Güvenlik duvarı üzerinden uzaktan yapılan tüm erişimlerin günlük kayıtları (log) tutulur ve değiştirilmeye karşı korunur.

3.4. Uygulama Erişim Kontrolü

- Uygulamalara erişim yetkileri, **Kullanıcı Hesap Tanımlama ve Yetkilendirme Prosedürü**nde belirtildiği şekilde yapılır.
- Kullanıcı adı ve parola kullanımı haricinde uygulamalara erişimler tanımlanmaz.

3.5. Bilgiye Erişimin Kısıtlanması

- Erişim izinlerinde kullanıcıya tanımlanması gerekenden daha fazla erişim izni tanımlanmaz.
- Hangi verinin hangi kullanıcı için olduğu belirlenir. Kullanıcıların erişim hakları Erişim Yetki Matrisinde detaylıca belirlenir.
- Kullanıcıların erişim hakları okuma, yazma, silme ve yönetme gibi yetkiler olarak düzenlenir.

- Diğer uygulamaların veriye olan erişimleri gözden geçirilir.
- Hassas bilgiler ve kişisel veri içeren sistemler için fiziksel ve mantıksal ek güvenlik önlemleri alınır**.**
- Kişisel verilere erişim yetkisi olmayan kullanıcıların, kişisel verilere erişimlerine izin verilmez.

3.6. Üçüncü Taraf Erişim Kontrolü

- Üçüncü taraf bağlantıları için yapılan gizlilik anlaşmaları ile sorumluluklar iletilir.
- Üçüncü taraf bağlantılar için ayrı kullanıcı adları oluşturulur.
- Üçüncü taraflar için oluşturulan kullanıcı hesaplarının diğer sistemlere erişimleri kısıtlanır.
- Üçüncü tarafların tüm erişimleri kayıt altına alınır.
- İşi biten tarafların hesapları pasif hale getirilir.

3.7. Uzaktan Erişim Kontrolü

3.7.1. VPN Kullanımı

- Kullanıcılara VPN hakkı verme kuralları Kullanıcı Hesap Tanımlama ve Yetkilendirme Prosedürüne göre yönetilir.
- VPN konfigürasyonu mümkünse tek yönlü şifreleme ‘one-time password authentication’ ile yapılır.
- Şirket ağına bağlanıldığında, bilgisayardan çıkan ve giren trafik sadece VPN kanalından iletilecektir.
- Şirketin VPN ağ geçitlerinin kurulması ve yönetimi sistem yöneticisi tarafından yapılır.
- Dâhili kullanıcı VPN bağlantıları (SSL VPN) süresizdir.
- Periyodik olarak yapılan kontrollerle kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların VPN hakları ivedilikle kaldırılır.
- VPN erişim kayıtları (log) tutulur ve 2 yıl saklanır.

3.7.2. Uzak Masaüstü Çalışması (RDP)

Uzak masaüstü bağlantısı VPN üzerinden yapılır. VPN üzerinden yapılan uzak masaüstü bağlantılarda aşağıdaki kurallar geçerlidir.

- Şirket ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir VPN ağına bağlı olmadıklarından emin olmalıdırlar.
- Şirket ağına standart dışı erişim isteğinde bulunan organizasyon veya kişilere Kullanıcı Hesap Tanımlama ve Yetkilendirme Prosedürüne göre geçici izin verilir.
- Teamviewer / Ammy / Real VNC vb. gibi sisteme yazabilen yardımcı programlar ile uzaktan bağlanma söz konusu olursa, Şirketin yetkili kullanıcısı karşı tarafın işini bitirmesine kadar ekranı terk edemez. Herhangi bir güvenlik ihlali halinde kullanıcı doğrudan sorumludur.

3.8. Kişisel ve Özel Nitelikli Kişisel Verilere Erişim

Bu Politika dokümanında yer alan tüm erişim ilkeleri kişisel ve özel nitelikli kişisel veriler için uygulanmaktadır.

Kişisel veri kategorilerine ve kişisel veri barındıran alanlara erişim yetkileri **Erişim Yetki Matrisi**nde belirlenmiştir.

Ayrıca "**Özel Nitelikli Kişisel Veri İşleme Prosedürü**" içerisinde özel nitelikli kişisel verilere yönelik bilgiler detaylandırılmıştır.

3. İLGİLİ DOKÜMANLAR

- Erişim Yetki Matrisi
- Özel Nitelikli Kişisel Veri İşleme Prosedürü
- Kriptografik Kontroller ve Anahtar Yönetim Politikası
- Kullanıcı Hesap Tanımlama ve Yetkilendirme Prosedürü

4. DAĞITIM

Şirket çalışanları ve ilgili taraflar ile paylaşılmaktadır.