



ERİŐİM KONTROL POLİTİKASI

KVKK_P7 VERSİYON 1.00

KARDELEN BOYA VE KİMYA SANAYİ TİCARET LİMİTED ŞİRKETİ

ERİŞİM KONTROL POLİTİKASI

1. Amaç ve Kapsam

Kardelen Boya, sunulan hizmete uygun şekilde katmanlara ayrılarak yetkilendirme yapılmış, ayrıntılı, denetlenebilir ve uygun kullanıcı erişimi sağlamak ve Bilgi Güvenliği Politikası uyarınca veri gizliliği, bütünlüğü ve kullanılabilirliğini temin ve muhafaza etmek için Şirketin kullandığı ağlarda, IT sistemlerinde ve hizmetlerinde fiziksel ve mantıksal erişim kontrolleri uygulamaktadır.

Erişim kontrol güvenli, emniyetli ve erişilebilir bir çalışma ortamı oluşturmak suretiyle Kardelen Boya'nın kullanmakta olduğu IT sistemlerinin tüm yetkili kullanıcılarının çıkarlarını ve üçüncü şahıslar tarafından sağlanan verileri korumayı amaçlamaktadır.

1.1. İşbu Politika, Kardelen Boya tarafından kullanılan IT ve elektronik haberleşme sistemlerine erişim sağlanan tüm lokasyonlarda Kardelen Boya tarafından sahip olunan ya da işletilen tüm veri, bilgi ve sistemler için geçerlidir. İşbu Politika hükümleri ayrıca Kardelen Boya IT ve elektronik haberleşme sistemlerine erişim sağlamasına izin verilen üçüncü taraf ve kurumlarla ilişkili olan üçüncü kişiler dâhil olmak üzere tüm tedarikçi, yüklenici, alt yüklenici, danışman, gönüllü, araştırma çalışmalarına eşlik eden personel, stajyer öğrenci, geçici işçiler bakımından geçerlidir. İşbu Politikada geçen Bilgi Varlığı Kullanıcısı ya da Kullanıcı ibareleri yukarıda zikredilen kişi gruplarını kapsayacak şekilde kullanılacaktır.

1.2. Şirketin kamuya açık web sitesi ve "Herkes Açık" olarak sınıflandırılan diğer bilgiler. Kardelen Boya'nın kontrolü dışındaki sistemler işbu Politika'nın kapsamı dışındadır. Şirketin idaresi altında olmayan sistemlere, kaynaklara ve uygulamalara ayrıcalıklı erişim, Kardelen Boya'nın değil, sistemin, kaynağın veya uygulama sahibinin sorumluluğundadır. Bu kaynaklara erişim yetkisi verilmesiyle ilgili yetkilendirme ve denetim süreçleri, kaynak sahiplerinin sorumluluğundadır.

2. Tanımlamalar Ve Katılımcıların Üstleneceği Görevler

2.1. Veri, bilgi ve sistemlere erişim yetkisi ancak meşru bir iş gerekliliğinin ortaya konması, erişime Bilgi Varlığı Sahibi tarafından izin verilmesi ve tüm uygulanabilir politika, usul, esas ve koşullara riayet edilmesi halinde verilebilir. İlgili kullanıcının görev değişimi, emeklilik, iş akdi ya da projenin sona ermesi gibi nedenlerle sisteme erişim sağlamasına gerek kalmadığı durumlarda tüm tanımlanan erişim ayrıcalıkları iptal edilerek bilgiye erişim yetkisinin kullanımı sonlandırılmalıdır.

2.2. Kullanıcı ayrıcalıkları, kullanıcıların diğer Kullanıcıların müşahhas faaliyetlerine veya Bilgi Sahibinin ilgili Kullanıcı için özel olarak erişim yetkisine tanımlamadığı herhangi bir veriye erişmesini veya başka şekilde müdahale etmesini engelleyecek şekilde tanımlanmalıdır.

- 2.3.Hem fiziksel hem de mantıksal varlıklara erişim hakları, en düşük erişim hakkı ve bilmesi gerekenler ilkeleri doğrultusunda verilecektir.
- 2.4.En düşük erişim hakkı prensibi belirli bir Kullanıcının yalnızca kendisine verilen görev ve yetkileri icra etmesi için gerekli olandan daha fazla erişim ayrıcalığına sahip olmamasını icap ettirir. En düşük erişim hakkı prensibinin etkin bir şekilde uygulanabilmesi için Kullanıcının yaptığı iş tanımlanmalı, icra edilen görevin yerine getirilmesi için gerekli asgari erişim ayrıcalıkları seti tespit edilmeli ve Kullanıcıya tanımlanan erişim yetkileri bahse konu asgari ayrıcalık seti ile sınırlandırılmalıdır. Tüm sistemler için erişim kontrol izinleri, yetkisiz Kullanıcıların erişimini engelleyen bir varsayılan ayarlarına tabi tutulacak ve spesifik olarak izin verilmeyen her bilgi sistemi ayrıcalığının yasaklanmasını gerektiren en az ayrıcalıklı erişim hakkı ilkesi uygulanacaktır.
- 2.5.Derinlemesine güvenlik prensibi, büyük ölçüde daha iyi koruma sağlamak için bir güvenlik savunmasının farklı türlerdeki birden çok katmanda uygulanmasını ifade eder. Ağ, donanım aygıtları, sistem yazılımı, uygulamalar ve veriler dâhil olmak üzere sistemin her katmanında erişim kontrolü gerektiren derinlemesine güvenlik prensibi uygulanacaktır.
- 2.6.Görevler Ayrılığı: Bir iş süreci öze nitelikli ya da kurumsal olarak kritik olan bilgilerin işlenmesini ihtiva ediyorsa sistem kullanıcıların görevler ayrılığı ya da diğer telafi edici kontrol mekanizmaları içermelidir. Bahse konu kontrol mekanizmaları sayesinde hiç kimse bahse konu bilgi varlıkları ya da bunlarla ilintili işlevler üzerinde tek başına yetkili olmamasını temin etmelidir. Görevler ayrılığı prensibine aykırı bir örnek olarak çek yazılması ve mali işlemlere ilişkin tarih verilerinin muhafazasını sağlayan görevlinin aynı kişi olması verilebilir. Mümkün olduğunda, özel nitelikli, hassas veya kritik bilgileri içeren bir görevi baştan sona tamamlamaktan hiçbir zaman sadece bir kişi sorumlu olmamalıdır. Aynı şekilde, bir kişi kendi işini onaylamaktan sorumlu olmamalıdır. Mümkün olduğu ölçüde, her görev için en az iki kişinin bilgi işleme faaliyetlerini koordine etmesi gerekir.
- 2.7.Kabul edilebilir Kullanım: Kullanıcı adı ve şifresi tanımlanmadan önce Kardelen Boya'nın kullandığı sistemlere bağlanmak amacıyla yetkilendirilmek isteyen her bir kullanıcı IT ve Elektronik Haberleşme Kaynaklarının Kabul edilebilir Kullanım Politikası hakkında bilgilendirilmeli ve Bilgi Güvenliği farkındalık Bildirgesini imzalaması sağlanmalıdır.
- 2.8. Şirket verilerine, bilgilerine ve sistemlerine erişim hakkı olan tüm üçüncü taraflar, Kardelen Boya tarafından halka açık olmadığı düşünülen herhangi bir bilgiyi ifşa etmekten imtina etmekle mükelleftir. Bir sözleşme, satın alma emri veya alt yüklenicilik sözleşmesi kapsamında istihdam edilen üçüncü taraflar için, Kardelen Boya ile Kardelen Boya verilerine, bilgilerine ve sistemlerine erişim izni verilen üçüncü taraf arasındaki tüm sözleşmelere ve satın alma emirlerine standart bir Gizliliği Maddesi dâhil edilecektir. Kardelen Boya'ya hizmet sağlayan (gizli verilere erişim gerektiren) ancak Kardelen Boya ile sözleşmesi olmayan tüm bireyler veya kuruluşlar için yazılı bir Gizlilik Sözleşmesi akdedilecektir.
- 2.9.Erişim Kontrolü: Erişim Kontrolü, veriye erişim sağlayan her türlü mekanizmayı ifade eder. Bilgisayarlara erişim için, Kullanıcı ilk olarak sisteme uygun bir kimlik onaylama metodu kullanarak oturum açmalıdır. Erişim kontrol mekanizması ile Kullanıcıya tanımlanan Kullanıcı adı erişim kontrol listesi ile karşılaştırılmak suretiyle

ilgili Kullanıcının hangi iş ve işlemleri gerçekleştirip gerçekleştiremeyeceği kontrol altına alınır.

Erişim kontrol sistemleri aşağıda sıralanan unsurları içerir:

- Bir dosya sunucusunda dosya oluşturma, okuma, düzenleme ya da silme gibi dosya izinleri
- Bir uygulama sunucusunda belirli bir programı çalıştırma hakkı gibi program izinleri
- Bir veri tabanından veri çekmek ya da bilgi güncellemek gibi veri hakları.

Erişim kontrol prosedürleri Bilgi Varlığı Sahiplerinin Kullanıcıların ver, bilgi ya da sistemlere erişim izinlerini onaylamak için kullandıkları metot ve uygulamaların bütünü ifade eder.

- 2.10. **Kimlik Doğrulama:** Kimlik doğrulama bir Bilgi Kullanıcısının kimlik bilgilerini tanımlamakla yetkili Bilgi Varlığı Sahibi tarafından kimlik bilgilerinin doğrulanması işlemi ifade eder. Bilgisayar sistemlerinde genellikle kimlik doğrulama işlemi, yalnızca Bilgi Kullanıcısı tarafından bilinen ve bahse konu kullanıcı için tanımlanmış olan özgün kullanıcı adı ve şifre kombinasyonunun kullanılması yoluyla gerçekleştirilir. Diğer kimlik doğrulama yöntemlerinin kullanılmasına IT Sorumlusu ve KVKK Danışmanının önerisi üzerine Genel Müdür tarafından izin verilebilir.
- 2.11. **Sistem:** Sistem, ortak işlevselliği paylaşan aynı doğrudan düzenleme kontrolü altında birbirine bağlı bir dizi bilgi kaynağını ifade eder. Bir sistem, donanım, yazılım, bilgi, veri, uygulamalar veya iletişim altyapısından ibaret olabilir. Kurumsal sistem ise devam eden iş süreçlerini desteklemek için bilgi işleyen sistemleri ifade eder. Kurumsal sistem olarak belirlenen sistemler iş gerekliliklerine göre tanımlanacak güvenlik gerekliliklerine sahip olacaktır.
- 2.12. **Bireysel Sorumluluk:** Kardelen Boya tarafından sunulan ve kullanılan elektronik kaynaklara erişim noktasında her bir kullanıcı bireysel olarak sorumludur. Bilgisayar sistemleri ve ağlara erişim için kullanıcı adı olarak bilinen her bir kullanıcı için bireysel olarak atanmış özgün bilgisayar kimlik bilgisi kullanılması zorunludur. Kardelen Boya bilgi işlem araçlarını kullanan her bir kullanıcı yalnızca yetkili olduğu kaynaklara erişim sağlayabilir. Her bir kullanıcı adı için ayrıca veri, bilgi ya da sisteme erişim esnasında kullanıcının kimliğinin doğrulanması için giriş şifresi gibi akıllı anahtar kullanılması zorunludur. Şifre bilgileri gizli bilgi olarak değerlendirilerek kimseye ifşa edilmemelidir. Her bir kullanıcı şifre bilgilerinin yetkisiz faaliyetler için kullanılmaması için gerekli olan makul güvenlik tedbirlerini almakla mükelleftir. Ayrıntılı bilgi için lütfen bkz: Kullanıcı Şifrelerinin Belirlenmesi, Kullanımı Ve Korunmasına İlişkin Usul Ve Esaslar Hakkında Yönetmelik
- 2.13. **Bilgi Varlığı Sahipleri:** Bilgi Varlığı Sahipleri korunan kaynaklara kimlerin erişebileceğini ve tanımlanan erişim ayrıcalıklarının ne olacağını (okuma, güncelleme vb.) belirlemekle görevlidirler. Bahse konu erişim ayrıcalıkları Bilgi Kullanıcısının görev sorumlulukları ile uyumlu olacaktır. Bilgi Varlığı Sahipleri idari sorumluluklarından bir kısmını mahiyetinde çalışanlara devredebilirler ancak bilgi varlıklarından nihai olarak kendileri sorumludur.
- 2.14. **Departman Şefleri:** Departman Şefleri Kardelen Boya'nın bilgi güvenliğinin sağlanmasında baş at rol oynar. Departman Şefleri iş süreçlerinin yerine getirilmesi için erişim sağlanması gerektiği durumlarda Bilgi Kullanıcıları adına sisteme erişim

taleplerini belgelendirmekle görevlidir. Görev sorumluluklarının ya da Bilgi Kullanıcısının statüsünün değişmesi halinde Kullanıcının erişim yetkilerinin değiştirilmesi ve/veya iptal işlemlerini yürütmek Departman Şeflerinin görevidir.

3. ERİŞİM KONTROLÜ USULLERİNE İLİŞKİN KILAVUZ İLKELER

- 3.1.Kardelen Boya, tüm çalışanlarının ve tedarikçi olan üçüncü tarafların Şirket tarafından kontrol edilen verilere kendilerine verilen sorumlulukları mümkün olan en etkin bir şekilde yerine getirmelerini teminen uygun erişim yetkileri sağlayacaktır.
- 3.1.1. Genel Kullanıcı Kimlikleri: genel ya da grup kimlik bilgilerinin kural olarak Kardelen Boya verilerine erişim için tanımlanmasına izin verilmez ancak yeterli kontrol mekanizmalarının sağlanması durumunda istisnai durumlarda izin verilebilir.
- 3.1.2. Her koşul altında Kardelen Boya'nın internet hizmet sağlayıcısı olmasından kaynaklanan yasal sorumluluklarını yerine getirmesi ve Elektronik Kaynakların Uygun Kullanımı Politikası hükümlerinin uygulanması amacıyla kurumsal kimlik bilgisine sahip olan kullanıcıların kimlikleri tespit edilebilir olmalıdır. Genel Kullanıcı kimlikleri ile asla gizli bilgi ya da özel nitelikli verilere erişim sağlanamaz.
- 3.1.3. Ayrıcalıklı Erişim Hakkına Sahip Hesaplar: Yerel yönetici, alan yöneticisi, süper kullanıcı, yönetici erişimi gibi ayrıcalıklı erişim haklarının tayini yalnızca Üst Yönetim tarafından uygun görülecek kullanıcılarla sınırlanacak olup var sayılan olarak bu haklar tanımlanamaz.
- 3.1.3.1. Bu tür hesapların kullanımına ilişkin yetki, yalnızca üst düzey bir yöneticinin (Departman Şefi, Genel Müdür Yardımcısı) yazılı talebi üzerine Genel Müdür tarafından açıkça sağlanacak ve belgeleneyecektir.
- 3.1.3.2. Teknik ekipler, potansiyel gizlilik ve / veya bütünlük kayıplarını önlemek için tüm ekiplere ayrıcalık hakları verilmesine karşı önlem alacaktır.
- 3.1.3.3. Ayrıcalıklı hesaplar mutlak faaliyetler için kullanılmalıdır; Programın çalıştırılması başka türlü imkânsız olmadığı sürece program kullanımı için değil, programın yüklenmesi ve sistemin yeniden yapılandırılması işlemleri ile sınırlı olarak bahse konu tanımlamalar yapılabilir.
- 3.1.4. En Az Düzey Ayrıcalık ve Bilmesi Gerekenler Prensipleri: Hem fiziksel hem de mantıksal varlıklara erişim hakları, en az erişim ayrıcalığı ve bilinmesi gerekenler ilkeleri izlenerek verilecektir.
- 3.2. Erişim Kontrol Yetkilendirmeleri
- 3.2.1. Kullanıcı Hesapları: Kardelen Boya'nın kullandığı IT kaynakları ve hizmetlerine erişim yetkisi özgün kullanıcı hesabı ve karmaşık şifrenin girilmesi ile sağlanacaktır.
- 3.2.2. Kullanıcı Hesapları, İK bilgi sistemlerinde geçerli bir personel kaydının bulunması temelinde sağlanır. Personel kaydı olmayan herhangi bir kullanıcı için, bir Departman şefi tarafından imzalanan erişim izni verilir. Varsayılan erişim yalnızca belirli bir alana, saklama ortamına ve bir e-posta hesabına erişim için kullanılabilir.
- 3.2.3. Gizli, Erişimi Kısıtlanmış ve Yalnızca Belirli bir Birim İçinde Kullanılması gereken Bilgilere Erişim ilgili yasa, ilgili taraflarla akdedilen doğrultusunda üstlenilen iş veya çalışma sorumlulukları nedeniyle ilgili bilgiye erişimi gereken yetkili

çalışanlarla sınırlı olacaktır. Bahse konu bilgilere erişim, güvenlik duvarları, ağ ayırımı, güvenli oturum açma prosedürleri, erişim kontrol listesi kısıtlamaları ve uygun görülecek sair diğer kontrollerin kullanılmasıyla kısıtlanacaktır. Erişim kısıtlamalarını uygulama sorumluluğu ilgili bilgileri işleyen birim şefleri ve IT departmanının sorumluluğunda olup işbu Politika hükümlerine uygun bir şekilde yürütülecektir. Rol tabanlı erişim denetimi yöntemi, Kardelen Boya'nın etkin dizin etki alanlarında bulunan ve Kardelen Boya tarafından yönetilen tüm dosya tabanlı kaynaklara erişimin güvenli hale getirilmesi için tatbik edilecektir.

- 3.3. Kimlik Tespiti ve Doğrulama: Kardelen Boya ağlarına bağlı olan tüm bilgisayarların erişim kontrolünün yapılabilmesi için kullanıcı adı ve giriş şifresi gibi kimlik doğrulama mekanizması ile donatılması şarttır. Çok kullanıcıli sistemler her bir kullanıcı için özgün olarak tanımlanacak kullanıcı adı ve şifreleri ile kullanıcı erişim ayrıcalığı kısıtlama mekanizmalarına sahip olmalıdır. Ağlara erişimi olup olmadığına bakılmaksızın tüm iş istasyonlarında yetkisiz erişimi engelleyecek yazılım ve donanım kontrol araçları IT Sorumlusu tarafından onaylanarak uygulamaya konulacaktır.
- 3.4. Tüm Kullanıcılar her türlü bilgi, veri ya da sisteme erişim sağlamadan önce kimlik doğrulama işlemine tabi tutulmalıdır. Bu amaçla her bir bireysel kullanıcı için özgün olarak tanımlanan kullanıcı adı ve şifresi Şirket içi ağlara erişim sağlanmadan önce talep edilecektir.
- 3.5. Kullanıcılar Kardelen Boya tarafından kullanılan sistem ve bilgi işlem kaynaklarına erişim için kullandıkları kullanıcı adı ve şifreleri özellikle internette kullandıkları hesaplar da dahil olmak üzere Kardelen Boya harici sistemlere erişim sağlamak için kullanılmaktan kaçınılmalıdır.
- 3.6. Ağ bağlantılı bilgisayar sistemlerindeki kullanıcı oturum açma ekranında sadece kullanıcıdan giriş yapmak için kullanıcı adı ve şifresini girmesini talep eden bilgiye yer verilecektir. Bilgisayar, bilgisayar işletim sistemi, ağ konfigürasyonu ya da diğer Şirkete özel bilgiler Kullanıcı geçerli kullanıcı adı ve şifresini kullanarak başarılı bir şekilde giriş yapmadan asla paylaşılmamalıdır. Oturum açma adımlarından her hangi birisi yanlış girildiği takdirde Kullanıcıya oturum açma problemi ile ilgili problemin kaynağı hakkında bilgi verilmeksizin sadece oturum açma işleminin başarısız olduğu bildirilecektir.
- 3.7. Özgün Kullanıcı Adları: Her bir kullanıcı adı tanımlandığı kullanıcı için özgün olmalı ve sadece tanımlandığı kullanıcı ile bağlantılı olmalıdır. Eğer bir Kullanıcının sisteme erişim ayrıcalıklarına son verilirse bahse konu kullanıcının kullanıcı adı tekrar asla kullanılmamalıdır. Her bir kullanıcı adı ve şifresi spesifik bir bireyin münhasır kullanımı amacıyla sınırlı olarak tanımlanmalıdır. Kullanıcı Adları elektronik posta mesajlarında ve sair ortamlarda paylaşılabilir ancak şifreler hiç kimseyle hiçbir ortamda paylaşılmayacaktır. (IT Destek ekibinin kendi erişim ayrıcalıkları var olup Kullanıcıların şifrelerine erişim sağlama ihtiyaçları bulunmamaktadır.)
- 3.8. Kullanıcı Kimlik Doğrulaması İşlemleri: Tüm kurumsal bilgi sistemleri kullanıcı adlarının tanımlı şifreleri ya da daha güçlü dinamik şifreleme yöntemi ile yalnızca yetkili Kullanıcıların kullanıcı adını istimal etmesini temin edecektir. Kullanıcılar kullanıcı adı ve şifreleri ya da diğer kimlik doğrulama mekanizmaları kullanılmak suretiyle açılan oturumlarda gerçekleştirilen tüm iş ve işlemlerden ötürü bireysel olarak sorumludurlar. Kullanıcılar oturum açma bilgilerinin ifşa olduğunu ya da üçüncü taraflarca kullanıldığını tespit ettikleri takdirde şifrelerini derhal değiştirmekle mükelleftir. Aynı şekilde Kullanıcılar oturum bilgisi ile erişim kontrol

mekanizmalarının gizliliğinin ihlal edildiğinden şüphe duydukları takdirde IT Departmanı Teknik Hizmet birimini derhal bilgilendirmekle mükelleftir. Kullanıcı adları yalnızca kendilerine tanımlanan görevliler tarafından kullanılabilir. Kullanıcılar kesinlikle diğer kişilerin kendi kullanıcı adını kullanarak her hangi bir işlem yapmasına izin vermemelidir. Aynı şekilde Kullanıcılar diğer Kullanıcılara tanımlanan kullanıcı adlarını kullanarak her hangi bir iş ve işlem yapamazlar.

- 3.9. TAŞINABİLİR BİLGİSAYAR VE SAİR CİHAZLAR: Taşınabilir dizüstü bilgisayar, İpad, note book, avuçiçi bilgisayar ve benzeri cihazlarda gizli ya da özel nitelikli veriler yukarıda açıklanan oturma açma süreçleri tarafından korunmadıkça muhafaza edilemez. Kullanıcılar bahse konu cihazların fiziki güvenliği ve içerlerinde yer alan bilgi ve belgelerin gizliliği hususunda bireysel olarak sorumludurlar.
- 3.10. TAŞINABİLİR BELLEKLER: Şirket tarafından kamuya açıklanmamış olan bilgiler yumuşak disk, manyetik teyp, akıllı kart ya da sair saklama ortamına yazılır ise bahse konu saklama ortamı ilgili en yüksek gizlilik hassasiyet düzeyine göre işaretlenmelidir. Kullanılmadıkları zaman saklama ortamları güvenli bir alanda muhafaza altına alınmalıdır.
- 3.11. Uzaktan Yazma İşlemleri: Uzaktan yazma işlemlerinde gizli ya da özel nitelikli verilerin yetkisiz kişilerce erişimine engel olmak için gerekli kontroller sağlanmalıdır. Kullanıcılar gizli kalması gereken bilgilerin güvenli bir yazıcıda yazıldığından ya da yazılan materyali incelemeye yetkili olan bir görevli gözetiminde yazma işlemi yapıldığından emin olmalıdırlar.
- 3.12. GİZLİ VE ÖZEL NİTELİKLİ VERİLERİN PAYLAŞIMI VE AKTARIMI: Kullanıcılar IT Departmanından önceden izin almaksızın mevcut yerel alan ağlara ya da diğer çoklu kullanıcı sistemlere bilgi iletimi amacıyla elektronik bellekten, yerel alan ağları, dosya alışveriş sunucusu(ftp), web sunucusu ya da modem bağlantıları KURAMAZLAR. Yalnızca IT Sorumlusu tarafından hususi olarak görevlendirilmiş özel ayrıcalıklı erişim haklarına sahip personeli bu tür servisleri kurmakla yetkilidir.
- 3.13. EKİPMAN VE SAKLAMA ORTAMLARININ İMHA VE ELDEN ÇIKARILMASI: Bilgisayar saklama ortamları takas, bakım ya da imha işlemi için bir tedarikçi firmaya gönderilecek ise tüm gizli ve özel nitelikli veriler onaylanmış yöntemler kullanılarak imha edilir ya da gizlenir.
- 3.14. ERİŞİM AYRICALIKLARININ ASKIYA ALINMASI VE İPTALİ:
- 3.14.1. Bilgi Varlığı Sahipleri muhafazası altında olan bilgi varlıklarına kullanıcı erişim ayrıcalıklarının kaldırılması için geçerli yönergeleri belirlemekle mükelleftir. Bilgi Varlığı Sahibinin görevlendireceği görevliler Bilgi Varlığı Sahibi adına kullanıcılara erişim hakkı tanınması ve tanınan hakların kaldırılması işlemlerine belirlenen yönergelerle göre yürütürler.
- 3.14.2. Departman Şefleri Kullanıcıların kendilerine tanımlanan erişim ayrıcalıklarının değiştirilmesini gerektirecek görevleri ya da istihdam durumlarında ortaya çıkan değişiklikleri gecikmeksizin raporlamakla sorumludurlar. Şirketle ilişik kesme durumunda İnsan Kaynakları Sorumlusu ilgili Kullanıcının tüm veri, bilgi ve sistemlere erişim yetkilerinin iptali süreçlerini yöneterek IT Sorumlusuna bildirecektir.
- 3.14.3. Departman Şefleri her yılda bir kez Kullanıcılara tanımlanan erişim ayrıcalıkları sistemini gözden geçirerek güncellemekle mükelleftir. Kullanıcıların erişim ayrıcalıklarının değiştirilmesi durumunda Departman Şefleri kullanıcı hesap yönetim mekanizmasında gerekli detaylı değişiklikleri gerçekleştireceklerdir.

- 3.14.4. Kullanıcının Kardelen Boya ile iliřinin kesilmesi durumunda bilgisayar yerleřik dosyaları ve kağıt ortamında manuel olarak tutulan dosyalar ilgili Departman Őefi tarafından gecikmeksizin incelenerek ilgili dosyaların kimin gőzetimine verileceđi ve/veya dosyaların imhası iin uygun yőntemler belirlenecektir. Akabinde Departman Őefi daha nce ilgili Kullanıcının kullanımına atanan dosyaların sorumluluđunu spesifik olarak yeni belirlenecek kullanıcıya delege ederek bilgisayar kullanıcısının gőrevlerini yeniden belirlemelidir.
- 3.14.5.  aylık bir sre boyunca kesintisiz olarak herhangi bir faaliyet gősterilmeyen kullanıcı kimlikleri otomatik olarak askıya alınacaktır. Bir ayı ařkın izin, geici gőrevlendirme ya da ücretsiz izin bitiminde gőrevlerine yeniden bařlayan kullanıcıların eriřim ayrıcalıkları ilgili Departman Őefi tarafından yeniden tanımlanacaktır.
- 3.14.6. Oturum: Bir iř istasyonunda yirmi dakika boyunca her hangi bir aktivite gőrlmemesi halinde sistem otomatik olarak ekranı karartarak oturumu sonlandırmalıdır. Oturumun yeniden aılmasına ancak ilgili kullanıcının geerli Őifre bilgilerini girmesi durumunda izin verilmelidir.
- 3.14.7. Őifre Yőnetimi: Őifreler, eriřim kontrol listeleri ve sair eriřim kontrol bilgileri depolanırken ya da ađ zerinde aktarılırken Őifrelenmelidir. Depolanan Őifre ve eriřim kontrol bilgilere yetkisiz eriřim sađlanması ve sz konusu bilgilerin kullanılmasını nlemek iin gerekli kontroller sađlanmalıdır.
- 3.14.8. Őifrelerin gerektiđinde deđiřtirilebilmesi iin Őifreler kullanılan yazılım ya da uygulamalara dođrudan gmlmemelidir(hard code).
- 3.14.9. Yeni kullanıcıya verilen Őifreler ilgili kullanıcının yalnızca ilk oturum ama iřlemi iin geerli olmalıdır. Oturum aıldıktan sonra Kullanıcı bařka bir Őifre belirlemek zorundadır. Aynı usul Kullanıcının Őifresini unuttuđu durumlarda Őifrenin resetlenmesi iřlemlerinde de uygulanacaktır.
- 3.14.10. Tedarikilerden temin edilen cihazlarda mevcut olan var sayılan Őifreler ilgili ekipman ilk kullanıma bařlamadan nce deđiřtirilmelidir. Bu prosedr son kullanıcı kimlik bilgilerinin yanı sıra sistem yőneticisi ve diđer ayrıcalıklı kullanıcı kimlikleri iin de geerlidir.
- 3.14.11. Kullanıcılar kendilerine bireysel olarak atanan kullanıcı hesabına iliřkin Őifreleri birim Őefleri ve alıřma arkadařları dahil olmak zere kimseyle paylařmamalıdır. Dosya ve bilgi paylařımı iin Kullanıcılar yerel ađ paylařımlı dizinleri, elektronik posta, intranet sayfaları ya da flopi disk gibi IT Departmanı tarafından onaylanarak izin verilen mekanizmaları kullanmalıdır.
- 3.14.12. **Sistem Geliřtirme:** Ařađıda aıklanan standartlar kurumsal olarak retilen verilerin yetkisiz personelin eriřimine aılmasını nlemek ve uygulamaların btnlđn geliřtirmek iin kullanılacaktır.
- Kurumsal Veri, Geliřtirme ve Test Sistemlerinin Ayrılması: Kurumsal iř sreleri nihayetinde retilen veriler ile geliřtirme ve test ortamları birbirinden ayrılmalıdır. Bu sayede kurumsal bilgilerin daha iyi bir Őekilde korunması temin edilebilir. Geliřtirme ve test ortamlarında alıřan personelin ilke olarak kurumsal sistemlere eriřimine izin verilmez. Yalnızca Departman Őefleri geliřim srelerinde alıřanların kurumsal verilere eriřimine izin verebilir. Benzer Őekilde tm kurumsal yazılım testlerinde gizli ve zel nitelikli bilgi ve verilerin yerine sahte verilerin kullanıldıđı ayıklanmıř veriler iřlenmelidir. Kurumsal sistem ve bilgilerin

değiştirilmesinin kısıtlanması ve onaylanması için resmi ve belgelendirilmiş değişim kontrol süreçleri kullanılmalıdır.

Yazılım Geliştirme: Yazılımın kurumsal kullanıma sokulmasından önce program geliştirici ve sair teknik personel erişimin yalnızca normal güvenli yollardan sağlanmasını temin etmek üzere tüm özel erişim yollarını ortadan kaldırmalıdır. Dolayısıyla sistem güvenliğini ihlal etmek için kullanılabilir tüm gizli kapı yazılım ve sair kısa yollar kaldırılmalıdır. Bilgi Güvenliği Politikaları ve yönetmeliklerde ön görülen her türlü kullanıcı düzeyi ve yönetici düzeyi erişim kontrol prosedürleri geliştirilen sistemler kurumsal kullanıma sunulmadan önce tanımlanarak etkin hale getirilmiş olmalıdır.

Ortam Taşıma Kontrolleri: Yazılımların geliştirme ve test aşamalarını tamamlamasından sonra nihai olarak kurumsal platformlara taşınması süreçlerinin düzenli ve kontrollü bir şekilde gerçekleştirilmesi için uygun bir metodoloji uygulanmalıdır. Uygulama geliştirme personeli kurumsal bilgi üretim ortamlarına doğrudan yazılım yükleme yetkisine sahip olmamalıdır. İzin verilmeyen uygulama kodlarının kurumsal bilgi üretim ortamına taşınmasını önlemek için gerekli kontroller yapılmalıdır.

Kurumsal bilgi üretim süreçlerinde değişiklik getirecek erişim ayrıcalıkları kurumsal bilgi üretim uygulamaları ile sınırlı olmalıdır. Ayrıcalıklar tanımlanırken sistem kullanıcılarının sistem verilerini kısıtlamasız bir şekilde değiştirebilmelerine izin verilmemelidir. Kullanıcılar kurumsal verileri sistemlerinin bütünlüğünün korunarak güçlendirilmesi için sadece daha önceden tanımlanan biçimlerde değişiklik yapabilmelidirler. Kurumsal veri tabanlarında yapılacak güncellemeler Üst Yönetim tarafından onaylanan belirlenmiş yöntemler kullanılarak yapılmalıdır. Kurumsal bilgi üretim ortamında direkt veri tabanı erişim araçlarının kullanımına bahse konu programların veri tabanı senkronizasyonu ve tıpkılama yordamları, girdi hatası kontrol rutinleri ve diğer önemli kontrol mekanizmalarını ihlal edebilecek olmaları nedeniyle izin verilmemelidir.

Loglar ve Diğer Güvenlik Araçları: Gizli ya da özel nitelikli veri ihtiva eden bilgisayar ve iletişim sistemleri kayda değer tüm güvenlikle ilgili olayları kaydetmelidir. Güvenliği ilgilendiren olaylara örnek olarak şunlar sıralanabilir:

Çevrim içi oturum esnasında kullanıcıların kullanıcı kimlik bilgilerini değiştirmeleri, şifreleri tahmin etme girişimleri, yetkilendirilmemiş erişim ayrıcalıklarını kullanma girişimleri, kurumsal uygulama yazılımlarının değiştirilmesi, sistem yazılımlarına getirilen değişiklikleri kullanıcılara tanımlanan ayrıcalıkların değiştirilmesi ve loglama alt sistemlerinin değiştirilmesi.

IT Sorumlusu erişim güvenliğini ilgilendiren gelişmeler, olaylar, durumlar, politikalara uyum düzeyi, değişiklikler ve sair hususlarda Üst Yönetime düzenli olarak rapor sunacaktır.

Raporlanması Gereken Durumlar: Yetkisiz erişim ya da erişim teşebbüsleri, şifre ya da erişim kontrollerinin çalınması ya da ifşa edilmesi, veri kaybı, değişimi ya da ifşa olunmasından şüphelenen durumlar, güvenlik standartları, prosedürleri ya da politikalarının ihlal edilmesi durumları derhal en yakın birim şefi ya da IT Teknik Destek ekibine Veri İhlali Müdahale Planında yer alan form doldurulmak suretiyle derhal rapor edilecektir.

4. Fiziki Eriřim Kontrolü: Kardelen Boya tarafından kullanılan tesisler içerisinde bulunan kaynak ve verilerin hassasiyeti nedeniyle eriřim kısıtlaması getirilmesi durumunda eriřim kontrolü öncelikle RFID teknolojisi kullanılan Kardelen Boya Kimlik Kartları aracılıđıyla sađlanacaktır. Sistem odası ve AR-GE verilerinin bulunduđu alana eriřim için ayrıca parmak izi tanıma sistemleri Genel Müdürden önceden yazılı izin alınmak suretiyle kullanılabilir. Kart ve parmak izi tanıma sistemleri yalnızca eriřimin yetkili personel ile kısıtlandıđı alanlara eriřim sađlanması amacıyla kullanılabilir olup personelin mesai saatlerine uyumunun takibi amacıyla kesinlikle kullanılamaz.

4.1.Kardelen Boya kimlik kartlarının kaybolması durumunda durum derhal IT Sorumlusuna bildirilir. IT Sorumlusu derhal ilgili kartın Őirketin fiziki eriřim kontrol sisteminden silinmesini sađlar. Kaybolan kart yerine ikame edilecek kart ancak kayıp kartın iptal işleminden sonra yerine getirilir. İkame için verilen kartta eskisi ile aynı eriřim yetkileri tanımlanır.

4.2.Eriřim Kontrol Sistemlerinde Tutulacak Veriler: Őirketin Eriřim Kontrol Sistemi ile ilgili olarak tuttuđu veriler Őunlardır:

• Kart Hamiline İliřkin Veriler:

- İsim ve Soy isim
- Görev Unvanı
- Çalıştıđı Birim
- E-Mail Adresi
- Çalışan sicil numarası
- Cep Telefonu

• Kart Hamiline Tanımlanan Kartlar

• Kart okuma işlemlerinin gerçekteđi lokasyon, tarih ve saat

4.2.1. Eriřim kontrol verilerine görevleri geređi eriřim kontrol yazılımlarına eriřmek durumunda olan görevliler eriřim sađlayabilir. Bahse konu görevliler Őunlardır:

- Güvenlik Görevlileri
- Giriř kartı veren ya da kartları deđiřtirme ve imha işlemlerini gerçekteřtiren teknik personel
- IT Teknik Destek Personeli

4.2.2. Verilerin eriřim kontrol sisteminden talep eden alıcıya aktarılacađı durumlarda, işbu Politikada belirtilen usullere uygun olarak, pratik olarak mümkün olduđunda, verileri belirli bir kiřiye ait olarak tanımlanabilir kılan tüm alanlar kaldırılmalıdır. Örneđin, belirli bir süre içinde kaç kiřinin bir okuyucu kullandıđı bilinmek isteniyorsa, raporda kart sahiplerinin adlarını, fotođraflarını veya diđer kiřisel bilgileri ifřa etmek gerekmeyecek olup sadece kart okuması işlemine iliřkin veri aktarılacaktır.

4.3.Eriřim Kontrol Yöntemleri

Verilere eriřim, veri sınıflandırma seviyelerine göre ařađıda sıralanan yöntemler kullanılarak çeřitli řekillerde sađlanır.

Varsayılan olarak kullanılan eriřim kontrol yöntemleri Őunları ięerir:

- Cihazlarda açık oturum açma,
- Windows paylaşım ve dosya ve klasörlere dosya izinleri,
- kullanıcı hesabı ayrıcalık sınırlamaları,

- sunucu ve iş istasyonu erişim hakları,
 - güvenlik duvarı izinleri,
 - ağ bölgesi ve VLAN erişim kontrol listeleri,
 - Intranet / extranet kimlik doğrulama hakları,
 - Kardelen Boya kullanıcı oturum açma hakları,
 - Veri tabanı erişim hakları ve erişim kontrol listeleri,
 - Beklemede ve hareket halindeyken şifreleme
 - İlgili taraflarca sözleşmenin gerektirdiği diğer yöntemler
- 4.4.Erişim kontrolü, Kardelen Boya'nın sahip olduğu tüm ağlar, sunucular, iş istasyonları, dizüstü bilgisayarlar, mobil cihazlar için geçerlidir.
- 4.5.Rol tabanlı erişim denetimi, Kardelen Boya'nın aktif dizin etki alanlarında bulunan tüm dosya tabanlı kaynaklara erişimi güvenli hale getirme yöntemi olarak kullanılacaktır.
- 4.6.Sızma(penetrasyon) Testleri: Kardelen Boya'nın erişim kontrol mekanizması, mevcut kontrollerin etkinliğini tespit etmek ve herhangi bir zayıflığı ortaya çıkarmak için düzenli olarak sızma testlerine tabi tutulacaktır. Testler, uygun olduğu ve mutabık kalınan durumlarda bulut hizmeti sağlayıcılarının sistemlerini de içerecektir.



ERİŐİM KONTROLÜ VERİLERİ İLE İLGİLİ TALEPLER İÇİN GEÇERLİ SÜREÇ AKIŐI

Eriőim talebi teknik personele bildirilir.

Eriőim Kontrol Verisi Talep Formunun doldurulması talep eden makamdan istenir

Form elektronik ya da kağıt ortamında izin verecek makama sunulur.

İZİN VERECEK MAKAM

1.Genel Müdür

2.Genel Müdür Yardımcısı

İzin verecek makam tarafından onay ve ret kararı yazılı olarak bildirilir

Talep edilmeyen/ gerekli olmayan veriler avıklanarak ilgili veri sistemden alınarak

Veri erişim talebi olay defteri ve/veya log kayıtlarına işlenir.