BİLGİ GÜVENLİĞİ VE VERİ KORUMA POLİTİKASI

DCS

Uyum Programı

Bilgi Güvenliği ve Veri Koruma Politikası

1 Amaç

DCS Bilgi Güvenliği ve Veri Koruma Politikası, DCS bünyesindeki bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini korumaya yönelik önlemleri ve sorumlulukları ana hatlarıyla belirler.

Bu politika, yürürlükteki veri koruma mevzuatına tam uyumu sağlamayı amaçlar ve kişisel, özel nitelikli ve müşteri verilerinin güvenli bir şekilde işlenmesi için güvenilir bir ortam oluşturur.

Politikanın hiçbir maddesi şirketin tabi olduğu ilgili yasalar ile çelişemez.

2 Kapsam

Bu politika, ISO/IEC 27001:2022 Uluslararası Bilgi Güvenliği Yönetimi standardında belirtilen kontrol yönergelerine dayanmaktadır.

Politika şirketin tüm çalışanları, yüklenicileri, danışmanları, üçüncü taraf ortakları ve DCS'in bilgi sistemlerine veya verilerine erişimi olan diğer tüm kişi veya kuruluşlar için geçerlidir.

Elektronik, fiziksel ve sözlü dahil olmak üzere her türlü verinin yanı sıra bu verileri yönetmek, saklamak veya iletmek için kullanılan tüm sistem ve süreçleri kapsar.

İş süreçleri ve tüm ilgili prosedürler bu politikaya uygun olarak hazırlanır, uygulanır ve denetlenir.

3 Tanımlar

Bilgi Güvenliği: Bilginin gizliliğine, bütünlüğüne ve kullanılabilirliğine yönelik riskleri azaltarak bilgiyi koruma uygulaması.

Bilgi Sistemi: Şirketin sahip olduğu ya da korumakla yükümlü olduğu tüm sunucuları, istemcileri, ağ altyapısını, verileri ve bilgisayar bileşenlerini içerir. Bilgi sistemlerinin kullanımı, aynı zamanda internet erişimi, e-posta hizmeti gibi iç ve dış servisleri de içerir.

Bilgi Varlıkları: Bu politika özelinde, bilgi sistemleri, yazılı dokümanlar, ekipman, telefonlar, taşınabilir bilgisayarlar, saklanan veri gibi varlıklardır.

Veri Koruma: Kişisel verileri yetkisiz erişim, kullanım, ifşa veya imhaya karşı korumak için yasal ve düzenleyici önlemler.

Kişisel Veriler: İsimler, iletişim bilgileri, kimlik numaraları ve finansal bilgiler gibi tanımlanmış veya tanımlanabilir bir bireyle ilgili her türlü bilgi.

Gizli Bilgiler: Ticari sırlar, iş stratejileri ve diğer hassas veriler dahil olmak üzere DCS'e veya müşterilerine özel bilgiler.

Veri İhlali: Verilere yetkisiz erişim, ifşa, değiştirme veya imha ile sonuçlanan bir güvenlik olayı.

4 Politika Beyanları

4.1 Genel Bilgi Güvenliği

DCS, bilgi varlıklarını yetkisiz erişim, kullanım, değişiklik, ifşa veya imhaya karşı korumayı taahhüt eder. Bu kapsamda tüm çalışanlar, bilgi güvenliği politikalarına uymak ve gerekli güvenlik önlemlerini uygulamakla yükümlüdür.

Bilgi varlıkları yalnızca şirket faaliyetlerinin yürütülmesi amacıyla kullanılmalıdır. DCS'in bilgi sistemlerine ve verilerine erişim, rol ve iş gereksinimlerine göre sınırlandırılır; yalnızca yetkili kişilerin ilgili bilgilere erişimi sağlanır.

Tüm bilgi varlıklarının, varlık envanterinde tanımlanmış bir sahibi bulunur. Varlık sahibi, ilgili varlığın gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunmasından sorumludur. Bilgi sistemlerini kullanan kişiler, yalnızca kendilerine varlık sahibi tarafından tanımlanmış yetkiler kapsamında bilgi varlıklarına erişebilir. Bu yetkiler, yalnızca verildiği amaca uygun şekilde kullanılmalıdır.

Hassas sistemlere veya verilere erişim sağlanmadan önce, kullanıcı kimliğinin doğrulanması zorunludur. Bu doğrulama sürecinde çok faktörlü kimlik doğrulama (MFA) gibi güçlü yöntemlerin kullanılması gereklidir.

4.2 Yasaklanan Eylemler

Kullanıcı Hesap Kısıtlamaları:
Kullanıcılar, bilgi güvenliği önlemlerini atlatmaya, etkisiz hale getirmeye veya devre dışı bırakmaya yönelik herhangi bir girişimde bulunamazlar.

Kullanıcılar, doğrudan ya da dolaylı yoldan, erişim yetkilerini başkalarıyla paylaşamaz veya başka bir kişinin bu yetkileri kullanmasına izin veremez. Örneğin; kullanıcı adı ve şifre gibi kimlik bilgileri kesinlikle üçüncü kişilerle paylaşılmamalıdır.

Her kullanıcı hesabı, yalnızca ilgili personele özeldir ve bu hesaptan gerçekleştirilen tüm erişim ve işlemlerden, hesabın sahibi sorumludur.

Yazılım Kurulum Kısıtlamaları
Kullanıcılar, doğrudan veya dolaylı olarak şirket bilgisayarlarının işletim sistemi üzerine herhangi bir yazılım kuramazlar. Yazılım kurulumu gerektiren durumlarda, ilgili personel ihtiyacını ve gerekçesini açıkça belirterek, bağlı olduğu yöneticisi aracılığıyla Bilgi Teknolojileri birimine e-posta yoluyla talepte bulunmalıdır.

Yapılan talep, Bilgi Teknolojileri ile üst yönetim tarafından değerlendirilir. Uygun görüldüğü takdirde, gerekli lisanslar temin edilir ve yazılım kurulumu yalnızca Sistem Destek Uzmanı tarafından gerçekleştirilir.

Kullanıcılar, kendilerine zimmetlenmiş bilgisayarlarda, işletim sistemiyle birlikte gelen yazılımlar haricinde kurulu olan tüm yazılımların listesini her yıl düzenli olarak Bilgi Teknolojileri birimine bildirmek ve onay almakla yükümlüdürler.

4.3 Veri Koruma Uyumluluğu

DCS, ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi Standardı'na, Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), Kişisel Verilerin Korunması Kanunu (KVKK) ve ilgili yerel mevzuatlar da dahil olmak üzere yürürlükteki tüm veri koruma yasa ve yönetmeliklerine tam uyum sağlamayı taahhüt eder. Bu kapsamda, kişisel verilerin yasal, adil ve şeffaf bir şekilde işlenmesi esastır.

Kişisel veriler yalnızca açıkça tanımlanmış ve meşru amaçlar doğrultusunda toplanacak ve işlenecek olup, bu amaçlarla bağdaşmayan herhangi bir şekilde kullanılmayacaktır.

DCS, kişisel verilerin işlenmesiyle ilgili risklere uygun bir güvenlik düzeyi sağlamak için uygun teknik ve organizasyonel önlemleri uygulayacaktır. Kişisel verilerin yer aldığı tüm iş süreçleri, bu Politika, **“Kişisel Verilerin Korunması ve İşlenmesi Politikası”** ile **“Kişisel Verilerin Silinmesi, İmha Edilmesi ve Anonimleştirilmesi Politikası”** hükümlerine uygun şekilde yürütülür.

4.4 Veri Toplama ve Kullanma

DCS, yalnızca meşru iş amaçları doğrultusunda veya yasal yükümlülükler kapsamında gerekli olan kişisel verileri toplayacaktır. Veri sahipleri, verilerin toplanma amacı ve bu verilerin nasıl işleneceği konusunda açık ve anlaşılır şekilde bilgilendirilir.

Toplanan kişisel verilerin doğru, eksiksiz ve güncel olması esastır. Yanlış ya da güncelliğini yitirmiş veriler tespit edildiğinde, derhal düzeltilmeli veya silinmelidir.

Kişisel veriler, yalnızca toplandıkları amaca ulaşmak için gerekli olan süre boyunca ya da ilgili mevzuatın öngördüğü süre kadar saklanacaktır.

Kişisel verilerin işlenmesine ilişkin ilke, usul ve detaylar **Kişisel Verilerin Korunması ve İşlenmesi Politikası**'nda ayrıca düzenlenmiştir.

4.5 Veri Depolama ve Güvenlik

Elektronik veya fiziksel ortamda depolanan tüm veriler, yetkisiz erişim, kayıp, bozulma veya imhaya karşı uygun yöntemlerle korunmalıdır. Bu koruma; şifreleme, erişim kontrolleri ve güvenli fiziksel depolama alanlarının kullanımı gibi güvenlik önlemlerini içerir.

Kişisel veriler, gizli bilgiler ve diğer hassas veri türleri, gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak amacıyla güvenlik politikalarına uygun biçimde saklanmalıdır. Bu tür verilerin korunması için özellikle şifreli depolama yöntemleri tercih edilmelidir.

Veri kaybı, sistem arızası veya benzeri olaylar karşısında verilerin erişilebilirliğini sürdürmek amacıyla, kritik verilerin düzenli aralıklarla yedeklenmesi zorunludur. Yedekleme süreçleri, test edilmeli ve gerektiğinde hızlıca geri yükleme yapılabilecek şekilde yapılandırılmalıdır.

4.6 Veri Erişimi ve Gizliliği

KKişisel verilere ve gizli bilgilere erişim, yalnızca görev tanımı gereği bu bilgilere ihtiyaç duyan yetkili kişilerle sınırlandırılmalıdır. Bu ilkenin etkin biçimde uygulanabilmesi için rol tabanlı erişim kontrolleri ve gerekli teknik önlemler devreye alınacaktır.

Tüm çalışanlar, iş sözleşmelerinin bir parçası olarak DCS'e ait bilgi varlıklarının gizliliğini anladıklarını ve korumayı taahhüt ettiklerini beyan eden gizlilik sözleşmeleri imzalamakla yükümlüdür.

Çalışanlar, kişisel verileri veya gizli bilgileri, DCS içerisinde veya dışında, yetkisiz kişi ya da taraflarla hiçbir koşulda paylaşmamalıdır. Bu yükümlülük, çalışanların görev süreleri sona erdikten sonra da geçerliliğini korur.

4.7 Veri Paylaşımı ve Aktarımı

Şirkete ait veriler, kişisel veriler ve gizli bilgiler üçüncü taraflarla paylaşılırken, veri güvenliğini sağlamak amacıyla veri işleme sözleşmeleri, gizlilik hükümleri ve diğer uygun koruma önlemleri mutlaka uygulanmalıdır.

Uluslararası veri aktarımları, yürürlükteki veri koruma mevzuatına tam uyum içinde gerçekleştirilmelidir. Bu tür aktarımlar sırasında, verilerin güvenliğini sağlamak üzere gerekli teknik ve idari tedbirler alınmalı, verilerin yeterli koruma düzeyine sahip ülkelere aktarılması sağlanmalıdır.

Kişisel verilerin paylaşımı ve aktarımına ilişkin ilke ve prosedürler, Kişisel Verilerin Korunması ve İşlenmesi Politikası'nda ayrıntılı olarak tanımlanmıştır.

4.8 Verilerin İmhası

Şirkete ait veriler, kişisel veriler veya gizli bilgiler, saklama süreleri dolduğunda veya işleme amaçları sona erdiğinde, ilgili yasa ve düzenlemelere uygun yöntemlerle imha edilmelidir. Verilerin kalıcı olarak erişilemez hale getirilmesini sağlamak amacıyla, fiziksel imha, dijital veri silme veya maskeleme gibi uygun imha yöntemleri uygulanmalıdır.

Verilerin anonim hale getirilmesi gerektiğinde, kimlik bilgilerinin geri döndürülemez şekilde ayrıştırılması sağlanmalı ve anonimleştirme işlemi, yasal gereksinimlere uygun olarak gerçekleştirilmelidir.

Kişisel verilerin imhası ve anonimleştirilmesine ilişkin detaylar Kişisel Verilerin Silinmesi-İmha Edilmesi ve Anonimleştirilmesi Politikası'nda düzenlenmiştir.

4.9 Şifre Kullanımına İlişkin Veri Güvenliği Önlemleri

Kullanıcılar şifrelerle ilgili olarak aşağıdaki hususlara uymakla yükümlüdür;

- Şifreler, sistem yöneticileri ve şirket yöneticileri dahil hiç kimseyle paylaşılmamalıdır.
- Şifreler, sadece zorunlu hallerde erişimi sınırlı ve kilitli bir ortamda, kapalı zarf içinde saklanabilir, bunun dışında yazılı olarak bulundurulmamalıdır.
- Şifreler, iş süreçlerinin ilgili ve yetkili çalışanlarca yürütülebilmesini teminen, güvenirliği Bilgi Teknolojileri tarafından onaylanmış "Vault" yazılımları ile saklanabilir ve yönetilebilir. İlgili "Vault" yazılımının güvenliği ve yönetilmesinden Bilgi Teknolojileri sorumludur.
- Şifreler minimum ayda bir kez olmak üzere değiştirilmelidir.
- Şifreler, sistem ya da şifrelerin ele geçirildiğinden ya da geçirilmesi ihtimalinden şüphelenildiğinde değiştirilmelidir.

Aşağıdaki kriterlere göre güçlü̈ şifreler seçilmelidir;

- En az 8 karakterli olmalıdır.
- Karakterlerden en az bir tanesi rakam olmalıdır (1234567890 gibi)
- Karakterlerden en az bir tanesi büyük harf, en az bir tanesi küçük harf olmalıdır (Aa gibi)
- Şifreler, düz ya da ters okunduğunda hiçbir dilin sözlüğünde bulunan anlamlı kelimelerden oluşmamalıdır (kedi, idek, cat, tac gibi)
- Kişisel bilgi içeren şifre kullanılmamalıdır (doğum tarihi, adres, aileden birinin adı, tuttuğu takım gibi)
- Geçmişe dönük en az 3 şifre yeniden kullanılmamalıdır.
- Şifreler ilk kez kullanıldığında değiştirilmelidir.
- Şifreler, şifremi hatırla gibi yöntemlerle kaydedilmemelidir.
- Kişisel amaçla kullanılan şifreler iş amacıyla kullanılmamalıdır.
- Şifreler 10 defa yanlış girildiğinde kullanıcı hesabı bloke olacaktır.

4.10 İnternet Kullanımına İlişkin Veri Güvenliği Önlemleri

İnternete sadece kurumun lokal ağından ve güvenlik duvarı gibi önlemlerin uygulandığı bir altyapıyla erişilir. Modemler, mobil internet, kablosuz ağ vb. cihazlarla internete direkt erişim yasaktır.

DCS, gerek görmesi halinde, kullanıcıların bireysel, grup erişimi ya da toplu olarak internete erişiminde bazı sayfaları engelleme yetkisine sahiptir. Kullanıcılar, engellenen web sayfasına erişim yetkisi taleplerini, talebin gerekçesini de belirterek Bilgi Teknolojileri'ne yazılı olarak iletirler. Kullanıcılar bu önlemi hiçbir şekilde devre dışı bırakamazlar.

4.11. İçeriden Öğrenilen Bilginin Ticareti

DCS, içeriden bilgi ticaretine (insider trading) karşı sıfır tolerans ilkesini benimsemektedir. İçeriden öğrenilen bilginin kapsamı Türk hukukunda ele alındığı gibi sermaye piyasası araçlarını etkileyebilecek nitelikteki bilgilerle sınırlı tutulmaz ve geniş yorumlanır. Finansal performans bilgileri, stratejik plan ve projeler, müşteri ve tedarikçi bilgileri, birleşme, devralma ve işbirliği anlaşmaları vb. kapsamındaki bilgilerin menfaat karşılığı paylaşılması veya kullanılması içeriden bilgi ticareti kapsamına girmektedir.

Çalışanların, görevleri veya yetkileri kapsamında eriştikleri gizli, finansal veya ticari bilgileri, kişisel veya üçüncü kişilere kazanç sağlamak amacıyla kullanmaları kesinlikle yasaktır. Şirket, içeriden bilgi ticaretini önlemek için tüm çalışanlarını, iş ortaklarını ve ilgili tarafları kapsamlı şekilde bilgilendirmeyi ve gerekli önlemleri almayı taahhüt eder.

4.12 Vaka Müdahalesi ve Veri İhlalleri

DCS, veri ihlallerini ve diğer güvenlik olaylarını ele almak için bir olay müdahale planı bulunduracaktır. Bu plan, ihlalin etkisini kontrol altına almak ve hafifletmek için atılacak adımların yanı sıra, yasaların gerektirdiği şekilde etkilenen tarafları ve düzenleyici makamları bilgilendirme sürecini ana hatlarıyla belirleyecektir.

Çalışanlar şüpheli veri ihlallerini veya güvenlik olaylarını derhal BT Güvenlik ekibine veya Veri Koruma Görevlisine (DPO) bildirmelidir.

DCS, herhangi bir veri ihlalinin nedenini belirlemek, etkisini değerlendirmek ve gelecekteki olayları önlemek için düzeltici önlemler uygulamak üzere kapsamlı bir soruşturma yürütecektir.

4.13 Çalışan Eğitimi ve Farkındalığı

Tüm çalışanlar, işe alım süreçlerinin bir parçası olarak bilgi güvenliği ve veri koruma konularında temel eğitim alacaktır. Bu eğitimler, görev süresi boyunca belirli aralıklarla verilen tazeleme eğitimleri ile desteklenecek ve güncel tutulacaktır.

Eğitim programları; verilerin güvenli biçimde işlenmesi, bilgi güvenliği ihlallerinin veya şüpheli durumların tanınması ve raporlanması, ayrıca yürürlükteki veri koruma mevzuatına uyum gibi konularda en iyi uygulamaları içerecektir.

Bu eğitimlerle çalışanların bilinç düzeyinin artırılması ve güvenlik kültürünün kurum genelinde yerleşmesi hedeflenmektedir.

5 Sorumluluklar

5.1 Çalışanlar ve Yükleniciler

- Bu politikaya uymak ve bilgi güvenliği ve veri koruma ile ilgili tüm prosedürleri izlemek
- Tüm güvenlik olaylarını veya şüpheli ihlalleri derhal BT Güvenlik Ekibi'ne veya Veri Koruma Görevlisi (DPO) bildirmek
- Kişisel verilerin ve gizli bilgilerin bu politikaya uygun olarak ele alınmasını ve korunmasını sağlamak

5.2 BT Güvenlik Ekibi

- DCS'in bilgi sistemlerini ve verilerini korumak için güvenlik önlemlerini uygulamak ve sürdürmek
- Olası güvenlik tehditlerine karşı sistemleri izleyin ve olaylara zamanında müdahale etmek
- Çalışanlara en iyi bilgi güvenliği uygulamaları konusunda rehberlik ve destek sağlamak

5.3 Veri Koruma Görevlisi (DPO)

- DCS'in veri koruma stratejisini denetlemek ve geçerli veri koruma yasalarına uyulmasını sağlamak
- Veri sahibi taleplerini ele almak ve veri ihlallerine verilen yanıtları yönetmek
- Bu politikaya uyumu değerlendirmek ve iyileştirme alanlarını belirlemek için düzenli denetimler gerçekleştirmek

6 İzleme ve Uyum

Bu politikaya uyumu sağlamak ve DCS'in bilgi güvenliği uygulamalarındaki olası güvenlik açıklarını belirlemek için düzenli denetimler ve değerlendirmeler yapılacaktır.

Bilgi sistemleri ve/veya verilerle temas halinde bulunan, kapsam dahilindeki tüm personel, tedarikçi ya da diğer 3. taraflar; zayıflıkları, güvenlik olaylarını ya da güvenlik olayına sebep olabilecek durumları tespit ettikleri anda olay yönetim prosedürüne uygun olarak DCS'e bildirmekle yükümlüdür. Bu politikanın her türlü ihlali soruşturulacak ve disiplin cezasını da içerebilecek uygun düzeltici önlemler alınacaktır.

7 Politikaya Aykırılık

Bu politikaya uyulmaması, iş akdinin veya dış paydaşla iş ilişkisini doğuran sözleşmenin feshi de dahil olmak üzere ciddi yaptırımlarla sonuçlanabilir. Ağır ihmal veya kasıtlı suistimal durumlarında yasal işlem başlatılabilir.

8 Bildirim ve Bildirimde Bulunanın Korunması

DCS, çalışanların, tedarikçilerin ve diğer paydaşların işbu politikanın ihlaliyle ilgili endişelerini gizlilik içinde ve misilleme korkusu olmadan bildirmeleri için gerekli mekanizmaları sağlar. Çalışanlar, bir uygunsuzluk veya şüpheli bir durumla karşılaştıklarında, söz konusu davranışta bulunan herkesi yöneticileri veya herhangi bir üstleri dahi olsa bildirmekle yükümlüdür.

Bildirimler Etik Kurulu'na etik@dcscustoms.com.tr adresinden veya yüz yüze yapılabilir.

DCS çalışanlarına kimliklerini açıklamadan da bildirimde bulunma hakkı tanır ve anonim bildirimleri de aynı ciddiyetle ele alır. Yapılan tüm bildirimler Bildirim, Danışma ve Misillemenin Önleme Politikası gereği gizlilikle ve bildirimde bulunan çalışanı misillemeden koruyacak önlemleri alarak ele alınır.

DCS, işbu politikanın ihlallerine ilişkin tüm bildirimleri derhal ve adil bir şekilde soruşturmayı taahhüt eder. Bir ihlalin teyit edilmesi halinde, şirket uygun düzeltici önlemleri alacak ve neden olunan her türlü zararı gidermek için çalışacaktır.

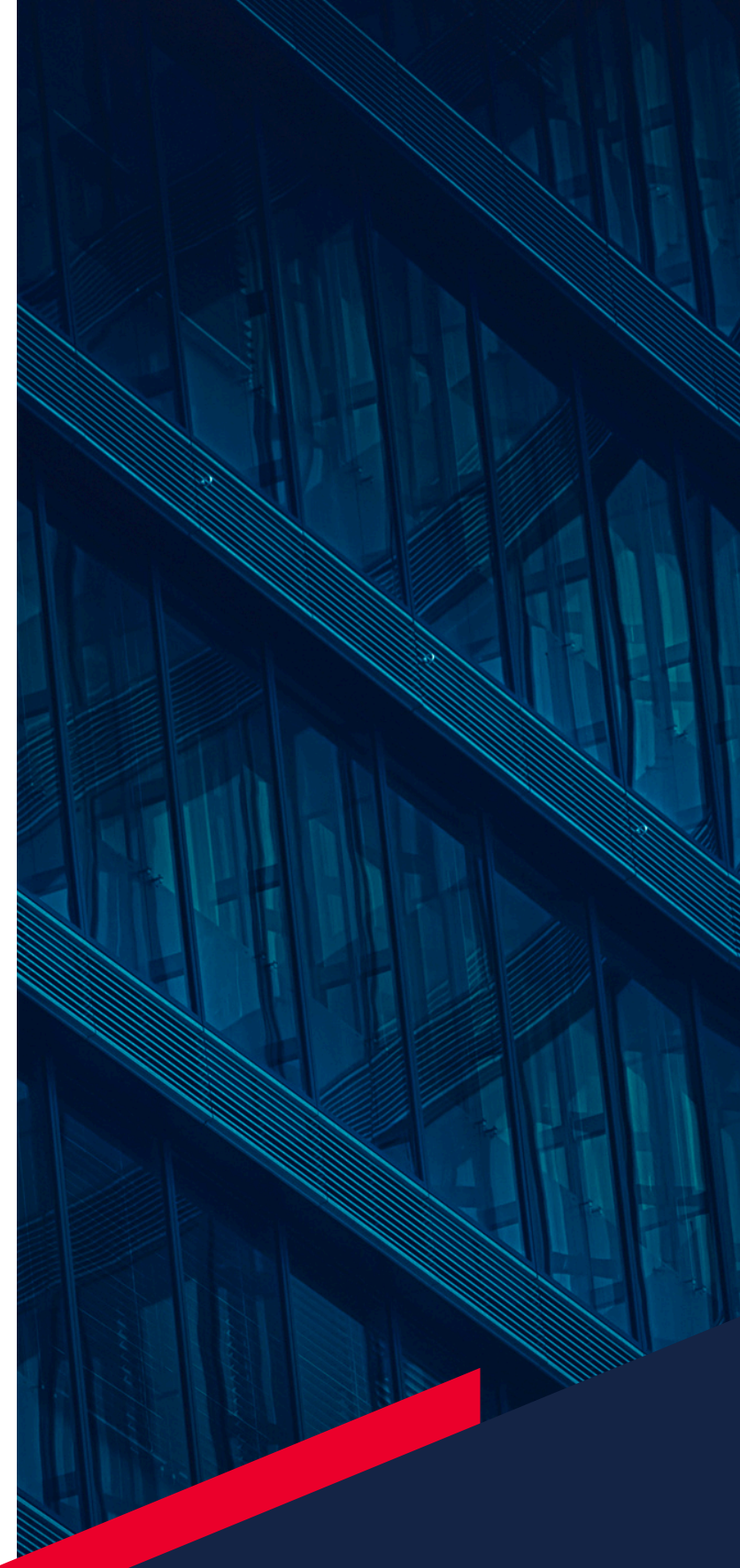
9 Gözden Geçirme ve Revizyon

Bu politika, yürürlüğe girdiği tarihten itibaren yerel ve uluslararası hukuka uygunluk açısından her yıl en az bir kez gözden geçirilir. Gözden geçirme süreci; Bilgi Teknolojileri ile Sürdürülebilirlik ve Uyum Direktörlüğü koordinasyonunda yürütülür. Politika, teknoloji, yürürlükteki yasa ve standartlar ile DCS'in iş uygulamalarında meydana gelen değişiklikleri yansıtacak şekilde gerektiğinde güncellenir.

Bunun dışındaki değişiklik ve revizyonlar Bilgi Teknolojileri'nin değerlendirmeleri sonucunda Sürdürülebilirlik ve Uyum Direktörlüğü tarafından hazırlanacak gerekçeli değişiklik veya revizyon önergesi ile Yönetim Kurulu'na sunulur ve Yönetim Kurulu onayı ile yürürlüğe girerek doküman yönetimi yazılımı marifetiyle kayıt altına alınır.

DCS

Uyum Programı



www.dcscustoms.com.tr