

FİZİKSEL VE FİNANSAL VARLIKLARIN KORUNMASI POLİTİKASI

DCS



Fiziksel ve Finansal Varlıkların Korunması Politikası

1

Amaç

DCS Fiziksel ve Finansal Varlıkların Korunması Politikası, DCS'in bilgi sistemleri ve bilgi varlıkları başta olmak üzere tüm fiziksel ve finansal kaynaklarının korunmasına yönelik ilkeleri belirler.

Bu politika, tüm varlıkların sorumlu bir şekilde kullanılmasını, uygun şekilde muhafaza edilmesini ve hırsızlık, kayıp, yanlış kullanım veya hasara karşı korunmasını sağlar.

Politikanın hiçbir maddesi şirketin tabi olduğu yasalar ile çelişmez.

2

Kapsam

Bu politika şirketin tüm çalışanları, yüklenicileri ve DCS'in fiziksel veya finansal varlıklarına erişimi olan veya bunları yöneten diğer kişiler için geçerlidir.

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

3

Tanımlar

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: Bilgi sistemleri, yazılım lisansları, hizmet abonelikleri, alan adları, yazılı dokümanlar, ekipman, telefonlar, taşınabilir bilgisayarlar ve saklanan veri gibi varlıklardır.

Fiziksel Varlıklar: DCS tarafından sahip olunan, kiralanmış veya yönetilen binalar, ekipmanlar, makineler, araçlar, mobilyalar, bilgisayar donanımı ve diğer tüm maddi kaynakları içerir.

Finansal Varlıklar: Nakit, banka hesapları, menkul kıymetler, alacaklar ve DCS'in kontrolü altındaki diğer tüm finansal kaynakları içerir.

4

Politika Beyanları

4.1 Genel Sorumluluklar

Tüm çalışanlar ve yükleniciler DCS'in fiziksel ve mali varlıklarının uygun şekilde kullanılmasından, bakımından ve korunmasından sorumludur.

Çalışanlar, varlıkların yalnızca meşru iş amaçları için ve yürürlükteki yasalara, yönetmeliklere ve şirket politikalarına uygun olarak kullanılmasını sağlamalıdır.

Varlıkların herhangi bir şekilde kötüye kullanılması, çalınması veya zarar görmesi derhal bir yöneticiye veya Etik ve Uyum Fonksiyonu'na bildirilmelidir.

4.2 Kurum Seçimi ve Finansal Kayıtlar

Varlık Bakımı: Çalışanlar, fiziksel varlıkların iyi çalışır durumda tutulmasını sağlamalıdır. Düzenli bakım programları takip edilmeli ve herhangi bir onarım veya servis işlemi derhal gerçekleştirilmelidir.

Varlık Kullanımı: Fiziksel varlıklar yalnızca yetkili personel tarafından ve yalnızca DCS iş amaçları için kullanılmalıdır. Yönetim tarafından açıkça yetkilendirilmedikçe şirket varlıklarının kişisel kullanımı yasaktır.

Erişim Kontrolü: Fiziksel varlıklara, özellikle hassas veya değerli öğelere erişim yetkili personelle sınırlandırılmalıdır. Yetkisiz erişimi önlemek için güvenli depolama tesisleri ve koruyucu önlemler kullanılmalıdır.

Varlık Envanteri: Tüm fiziksel varlıkların doğru bir envanteri tutulmalıdır. Bu nedenle şirket varlıkları Varlık Sınıflandırma Kılavuzu'na uygun şekilde sınıflandırılır ve Varlık Envanteri'ne kaydedilir. Bu envanter, varlıkların edinilmesi, elden çıkarılması veya devredilmesi gibi değişiklikleri yansıtacak şekilde düzenli olarak güncellenmelidir.

Varlıkların Şirket Dışına Çıkarılması: Ekipman, bilgi ya da yazılım; eğer dahili kullanım ya da gizli olarak sınıflandırılmış ise hangi ortamda bulunursa bulunsun (kâğıt, sabit olmayan veri aktarım cihazları, sabit disk vb.) varlığın kullanıldığı birim yöneticisinin izni olmadan şirket dışına çıkarılmamalıdır. Şirket dışına çıkarılmasına izin verilen bilgi varlıkları, izni veren bölüm yöneticisinin sorumluluğunda korunur.

Varlıkların İadesi: Çalışan, şirketten ayrılması ya da iş akdine son verilmesi durumunda kendine verilmiş olan tüm bilgi varlıklarını İnsan Kaynakları ve Destek Hizmetleri Direktörlüğü veya yöneticisine iade etmelidir.

Varlıkların Elden Çıkarılması ve İmhası: Bilgi varlığının sahibi gerekli gördüğü durumlarda söz konusu varlığı Elden Çıkarma ve İmha Politikası'na uygun şekilde elden çıkarmalı veya imha etmelidir.

4.2.1 Uzaktan Çalışmada Varlıkların Korunması

Uzaktan çalışma kapsamında çalışanlara tahsis edilen şirket varlıklarının, şirket ofisleri dışında da güvenliğinin sağlanması esastır. Bu doğrultuda çalışanlar, aşağıdaki ilkelere uygun hareket etmekte yükümlüdür.

- Şirket varlıklarını yalnızca meşru iş amaçları için kullanmak ve aile bireyleri de dahil olmak üzere yetkisiz üçüncü kişilerin kullanımına sunmamak.
- Varlıkları, hırsızlık, kayıp veya hasar gibi risklere karşı korumak için makul düzeyde fiziksel güvenlik önlemleri alarak (örneğin kullanılmadığı zamanlarda kilitli bir alanda tutarak) muhafaza etmek.
- Şirkete ait bilgisayar ve mobil cihazların her zaman güçlü parolalarla korunmasını ve kullanılmadığı zamanlarda ekranlarının kilitli kalmasını sağlamak.
- Varlıkların çalınması, kaybolması veya hasar görmesi durumunda derhal yöneticiye ve ilgili birimlere (Bilgi Teknolojileri, İnsan Kaynakları) haber vermek.

4.3 Bilgi Varlıklarının Korunması

DCS'in tüm bilgi varlıklarının korunması için tüm çalışanlar Bilgi Güvenliği ve Veri Koruma Politikası'na, ilgili prosedür ve talimatlara uygun şekilde hareket eder. Bilgi varlıklarını, kapasiteyi gereksiz kullanacak, bilgi sistemlerinin performansını gereksiz şekilde düşürecek ve bilgi güvenliğini tehlikeye atacak şekilde kullanmak yasaktır.

Ayrıca, aşağıdaki faaliyetler de yasaktır;

- İş amaçlı olmayan resim, müzik, video indirmek, zincir e-posta göndermek, oyunlar oynamak vb.
- İlgili onay mekanizmalarından geçmeksizin iş için zimmetlenmiş bilgisayar ve sair elektronik cihazlara (tabletler, mobil telefonlar vb.) uygulama kurmak
- İlgili onay mekanizmalarından geçmeksizin Java uygulamaları, ActiveX ve diğer mobil kodları kullanmak
- Varlık sınıflandırma kılavuzunda belirtilen haller dışında kendi bilgisayarında kriptolojik araçlar (şifreleme) kullanmak
- İlgili onay mekanizmalarından geçmeksizin taşınabilir bir ortamdan uygulama, kod parçacığı, yama ve script benzeri kodlar yüklemek
- İlgili onay mekanizmalarından geçmeksizin, modem, hafıza kartı, taşınabilir disk vb. gibi araçları kullanmak.

4.4 Finansal Varlıkların Korunması

Finansal İşlemler: Tüm mali işlemler dürüstlük ve şeffaflıkla yürütülmelidir. Tüm işlemler için uygun belgelendirme ve onay süreçleri takip edilmeli ve DCS'in finansal sistemlerine doğru bir şekilde kaydedilmeleri sağlanmalıdır.

Nakit Kullanımı ve Banka Hesapları: Nakit ve banka hesapları sıkı kontrollerle yönetilmelidir. Nakit kullanan veya hesapları yöneten çalışanlar, fonların güvende olduğundan ve sadece yetkili personel tarafından erişilebilir olduğundan emin olmalıdır. Herhangi bir tutarsızlığı tespit etmek için düzenli mutabakatlar yapılmalıdır. Banka hesaplarından yapılacak ödeme işlemleri, iki aşamalı kontrol mekanizmaları ile yürütülmelidir.

Gider Yönetimi: DCS adına yapılan harcamalar makul, gerekli ve uygun şekilde belgelendirilmiş olmalıdır. Çalışanlar, önemli harcamalar için önceden onay almak da dahil olmak üzere şirketin harcama politikalarına uymalıdır.

Yatırım ve Varlık Yönetimi: Finansal varlıklar, riski en aza indirirken değeri en üst düzeye çıkaracak şekilde yönetilmelidir. Yatırım kararları DCS'in mali politikalarına uygun olarak alınmalı ve Yönetim Kurulu tarafından onaylanmalıdır.

4.5 Güvenlik Önlemleri

Fiziksel Güvenlik: Ofisler, veri merkezleri ve diğer tesisler (bilgi varlıklarının bulunduğu veya işlendiği fiziksel alanlar); ekipmanlar ve fiziksel varlıklarla birlikte, kilit sistemleri, gözetleme kameraları ve alarmlar gibi uygun güvenlik önlemleri kullanılarak güvence altına alınmalıdır. Hassas alanlara (örneğin sunucu odaları, arşivler veya sadece yetkili personelin erişebileceği bölümler) erişim kontrol edilmeli ve izlenmelidir.

Siber Güvenlik: Finansal veriler ve kayıtlar, yetkisiz erişim, ihlal ve siber saldırılara karşı korunmalıdır. Çalışanlar, DCS'in Bilgi Güvenliği ve Veri Koruma Politikası ile ilgili tüm prosedür ve talimatlara uymakla yükümlüdür. Finansal bilgilerin işlenmesinde güvenli yöntemlerin kullanılması esastır.

Antivirüs Kullanımı: Bilgi Güvenliği Sorumlusu tarafından belirlenmiş antivirüs yazılımı tüm bilgisayarlarda yüklü ve güncel olmalıdır. Antivirüs yazılımı kullanıcı tarafından kaldırılmamalıdır. Antivirüs güncellemesi kullanıcı tarafından durdurulmamalıdır.

Sigorta: DCS, fiziksel ve finansal varlıkların hasar görmesi, çalınması veya diğer risklerden kaynaklanan kayıplara karşı koruma sağlamak için -uygun durumlarda- sigorta poliçeleri edinecek ve bunları yönetecektir.

5

Sorumluluklar

5.1 Çalışan

- Tüm DCS varlıklarını sorumlu bir şekilde kullanmak ve varlıkların korunmasına ilişkin her türlü sorunu veya endişeyi yöneticisine bildirmek
- Bu politikada ve ilgili varlık yönetimi politikalarında belirtilen kılavuz ilkelere ve prosedürlere uymak

5.2 Yöneticiler

- Çalışanların, kurum varlıklarının korunmasına yönelik bireysel sorumluluklarının farkında olmalarını sağlamak
- Sorumlu oldukları departmanda ki varlıkların kullanımını ve durumunu düzenli olarak izlemek
- Varlıklarla ilgili gerçekleştirilecek önemli işlemleri (örn. ekipman devri, imhası, bakımı) onaylamak, kaydının tutulmasını sağlamak ve denetlemek

5.3 Mali İşler Direktörlüğü, Bilgi Teknolojileri ve Etik ve Uyum Fonksiyonu

- Mali ve fiziksel varlıkların doğru kayıtlarını tutmak
- Bu politikaya uygunluğu sağlamak için düzenli denetimler ve değerlendirmeler gerçekleştirmek
- En iyi varlık koruma uygulamaları konusunda çalışanlara rehberlik ve destek sağlamak

6

İzleme ve Uygulama

Varlık koruma önlemlerinin etkinliğini değerlendirmek ve bu politikaya uygunluğu sağlamak amacıyla düzenli denetimler gerçekleştirilecektir.

Bu politika kapsamında tespit edilen herhangi bir ihlal araştırılacak ve gerekli görüldüğü durumlarda uygun düzeltici ve önleyici önlemler alınacaktır.

Politikanın uygulanmasına yönelik değerlendirmeler, düzenli olarak hazırlanan uyum raporlamalarının bir parçası olarak yürütülecektir.

7

Politikaya Aykırılık

Bu politikanın ihlali, iş akdinin veya ilgili dış paydaşla iş ilişkisinin dayandığı sözleşmenin feshine kadar varabilecek yaptırımlarla sonuçlanabilir. Hırsızlık, dolandırıcılık veya diğer suç teşkil eden faaliyetler söz konusu olduğunda 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 ya da şüpheli bir durumla karşılaştıklarında; söz konusu davranışta bulunan kişinin yönetici veya herhangi bir üst düzey çalışan olması fark etmeksizin, durumu bildirmelidir.

Bildirimler Etik ve Uyum Fonksiyonu'na etik@dcscustoms.com.tr adresinden 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 Önlenmesi Politikası gereği gizlilikle ve bildirimde bulunan çalışanı misillemekten 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; Mali İşler Direktörlüğü, Bilgi Teknolojileri ve Etik ve Uyum Fonksiyonu'nun koordinasyonunda yürütülür. DCS'in faaliyetlerindeki, varlık portföyündeki ve ilgili yasa veya yönetmeliklerdeki değişiklikleri yansıtmak için gerektiğinde güncellenir.

Dokümanın yeterliliği ve etkinliği gözden geçirilirken varlıkların uygun olmayan ve yetkilendirilmemiş kullanımından veya personelin yeterince farkındalık eğitimi almamasından kaynaklanan güvenlik olayları değerlendirilir.

Bunun dışındaki değişiklik ve revizyonlar şirketin ilgili risklerle ilgili değerlendirmeleri sonucunda Etik ve Uyum Fonksiyonu 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.

7

Politikaya Aykırılık

Bu politikanın ihlali, iş akdinin veya ilgili dış paydaşla iş ilişkisinin dayandığı sözleşmenin feshine kadar varabilecek yaptırımlarla sonuçlanabilir. Hırsızlık, dolandırıcılık veya diğer suç teşkil eden faaliyetler söz konusu olduğunda 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 ya da şüpheli bir durumla karşılaştıklarında; söz konusu davranışta bulunan kişinin yönetici veya herhangi bir üst düzey çalışan olması fark etmeksizin, durumu bildirmelidir.

Bildirimler Etik ve Uyum Fonksiyonu'na etik@dcscustoms.com.tr adresinden 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 Önlenmesi Politikası gereği gizlilikle ve bildirimde bulunan çalışanı misillemekten 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; Mali İşler Direktörlüğü, Bilgi Teknolojileri ve Etik ve Uyum Fonksiyonu'nun koordinasyonunda yürütülür. DCS'in faaliyetlerindeki, varlık portföyündeki ve ilgili yasa veya yönetmeliklerdeki değişiklikleri yansıtmak için gerektiğinde güncellenir.

Dokümanın yeterliliği ve etkinliği gözden geçirilirken varlıkların uygun olmayan ve yetkilendirilmemiş kullanımından veya personelin yeterince farkındalık eğitimi almamasından kaynaklanan güvenlik olayları değerlendirilir.

Bunun dışındaki değişiklik ve revizyonlar şirketin ilgili risklerle ilgili değerlendirmeleri sonucunda Etik ve Uyum Fonksiyonu 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