# ISO 27001 uyumluluğu için neden C-Dozer gerekli.

| EK A No | Tanım | Kontrol | Açıklama |
|---|---|---|---|
| A.5.1.1 | Bilgi güvenliği için politikalar | Kontrol<br>Bir dizi bilgi güvenliği politikaları, yönetim tarafından tanımlanmalı, onaylanmalı ve yayınlanarak çalışanlara ve ilgili dış taraflara bildirilmelidir. | Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'e uygun olarak ve kurum tarafından hazırlanan kişisel veri işleme envanteri göz önünde bulundurularak kişisel veri saklama ve imha politikası hazırlanmalıdır. |
| | | | |
| A.8.3.1 | Taşınabilir ortam yönetimi | Kontrol<br>Taşınabilir ortam yönetimi için prosedürler kuruluş tarafından benimsenen sınıflandırma düzenine göre uygulanmalıdır. | Onarım/tadilat için üçüncü kişilere (yetkisi servis vb.) verilecek taşınabilir bilgisayarlar fabrika ayarlarına döndürülmeli ve içindeki kurumsal veriler güvenli yöntemler kullanılarak silinmelidir. |
| | | | |
| | | | Kullanım ömrünü tamamlayan cihazların veri depolama üniteleri (HDD, SSD, USB, disk, harici bellek vb.) güvenli bir şekilde imha edilmelidir. Kurum içinde tekrar kullanılması durumunda ise veri kurtarmaya imkân sağlamayacak şekilde güvenli silme işlemine tabi tutulduktan sonra kullanıma alınmalıdır. |
| | | | Kurum tarafından satın alınan kullanıcı bilgisayarlarına ait sabit diskler, veri kurtarmaya imkân sağlamayacak şekilde güvenli silme işlemine tabi tutulduktan sonra sistemlere dâhil edilmelidir.<br>Yedekleme medyalarının envanteri tutulmalı ve envanter periyodik olarak gözden geçirilmelidir. Yedekleme medyaları, fiziksel olarak güvenli ve yedek alınan bölgeden farklı bir konumda saklanmalıdır. |

| | | | |
|---|---|---|---|
| | | | Yedeklenen verinin; ana sistemlerin bulunduğu ortamla benzer riskleri içermeyen başka bir ortamda saklandığı teyit edilmelidir. Yedeklenen veri tesis/yerleşke dışına taşınırken güvenliğinin sağlandığı ve bulunduğu ortamın fiziksel ve mantıksal güvenliğinin sağlanmış olduğu teyit edilmelidir. Yedekler kullanım süresinin sona ermesi sonrasında ulusal/uluslararası standartlara uygun olarak güvenli bir şekilde imha edilmeli ve imha kayıtları tutulmalıdır. |
| A.8.3.2 | Ortamın yok edilmesi | Kontrol<br>Ortam artık ihtiyaç kalmadığında resmi prosedürler kullanılarak güvenli bir şekilde yok edilmelidir. | Onarım/tadilat için üçüncü kişilere (yetkisi servis vb.) verilecek cihazlar fabrika ayarlarına döndürülmeli ve içindeki kurumsal veriler silinmelidir. Cihaz içindeki veri silinemeyecek durumda ise cihaz imha edilmelidir. |
| | | | Onarım/tadilat için üçüncü kişilere (yetkisi servis vb.) verilecek taşınabilir bilgisayarlar fabrika ayarlarına döndürülmeli ve içindeki kurumsal veriler güvenli yöntemler kullanılarak silinmelidir. |
| | | | Kullanım süresi dolmuş taşınabilir ortamlar veri sızıntılarını önlemek amacıyla güvenli olarak imha edilmelidir. |
| | | | Paylaşımlı/bulut ortamdan hizmet sağlayan servis sağlayıcılar hizmetin sonlanması durumunda hizmet alan tarafa ait profil ayarları, hizmet raporları vb. hizmete ilişkin tanımları silmelidir. Bulut sistemlerde barındırılan veriler, kullanımının sonlandırılması durumunda sistemlerden geri getirilemeyecek şekilde silinmelidir. |
| | | | Bulut hizmeti kapsamında herhangi bir sanal makinenin |
| | | | Sanal makineler silinmeden önce, sanal makineye ait disk dosyalarına sıfır yazılmalı ve daha sonrasında kalıcı silme işlemi yapılmalıdır. |

| | | | |
|---|---|---|---|
| | | | Kişisel veri barındıran yedeklerin güvenli şekilde yok edilmesi (geri getirilemeyecek, tekrar elde edilemeyecek vb. şekilde silme) için gerekli süreç tanımlanmalı ve uygulanmalıdır. |
| | | | |
| A.8.3.3 | Fiziksel ortam aktarımı | Kontrol<br>Bilgi içeren ortam, aktarım sırasında yetkisiz erişim, kötüye kullanım ve bozulmaya karşı korunmalıdır. | Yedeklenen verinin; ana sistemlerin bulunduğu ortamla benzer riskleri içermeyen başka bir ortamda saklandığı teyit edilmelidir. Yedeklenen veri tesis/yerleşke dışına taşınırken güvenliğinin sağlandığı ve bulunduğu ortamın fiziksel ve mantıksal güvenliğinin sağlanmış olduğu teyit edilmelidir. Yedekler kullanım süresinin sona ermesi sonrasında ulusal/uluslararası standartlara uygun olarak güvenli bir |
| | | | |
| A.9.4.2 | Güvenli oturum açma prosedürleri | Erişim kontrol politikası tarafından şart koşulduğu yerlerde, sistem ve uygulamalara erişim güvenli bir oturum açma prosedürü tarafından kontrol edilmelidir. | Kimlik doğrulamayla erişilen tüm sayfalardan oturum kapatma işlevine erişilebilmelidir. Buna ek olarak, oluşturulan oturum kimliğinin geçerlilik süresi belirlenmelidir. İlgili süre sonunda, belirli süre etkinlik olmadığında veya kullanıcı oturumu kapattığında oturum geçersiz hale gelmelidir. İlgili sürelerin güncellenmesi sürecinde yetkilendirme mekanizmasından faydalanılmalıdır. Ayrıca oturumun geçersiz olmasına sebep olacak bilgilerin değişmesi durumunda (kullanıcı parolasının güncellenmesi, yetkilerin güncellenmesi vb.) etkin oturumların sonlandırılması sağlanmalıdır. Oturum sonlandığında istemci ve sunucuda oturum ile ilgili tüm geçici depolama alanları ve çerezler uygulama tarafından silinmelidir. |
| | | | |
| A.10.1 | Kriptografik kontroller | Amaç: Bilginin gizliliği, aslına uygunluğu ve/veya bütünlüğü ’nün korunması için kriptografi’nin doğru ve etkin kullanımın temin etmek | Anahtar alma işleminde bütünlük hatası tespit edilirse veya depolanan anahtarda bütünlük hatası oluşması durumunda anahtar malzemesi hemen imha edilmeli ve işlem kayıt altına alınmalıdır. |

| | | | |
|---|---|---|---|
| A.11.2.5 | Varlıkların taşınması | Kontrol<br>Teçhizat, bilgi veya yazılım ön yetkilendirme olmaksızın kuruluş dışına çıkarılmamalıdır. | Yedeklenen verinin; ana sistemlerin bulunduğu ortamla benzer riskleri içermeyen başka bir ortamda saklandığı teyit edilmelidir. Yedeklenen veri tesis/yerleşke dışına taşınırken güvenliğinin sağlandığı ve bulunduğu ortamın fiziksel ve mantıksal güvenliğinin sağlanmış olduğu teyit edilmelidir. Yedekler kullanım süresinin sona ermesi sonrasında ulusal/uluslararası standartlara uygun olarak güvenli bir şekilde imha edilmeli ve imha kayıtları tutulmalıdır. |
| | | | |
| A.11.2.7 | Teçhizatın güvenli yok edilmesi veya tekrar kullanımı | Kontrol<br>Depolama ortamı içeren teçhizatların tüm parçaları, yok etme veya tekrar kullanımdan önce tüm hassas verilerin ve lisanslı yazılımların kaldırılmasını veya güvenli bir şekilde üzerine yazılmasını temin etmek amacıyla doğrulanmalıdır. | Yedeklenen verinin; ana sistemlerin bulunduğu ortamla benzer riskleri içermeyen başka bir ortamda saklandığı teyit edilmelidir. Yedeklenen veri tesis/yerleşke dışına taşınırken güvenliğinin sağlandığı ve bulunduğu ortamın fiziksel ve mantıksal güvenliğinin sağlanmış olduğu teyit edilmelidir. Yedekler kullanım süresinin sona ermesi sonrasında ulusal/uluslararası standartlara uygun olarak güvenli bir şekilde imha edilmeli ve imha kayıtları tutulmalıdır. |
| | | | Kişisel veri barındıran yedeklerin güvenli şekilde yok edilmesi (geri getirilemeyecek, tekrar elde edilemeyecek vb. şekilde silme) için gerekli süreç tanımlanmalı ve uygulanmalıdır. |
| | | | |
| A.12.3.1 | Bilgi yedekleme | Kontrol<br>Bilgi, yazılım ve sistem imajlarının yedekleme kopyaları alınmalı ve üzerinde anlaşılmış bir yedekleme politikası doğrultusunda düzenli olarak test edilmelidir. | benzer riskleri içermeyen başka bir ortamda saklandığı teyit edilmelidir. Yedeklenen veri tesis/yerleşke dışına taşınırken güvenliğinin sağlandığı ve bulunduğu ortamın fiziksel ve mantıksal güvenliğinin sağlanmış olduğu teyit edilmelidir. |
| | | | |

| | | | |
|---|---|---|---|
| A.12.4.2 | Kayıt bilgisinin korunması | Kontrol<br>Kaydetme olanakları ve kayıt bilgileri kurcalama ve yetkisiz erişime karşı korunmalıdır. | Tüm sistemlerde ve ağ cihazlarında kayıt mekanizması etkin olmalıdır. Kayıtlar, bilgi güvenliği gereksinimleri ve ilgili mevzuat gereği kabul edilebilir süre boyunca cihaz üzerinde veya harici sistemlerde tutulmalı, yetkisiz erişime ve değişime karşı korunmalıdır. Kayıtlar, muhafazaları için tanımlanan kabul edilebilir sürenin sona ermesi ile birlikte güvenli bir şekilde yok edilmelidir. |
| | | | |
| A.12.5 | İşletimsel sistemler üzerine yazılım kurulumu | Kontrol<br>İşletimsel sistemler üzerine yazılım kurulumunun kontrolü için prosedürler uygulanmalıdır. | Kurulum ile gelen örnek veriler (örnek tablolar, kayıtlar, kullanıcılar vb.) silinmelidir. (Veritabanları dahil) |
| | | | |
| A.14.1.1 | Bilgi güvenliği gereksinimleri analizi ve belirtimi | Kontrol<br>Bilgi güvenliği ile ilgili gereksinimler, yeni bilgi sistemleri gereksinimlerine veya var olan bilgi sistemlerinin iyileştirmelerine dâhil edilmelidir. | Geliştirilen uygulama/sistem kapsamında sunulan arayüzün kullanıcılar tarafından açıkça anlaşılabilir olması adına Türkçe dil desteği sağlanmalı, tedarik edilen ürünlerde ise Türkçe dil desteği olan ürünler tercih edilmelidir. |
| | | | |
| A.14.2.1 | Güvenli geliştirme politikası | Kontrol<br>Yazılım ve sistemlerin geliştirme kuralları belirlenmeli ve kuruluş içerisindeki geliştirmelere uygulanmalıdır. | İstemci ve sunucu uygulamalarında dosyalarda ve çerezlerde geçici olarak tutulan kişisel verilerin işleme gereksinimi veya kanuni saklama süresi sona erdiğinde güvenlik ihlali oluşturamayacak şekilde (geri getirilemeyecek, tekrar elde edilemeyecek vb.) yok edilmelidir. |
| | | | |
| | | | İstemci ve sunucu uygulamalarında dosyalarda ve çerezlerde geçici olarak tutulan kişisel verilerin işleme gereksinimi veya kanuni saklama süresi sona erdiğinde güvenlik ihlali oluşturamayacak şekilde (geri getirilemeyecek, tekrar elde edilemeyecek vb.) yok edilmelidir. |

| | | | |
|---|---|---|---|
| A.14.2.5 | Güvenli sistem mühendisliği prensipleri | Kontrol<br>Güvenli sistem mühendisliği prensipleri belirlenmeli, yazılı hale getirilmeli ve tüm bilgi sistemi uygulama çalışmalarına uygulanmalıdır. | Kimlik doğrulamayla erişilen tüm sayfalardan oturum kapatma işlevine erişilebilmelidir. Buna ek olarak, oluşturulan oturum kimliğinin geçerlilik süresi belirlenmelidir. İlgili süre sonunda, belirli süre etkinlik olmadığında veya kullanıcı oturumu kapattığında oturum geçersiz hale gelmelidir. İlgili sürelerin güncellenmesi sürecinde yetkilendirme mekanizmasından faydalanılmalıdır. Ayrıca oturumun geçersiz olmasına sebep olacak bilgilerin değişmesi durumunda (kullanıcı parolasının güncellenmesi, yetkilerin güncellenmesi vb.) etkin oturumların sonlandırılması sağlanmalıdır. Oturum sonlandığında istemci ve sunucuda oturum ile ilgili tüm geçici depolama alanları ve çerezler uygulama tarafından silinmelidir. |
| | | | |
| A.15.1 | Tedarikçi ilişkilerinde bilgi güvenliği | Amaç: Kuruluşa ait tedarikçiler tarafından erişilen varlıkların korunmasını sağlamak. | Paylaşımlı/bulut ortamdan hizmet sağlayan servis sağlayıcılar hizmetin sonlanması durumunda hizmet alan tarafa ait profil ayarları, hizmet raporları vb. hizmete ilişkin tanımları silmelidir. Bulut sistemlerde barındırılan veriler, kullanımının sonlandırılması durumunda sistemlerden geri getirilemeyecek şekilde silinmelidir. |
| | | | Bulut bilişim hizmeti kapsamında hizmet alınan taraf ile hizmet alan kurum arasında, karşılıklı yükümlülükleri ve gizlilik maddelerini içeren bir sözleşme yapılmalıdır. Alınan hizmetin kapsamı sözleşme içerisinde tam olarak belirtilmeli ve hizmet kapsamında işlenen verinin kritikliği doğrultusunda yeterli seviyede güvenlik önlemleri alınmalıdır. İlgili sözleşmenin geçerlilik süresi belirlenmeli ve periyodik olarak gözden geçirilmesi sağlanmalıdır. |

| | | | |
|---|---|---|---|
| | | | Bulut hizmeti kapsamında herhangi bir sanal makinenin hizmetinin sonlandırılması durumunda, sanal makinenin bulut bilişim sunucularında bulunan disk bölgeleri otomatik olarak servis sağlayıcı tarafından geri döndürülemeyecek şekilde silinmelidir. |
| | | | |
| A.18.1.4 | Kişi tespit bilgisinin gizliliği ve korunması | Kontrol<br>Kişiyi tespit bilgisinin gizliliği ve korunması uygulanabilen yerlerde ilgili yasa ve düzenlemeler ile sağlanmalıdır. | İstemci ve sunucu uygulamalarında dosyalarda ve çerezlerde geçici olarak tutulan kişisel verilerin işleme gereksinimi veya kanuni saklama süresi sona erdiğinde güvenlik ihlali oluşturamayacak şekilde (geri getirilemeyecek, tekrar elde edilemeyecek vb.) yok edilmelidir. |
| | | | Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'e uygun olarak ve kurum tarafından hazırlanan kişisel veri işleme envanteri göz önünde bulundurularak kişisel veri saklama ve imha politikası hazırlanmalıdır. |
| | | | |
| A.18.1.1 | Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama | Kontrol<br>İlgili tüm yasal mevzuat, düzenleyici, sözleşmeden doğan şartları ve kuruluşun bu gereksinimleri karşılama yaklaşımı her bilgi sistemi ve kuruluşu için açıkça tanımlanmalı, yazılı hale getirilmeli ve güncel tutulmalıdır. | İlgili kişi, açık rızasını geri alma talebini uygulama üzerinden gerçekleştirebilmelidir. İlgili kişinin açık rızasını geri alma talebi veri sorumlusu tarafından uygulanmalı ve ilgili kişinin açık rızasına dayanarak yapılan veri işleme faaliyetleri |
| | | | İlgili kişi tarafından talep edilen; güncelleme, anonimleştirme, silme, yok etme işlemleri gerçekleştirilmelidir. Talep edilmesi durumunda bu işlemler kişisel verinin aktarıldığı üçüncü taraflara da iletilmelidir. Yapılacak işlemlerle ilgili bilgilendirme Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'e uygun olarak gerçekleştirilmelidir. |
| *C-dozer sadece Windows dektop ve sunucu işletim sistemlerinde çalışmaktadır. | | | |