CBDD BigR uyumluluğu için neden C-Dozer gerekli.			
CBDD BigR Tedir KAT3	CBDD BigR Tedbir No.	27001:2017	Tedbir Tanımı
3.1.1. Donanım Varlıklarının Envanter Yönetimi	3.1.1.6	A.8.3.2 Ortamın yok edilmesi	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.
	3.1.1.9	A.8.3.2 Ortamın yok edilmesi	Kurum tarafından satın alınan kullanıcı bilgisayarlarına ait sabit diskler, veri kurtarmaya imkân sağlamayacak şekilde güvenli silme işlemine tabi tutulduktan sonra sistemlere dâhil edilmelidir.
3.1.8. İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi	3.1.8.1	3.1.8. İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi	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.
3.1.13. Felaket Kurtarma ve İş Sürekliliği Yönetimi	3.1.13.5	A.8.3.2 Ortamın yok edilmesi A.8.3.3 Fiziksel ortam aktarımı A.11.2.5 Varlıkların taşınması A.11.2.7 Teçhizatın güvenli yok edilmesi veya tekrar kullanımı A.12.3.1 Bilgi yedekleme	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.

3.2.2. Oturum Yönetimi	3.2.2.3	A.9.4.2 Güvenli oturum açma prosedürleri A.14.2.5 Güvenli sistem mühendisliği esasları	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.
3.3.1. Akıllı Telefon ve Tablet Güvenliği	3.3.1.12	A.6.2.1 Mobil cihaz politikası A.9.4.2 Güvenli oturum açma prosedürleri	Kaba kuvvet saldırılarından korunmak için, kurum tarafından belirlenecek sayıda hatalı giriş denemesi sonrası cihaz belleğinde bulunan veriler silinmelidir.
	3.3.1.6	A.6.2.1 Mobil cihaz politikası	Cihazı uzaktan fabrika ayarlarına döndürüp içindeki veriyi silebilecek bir mekanizma kullanılmalıdır.
	3.3.1.7	A.6.2.1 Mobil cihaz politikası A.8.3.2 Ortamın yok edilmesi	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.
3.3.2. Taşınabilir Bilgisayar Güvenliği	3.3.2.3	A.6.2.1 Mobil cihaz politikası A.8.3.1 Taşınabilir ortam yönetimi A.8.3.2 Ortamın yok edilmesi	Onarım/tadilat için üçüncü kişilere (yetkisi servis vb.) verilecek taşınabilir bilgisayarlar fabrika ayarlarına döndürülmeli ve içindeki kurumsal veriler güvenli yöntemler kullanılarak silinmelidir.
3.3.3. Taşınabilir Ortam Güvenliği (CD/DVD, Taşınabilir Bellek Ortamları)	3.3.3.4	A.8.3.2 Ortamın yok edilmesi	Kullanım süresi dolmuş taşınabilir ortamlar veri sızıntılarını önlemek amacıyla güvenli olarak imha edilmelidir.

4.1.1. Kayıt Yönetimi	4.1.1.10	A.14.2.1 Güvenli geliştirme politikası A.14.2.5 Güvenli sistem mühendisliği esasları A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması	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.
	4.1.1.2	A.5.1.1 Bilgi güvenliği politikaları A.18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması	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.
4.1.5. Yedekleme, Silme, Yok Etme ve Anonim Hale Getirme	4.1.5.6	A.8.3.2 Ortamın yok edilmesi A.11.2.7 Teçhizatın güvenli yok edilmesi veya tekrar kullanımı	Kişisel veri barındıran yedeklerin güvenli şekilde yok edilmesi (geri getirilemeyecek, tekrar elde edilemeyecek vb. şekilde silme) için gerekli süreç tanımlanmalı ve uygulanmalıdır.
4.1.7. Açık Rıza Yönetimi	4.1.7.6	A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama	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 durdurulmalıdır.
4.1.8. Kişisel Veri Yönetim Sürecinin İşletilmesi	4.1.8.3	A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama	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. Bk. Tedbir No: 4.1.8.1
	4.3.1.11	A.8.3.2 Ortamın yok edilmesi A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği	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.

4.3.1. Genel Güvenlik Tedirleri	4.3.1.2	A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği	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. Bk. Tedbir No: 3.5.3.1 Bk. Tedbir No: 3.5.3.3
	4.3.1.8	A.8.3.2 Ortamın yok edilmesi A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği	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.
4.4.2. Şifreleme ve Anahtar Yönetimi	4.4.2.22	A.10.1 Kriptografik kontroller	Anahtar alma işleminde bütünlük hatası tespit edilirse veya depolanan anahtarda bütünlük hatası oluşması durumunda anahtar malzemesi hemen imha edilmeli ve işlem kayıt altına alınmalıdır.
4.6.1. Genel Güvenlik Tedbirleri	4.6.1.4	A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi	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.
5.2.1. Genel Sıkılaştırma Tedbirleri	5.2.1.14	A.12.5 İşletimsel yazılımın kontrolü	Veri tabanından, kurulum ile gelen örnek veriler (örnek tablolar, kayıtlar, kullanıcılar vb.) silinmelidir.
5.3.2. Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri	5.3.2.12	A.8.3.2 Ortamın yok edilmesi	Sanal makineler silinmeden önce, sanal makineye ait disk dosyalarına sıfır yazılmalı ve daha sonrasında kalıcı silme işlemi yapılmalıdır.
*C-dozer sadece Windows dektop ve sunucu işletim sistemlerinde çalışmaktadır.			