IBM Bulut Hizmeti Açıklaması:

IBM Kenexa Prove It! Add-ons on Cloud

Siparişiniz için Hizmet Açıklaması aşağıda belirtildiği gibidir:

1. Bulut Hizmeti Açıklaması

Sipariş edebileceğiniz Bulut Hizmeti ürünü aşağıda belirtilmiştir. Bu Hizmet Açıklamasında sunulan ürün, bir "eklenti" ürünü olarak kabul edilmektedir, bu nedenle aşağıdaki Bölüm 1.1'de belirtilen eklerden herhangi birini sipariş etmeden önce IBM Kenexa Prove It! ürününe abone olmanız gerekmektedir. Sipariş etmiş olduğunuz ürünler, Sipariş Belgenizde belirtilmiştir. Sipariş Belgesi, bu Bulut Hizmetinin amaçları uyarınca, IBM'in size sunduğu Fiyat Teklifinden ve IBM'den alacağınız, Bulut Hizmetlerinin tahsis edilmiş olduğunu teyit eden, faturalandırmanın başlayacağını bildiren ve Bulut Hizmeti süresinin başlangıç ve sona erme tarihlerini belirten Yetki Belgesinden oluşacaktır.

1.1 IBM Kenexa Prove It! Add-ons on Cloud

IBM Kenexa Prove It! IBM Kenexa Skills Assessments uygulamaları ve desteği ile IBM Kenexa Behavioral Assessments seçimleri için sağlanan çevrimiçi bir çözümdür. IBM Kenexa Prove It!, Müşterinin belirli gereksinimlerinin karşılanması için Prove It! Web sitesinin özelleştirilmesine yönelik olarak aşağıda belirtilen yapılandırma hizmetlerini sağlamaktadır:

a. IBM Kenexa Prove It! Custom Web Site

   Bu eklenti ürünü, başlangıç sayfasındaki renkleri, logoları ve içeriği değiştirmenize olanak sağlamaktadır. Başlangıç sayfasında veya web sitesinin geri kalanında yapı, başlık sayfası veya düzen değişikliği yoktur.

b. IBM Kenexa Prove It! Corporate Custom Web Site

   Bu eklenti ürünü, başlangıç sayfasındaki renkleri, logoları, içeriği, ana başlığı ve yerleşim düzenini değiştirmenize olanak sağlar. Web sitesinin geri kalan kısmının yapısında veya düzeninde değişiklik yoktur.

2. Güvenlik Açıklaması

2.1 Güvenlik İlkeleri

IBM, IBM çalışanlarına duyurulan gizlilik ve güvenlik ilkeleri uygulamaktadır. IBM, dünyanın her yanındaki IBM veri merkezlerine destek sağlayan kişilerin güvenlik ve gizlilik eğitimi almasını gerektirmektedir ve bilgi güvenliğine odaklanan bir güvenlik ekibine sahiptir. IBM güvenlik ilkeleri ve standartları, yıllık olarak incelenmekte ve yeniden değerlendirilmektedir. IBM güvenlik olayları, kapsamlı bir olay müdahale prosedürü uyarınca ele alınmaktadır.

2.2 Erişim Denetimi

Görevler ayrılığı ilkeleri doğrultusunda yalnızca yetkili IBM destek temsilcilerinin müşteri verilerine erişmesine izin verilir. IBM destek personeli, bir ara "ağ geçidi" yönetim anabilgisayarına erişmek için iki etkenli kimlik doğrulaması kullanmaktadır.저Müşteri verilerine erişim için kullanılan tüm bağlantılar, şifrelenmiş kanallardır. Müşteri verilerine erişimin tamamı ve verilerin barındırma ortamına ve barındırma ortamı dışına aktarımı günlüğe alınır. IBM veri merkezleri içerisinde, bu Bulut Hizmetinin desteklenmesi amacıyla WIFI kullanılmaz.

2.3 Hizmetin Bütünlüğü ve Kullanılabilirliği

İşletim sistemi kaynaklarında ve uygulama yazılımlarında yapılan değişiklikler, IBM'in değişiklik yönetimi süreci aracılığıyla yönetilmektedir. Güvenlik duvarı kurallarındaki değişiklikler de değişiklik yönetimi sürecine tabidir ve uygulanmadan önce IBM güvenlik personeli tarafından ayrı olarak incelenir. IBM, veri merkezi kaynaklarını 7 gün, 24 saat izlemektedir. Potansiyel sistem güvenliği açıklarının tespit edilmesine ve çözülmesine yardımcı olması için yetkili sistem yöneticileri ve üçüncü kişi satıcı firmalar tarafından düzenli olarak dahili ve harici güvenlik açığı taraması gerçekleştirilmektedir. Tüm IBM veri merkezlerinde kötü amaçlı yazılım saptama (virüs önleme, izinsiz giriş saptama, güvenlik açığı taraması ve izinsiz giriş önleme) sistemleri kullanılmaktadır. IBM'in veri merkezi hizmetleri, verilerin halka açık ağlar üzerinden aktarılmasına ilişkin olarak çeşitli bilgi iletimi iletişim kurallarını desteklemektedir. Örnekler arasında

HTTPS/SFTP/FTPS/S/MIME ve siteler arası VPN yer almaktadır. Uzak konumda depolanmak üzere oluşturulan yedek veriler, aktarılmadan önce şifrelenir.

2.4 Etkinliklerin Günlüğe Kaydedilmesi

IBM, etkinlikleri günlüğe kaydetme yeteneğine sahip ve kaydetmek üzere yapılandırılmış sistemler, uygulamalar, veri havuzları, ara katman yazılımları ve ağ altyapısı aygıtları için etkinliklerinin günlüklerini tutmaktadır. Yetkisiz müdahale olasılığının en düşük seviyeye indirgenmesi ve merkezi analize, uyarı oluşturmaya ve raporlamaya olanak sağlanması için etkinlikler gerçek zamanlı olarak merkezi günlük havuzlarına kaydedilmektedir. Yetkisiz müdahalenin önlenmesi için verilere imza eklenir. Anormal davranışların aranması için, günlükler gerçek zamanlı olarak ve düzenli analiz raporları aracılığıyla analiz edilir. Anormallikler operasyon personeline bildirilir ve gerekli olması halinde 7 gün 24 saat nöbet esasına göre çalışan bir güvenlik uzmanı ile iletişim kurulur.

2.5 Fiziksel Güvenlik

IBM, veri merkezi kaynaklarına yetkisiz fiziksel erişimin kısıtlanması amacıyla tasarlanan fiziksel güvenlik standartları uygulamaktadır. IBM veri merkezlerine yalnızca sınırlı sayıda erişim noktası bulunmaktadır ve bu noktalar iki etkenli kimlik doğrulama ile denetlenmekte ve güvenlik kameraları kullanılarak izlenmektedir. Yalnızca erişimi onaylanmış yetkili personelin erişimine izin verilmektedir. Operasyon personeli, onayı doğrulamaktadır ve gerekli erişim yetkisini sağlayan bir erişim kartı düzenlemektedir. Anılan kartların sağlandığı çalışanlar, diğer erişim kartlarını iade etmeli ve etkinlikleri süresince yalnızca veri merkezi erişim kartına sahip olmalıdır. Erişim kartlarının kullanımı günlüğe kaydedilmektedir. IBM dışı ziyaretçiler, tesislere girişleri sırasında kaydedilmekte ve tesislerde bulundukları süre boyunca kendilerine eşlik edilmektedir. Teslimat alanları, yükleme platformları ve yetkisiz kişilerin binaya girebileceği diğer noktalar denetlenir ve ayrıştırılmıştır.

2.6 Uyumluluk

IBM, ABD Ticaret Bakanlığı'nın Safe Harbor: Bildirim, Tercih, Üçüncü Kişilere Bilgi Açıklama, Erişim ve Doğruluk, Güvenlik ve Denetim/Uygulama ilkeleri uyarınca gizlilik uygulamalarını her yıl tasdik etmektedir. Üretim veri merkezlerimizde her yıl endüstri standardı olarak kabul edilen SSAE 16 Tipi (eski adıyla SAS 70) veya eşdeğeri denetim gerçekleştirilmektedir. IBM, güvenlik ve gizlilik ile bağlantılı etkinlikleri IBM'in iş gereksinimlerine uygunluk açısından incelemektedir. IBM, bilgi güvenliği ilkelerine uygunluğu doğrulamak için düzenli olarak değerlendirmeler ve denetimler gerçekleştirmektedir. IBM'in ve satıcı firmaların çalışanları, her yıl işgücü güvenliği eğitimi ve farkındalık eğitimi almaktadır. İş hedefleri ile etik iş adabına, gizliliğe ve IBM'in güvenlik yükümlülüklerine uyma sorumlulukları, personele yıllık olarak hatırlatılmaktadır.

3. Yetki, Faturalandırma ve Süre Bilgileri

3.1 Ücret Sistemleri

Bulut Hizmeti ürünü, Sipariş Belgesinde belirtildiği şekilde, aşağıda belirtilen ücret ölçüsü doğrultusunda satılır:

a. Eşgörünüm, Bulut Hizmetinin edinilmesinde esas alınabilecek bir ölçü birimidir. Bir Eşgörünüm, Bulut Hizmetinin belirli bir yapılandırmasına erişimdir. Yetki Belgesinde veya Sipariş Belgesinde belirtilen ölçüm süresi içerisinde erişilmesine ve kullanılmasına izin verilen her Bulut Hizmeti Eşgörünümü için yeterli sayıda yetki edinilmelidir.

3.2 Ücretler ve Faturalandırma

Bulut Hizmeti ürünleri için ödenecek tutar Sipariş Belgesinde belirtilmiştir.

3.2.1 Kurulum

Kurulum ücretleri, Sipariş Belgesinde belirtilecektir.

3.2.2 İsteğe Bağlı Olarak Sunulan Seçenekler

İsteğe Bağlı seçenekler, isteğe bağlı seçeneğin tarafınızdan sipariş edildiği ayda, Sipariş Belgesinde belirtilen tarifeye uygun olarak fatura edilecektir.