Güvenlik Politikası

1. Genel Güvenlik Taahhüdü
Marex, müşteri bilgilerinin, iş süreçlerinin ve dijital altyapısının güvenliğini sağlamak için en yüksek standartları uygular. Tüm veri güvenliği önlemleri, uluslararası regülasyonlar ve en iyi uygulamalar doğrultusunda sürekli güncellenmektedir.

2. Veri Koruma ve Gizlilik
Marex, müşteri ve çalışan bilgilerinin gizliliğini sağlamak için en son şifreleme ve güvenlik protokollerini uygular. Veri erişimi, yalnızca yetkilendirilmiş kişilerle sınırlıdır.

3. Şifreleme Kullanımı
Tüm hassas veriler, AES-256 ve TLS 1.2/1.3 gibi güçlü şifreleme yöntemleriyle korunur. Veri transferleri güvenli kanallar üzerinden gerçekleştirilir.

4. Yetkilendirme ve Erişim Kontrolleri
Marex sistemlerine erişim, çok faktörlü kimlik doğrulama (MFA) ile korunur. Çalışanlar ve üçüncü taraflar, yalnızca görevleri için gerekli bilgilere erişebilir.

5. Ağ Güvenliği ve Güvenlik Duvarları
Marex, iç ve dış tehditlere karşı güçlü güvenlik duvarları ve saldırı tespit sistemleri (IDS/IPS) kullanır. Tüm ağ bağlantıları düzenli olarak denetlenir.

6. Siber Tehditlere Karşı Koruma
Şirket, DDoS saldırıları, kimlik avı girişimleri ve kötü amaçlı yazılımlara karşı sürekli izleme yapar v gelişmiş tehdit istihbaratı çözümlerinden faydalanır.

7. Güvenlik Güncellemeleri ve Yama Yönetimi
Tüm sistemler, güncellemeler ve güvenlik yamalarıyla düzenli olarak güncellenir. Güvenlik açıklar tespit edildiğinde, acil durum müdahale süreçleri devreye girer.

8. Veri Yedekleme Politikası
Marex, önemli verileri düzenli olarak yedekler ve yedekleme dosyalarını güvenli bir ortamda sakla

9. Çalışanlara Yönelik Güvenlik Eğitimi
Tüm çalışanlar, siber güvenlik farkındalık eğitimlerinden geçirilir ve güvenlik politikalarına tam uyum sağlamakla yükümlüdür.

10. Üçüncü Taraf Güvenliği
Marex, çalıştığı tüm üçüncü taraf firmaların güvenlik standartlarını denetler ve yalnızca güvenilir ortaklarla çalışır. Veri paylaşımı konusunda katı güvenlik protokolleri uygulanır.

14. Güvenlik Olayları Müdahale Planı
Bir güvenlik ihlali durumunda, önceden belirlenmiş acil durum protokolleri devreye girer. Tüm olaylar detaylı olarak incelenir ve raporlanır.

15. GDPR ve Uluslararası Regülasyonlara Uygunluk
Marex, Avrupa Birliği'nin GDPR (Genel Veri Koruma Yönetmeliği) ve diğer uluslararası veri koruma yasalarına tam uyum sağlar.

16. Kötü Amaçlı Yazılımlara Karşı Koruma
Tüm sistemlerde güçlü antivirüs ve anti-malware çözümleri kullanılarak kötü amaçlı yazılım tehditlerine karşı koruma sağlanır.

17. Mobil Cihaz Güvenliği
Mobil cihazlardan erişim, şifreleme ve güvenli bağlantılar üzerinden gerçekleştirilir. Kayıp veya çalınan cihazlar için uzaktan erişim kapatma ve veri silme protokolleri uygulanır.

18. Loglama ve İzleme Politikası
Marex, tüm sistem aktivitelerini kayıt altına alır ve güvenlik ihlallerini tespit etmek için düzenli olarak denetler.

19. Kullanıcı Güvenliği ve Parola Politikası
Tüm kullanıcılar, güçlü parola kullanımı konusunda yönlendirilir. Düzenli parola değişimi ve parola yöneticisi kullanımı teşvik edilir.

20. Güvenlik Denetimleri ve Testler
Bağımsız güvenlik firmaları tarafından penetrasyon testleri ve güvenlik denetimleri düzenli olarak gerçekleştirilir. Elde edilen sonuçlara göre gerekli iyileştirmeler yapılır.

21. İletişim Güvenliği
Marex, tüm dijital iletişim kanallarında şifreli iletişim protokolleri kullanır. E-posta ve mesajlaşma gibi platformlarda güvenlik önlemleri alınarak, veri sızıntıları ve dinlemelere karşı önlem alınır.

22. Sosyal Mühendislik Saldırılarına Karşı Koruma
Marex, sosyal mühendislik saldırıları (phishing, vishing, pretexting vb.) konusunda çalışanlarını eğitir. Kullanıcıların, bu tür saldırılara karşı farkındalıkları sürekli olarak artırılır.
23. Kullanıcı ve Sistem İzleme
Tüm kullanıcı hareketleri ve sistem etkinlikleri geriye dönük izlenebilir şekilde kaydedilir. Anormal hareketler, potansiyel güvenlik tehditleri olarak anında bildirilir ve incelemeye alınır.