ICBC Yatırım

## KULLANILAN BİLGİSAYAR AĞI VE ŞİFRELEME SİSTEMİNİN OLASI RİSKLERİ VE GÜVENLİĞİ

ICBC Yatırım tarafından sunulan hizmetlerin eksiksiz alınabilmesi için Müşteriler tarafından uzaktan erişimi sağlayabilecek nitelikleri haiz bilgisayar, modem, telefon hattı ve elektronik erişim programlarının son sürümlerin bulunduğu cihazlardan işlem yapılması gerekmektedir.
Müşteriler elektronik ortamda emir iletiminde kullandıkları cihazların güvenliğini sağlamakla yükümlüdür. Bunun için kullanıcının faaliyetlerini izleyen, cihazların sağlıklı çalışmasını engelleyen, ağ üzerindeki bilgi alış verişini takip eden, kötü amaçlı yazılımları temizleyen, faaliyetleri hakkında uyaran, engelleyen piyasadaki en son ve kapsamlı virüs tarama ve yok etme programlarından en az bir tanesinin en güncel halini bilgisayarında bulundurmak ve kendisine tahsis edilen şifre ve kullanıcı kodlarının gizliliğini sağlamakla yükümlüdür.
ICBC Yatırım iç ve dış ağları katmanlı koruma yapısına sahiptir. Dışarıdan gelebilecek tehditlere karşı bağımsız bir ağ ile konfigüre edilmiş yapı güvenlik donanım ve yazılımları ile de korunmaktadır.
Bilgisayar iç ağı sanal ağlara bölünerek daha güvenli bir yapı sağlanırken, iç ağa konuşlandırılmış olan ağ erişim kontrol sistemi ile kuruma ait olmayan hiçbir cihaz ağa bağlanamamaktadır.

Müşterilerimizin online işlemlerini yaptığı platformda 2048 Bit GlobalSign SSL sertifikası ile şifrelenerek yüksek düzeyde Organization SSL sertifikası ile güvenlik hizmeti verilmektedir.

İç ve dış ağlar her yıl gerçekleştirilen sızma testleri ile güvenlik açısından denetlenmekte, güncel tehditlere karşı sürdürülen bir yapıda tedbirler alınmakta ve düzenlemeler yapılmaktadır.
İnternet Şubemiz Secure nitelikli **https** oturumu olarak açılır. **https** protokolü kullanırken tarayıcı programınızın alt bölümünde bir asma kilit ikonu belirir. Bu ikona çift tıkladığınızda açılan sertifika penceresinde "verilen" alanında bankamızın İnternet adresi olan www.icbcyatirim.com.tr görülmelidir.

## KULLANILAN İŞLEM PLATFORMUNUN VE BİLGİSAYAR AĞININ ÖZELLİKLERİNE, VARSA RİSKLERİ VE GÜVENLİK TEDBİRLERİ İLE PLATFORMDA MEYDANA GELEBİLECEK RİSKLERE KARŞI KULLANILABİLECEK ALTERNATİF İLETİŞİM YÖNTEMLERİ

**Güvenlik gereksinimleri :**

1. Kullanıcıların emirleri ve hesap işlemlerinin tamamı, kullanıcı bilgisayarı ile kurum sunucu sistemleri arasında gerçekleşmektedir**.**
2. Kullanıcının emir ve işlem bilgileri doğrudan iletilmektedir.
3. Bir kullanıcının işlem yapma yetkisi, izinleri ve limitleri daima kurum sunucularında tanımlanmaktadır.
4. Sunucu yazılımları ve web servisleri ile yapılan haberleşmede SSL sertifikası kullanılmalıdır ve kullanılmaktadır.

5. Şifre bilgileri, cihazların saklama alanlarında saklanmamaktadır.
6. Kullanıcı bilgisayarında, virüs, trojan/truva atı vb. kötü niyetli yazılımları engelleyen güvenlik yazılımları kullanılmalıdır.
7. Kullanıcı cihazları ile sunucu arasında yapılan haberleşmede şifreleme kullanılmaktadır.
8. Şifreyi geri oluşturmak mümkün değildir.
9. Kurum sistemleri ilk kez tanımlanan kullanıcı hesaplarında, ilk girişte şifre değiştirmeye zorlamaktadır.
10. Kullanıcılar, online web şubemiz üzerinden şifrelerini kendileri değiştirebilmektedirler.
11. Terminal/Uç Birim uygulamalardan para transferi yapılamamaktadır. Para transferlleri online web şube üzerinden yapılmaktadır.
12. Terminal/Uç Birim uygulamalar ile birlikte online web şube üzerinden erişim için ikili kimlik doğrulama ( OTP ) kullanılmaktadır.
13. SMS Şifresi, İnternet Şubesimize giriş ve para transfer işlemleri için Bankamız tarafından sistemimizde kayıtlı cep telefonunuza gönderilen tek kullanımlık, 6 haneli bir şifredir. SMS Şifresi giriş ve para transferi işlemlerinde kullanılır.
14. Kullanıcının yaptığı işlemlere ait log/arşiv kayıtları, farklı seviyelerde saklanmaktadır. Kullanıcı bilgisayarında saklanan log/arşiv dosyalarının kapsamını sınırlandırabilmektedir.
15. Sisteme girilen emirlerin log/arşiv kayıtları, herhangi bir uyuşmazlık durumunda kullanılmak üzere, ayrı bir şifreli formatta saklanmaktadır.
16. İnternet Şubemize girerken ya da İnternet Şubesi içerisinde şifre sorduğumuz her alanda bir sanal klavye bulunduruyoruz. Böylece en önemli kişisel bilginiz olan şifrenizi, klavye hareketlerinizi kaydeden (key-logger gibi) kötü niyetli programlardan korumanıza yardımcı oluyoruz.
17. Pay senetleri, borsa yatırım fonları, varantlar, kredili işlem, açığa satış işlemleri, yatırım fonu alım satım işlemleri, vadeli işlem ve opsiyon piyasası işlemleri (VİOP); internet sitesi, veri yayın ekranları ve mobil uygulamalar vasıtasıyla yapılabilmektedir.
18. EFT/Havale, VIOP teminat yatırma ve çekme talimatları da internet sitesi üzerinden iletilebilmektedir. Emir iletiminde ve kabulünde mevzuat hükümlerine uygun hareket edilir. Ayrıca ICBC Yatırım Menkul Değerler A.Ş. tarafından sermaye piyasası aracı, müşteri ve tutar bazında sınırlamalar getirilebilir.
19. Müşterilere yapılan aylık bildirimin içeriğinde; ilgili dönem içerisinde alınan tüm pozisyonlara ilişkin tarih, zaman, fiyat ve miktar bilgileri, kapatılan pozisyonlara ilişkin kesin kar ve zarar tutarları, açık pozisyonlara ilişkin potansiyel kar ve zarar tutarları, ICBC Yatırım Menkul Değerler A.Ş. nezdinde tutulan nakit, menkul ve diğer varlıklara ilişkin tüm hareketler, hesaba tahakkuk ettirilen her türlü komisyon, ücret ve vergiler ile teminat durumlarına ilişkin bilgiler bulunmaktadır. Günlük Bildirim içeriğinde ise; en geç işlemin yapıldığı günü izleyen işgünü içerisinde, bir önceki gün içinde alınan tüm pozisyonlara ilişkin bilgiler iletilir.