EXIMBANK
GRUPPO VENETO BANCA

„POLITICA PRIVIND SECURITATEA TEHNOLOGIILOR INFORMAŢIONALE”

1. PRINCIPII GENERALE

În scopul garantării omogenităţii în cadrul Grupului:

- Compania-mamă (Veneto Banca Holding S.c.p.A) determină regulile şi politicile de Securitate Tehnologiilor Informaţionale valabile pentru întregul Grup, în baza exigenţelor strategice şi de lucru;
- Sucursalele străine, cu excepţia unor eventuale prevederi locale, trebuie să se conformeze propriilor politici de Securitate TI la liniile-directoare din prezentul document.

În cadrul fiecărei instituţii din cadrul Grupului, autorizaţiile privind prelucrarea datelor se atribuie fiecărui angajat ţinând cont de următoarele:

- instituţia de apartenenţă;
- unitatea organizatorică de apartenenţă;
- funcţia ocupată;
- tipul de contract încheiat cu instituţia;
- echipament electronic utilizat.

În baza acestor parametri sunt determinate aşa-numitele matricele de autorizare cu ajutorul cărora sunt identificate serviciile/echipament electronic ce pot fi utilizate în cadrul fiecărui context de lucru în parte (instituţie/unitate organizatorică/funcţie) şi, în caz de necesitate, tipul de acces autorizat.

2. PRINCIPII

Principii referitoare la Securitatea Tehnologiilor Informaţionale reflectă cerinţele stabilite de Codul cu privire la protecţia datelor personale şi se referă la următoarele aspecte:

1. Accesul la echipamente computerizate se acordă doar persoanelor autorizate ce dispun de mandat de autentificare conform funcţiile şi serviciile definite de matricele de autorizare. Pentru a obţine accesul este necesară activarea unei proceduri de autentificare ce ţine de prelucrare specifică sau de o serie de procesări.
2. Politicile privind modalităţile de backup şi restabilirea datelor definesc modalităţile operaţionale necesare pentru garantarea disponibilităţii datelor. Acestea fac parte din cadrul normativ definit de codul de protecţie a informaţiilor personale şi servesc drept suport pentru planurile de Disaster Recovery şi Business Continuity.
3. Informaţiile gestionate de băncile din cadrul Grupului Veneto Banca sunt protejate contra riscului de accesare neautorizată şi deteriorare prin activarea echipamentelor electronice adecvate. Acestea includ:
   - sistemele de protecţie antivirus
   - sistemele de firewall
   - sistemul de detectare a intruziunilor (IDS)
   - sistemele de acces protejat în reţelele publice (servicii VPN)
4. Accesul la instrumentele electronice ale instituţiei de către persoane sau parţi terţe care colaborează în vederea atingerii obiectivelor instituţiei este reglementat de dispoziţii speciale incluse în contractele de furnizare. Asemenea dispoziţii contractuale trebuie să respecte următoarele principii de securitate TI:
   - orice autorizare trebuie să fie asociată cu o declaraţie de responsabilitate pentru rolurile de Persoana responsabilă şi Administrator extern care, periodic, va fi selectată ca cel mai adecvat pentru corespunderea cu cerinţele.
   - în lipsa unei autorizaţii contractuale specifice, se interzice utilizarea echipamentelor electronice instituţionale de către terţi,
   - orice autorizaţie este eliberată prin verificarea prealabilă a corespunderii cu cerinţele de securitate TI şi trebuie să permită accesul doar la informaţiile necesare desfăşurării funcţiei / însărcinărilor solicitate.