# Carta Utilizatorilor pentru protecția informației și utilizarea resurselor IT

**Având în vedere:**

1. **Contractul** încheiat între **Furnizor** si **BRD – Groupe Societe Generale SA** ("**BRD**"), (denumit in continuare "**Contractul**");

2. Specificul activității desfășurate de BRD, care in calitatea de societate bancară are obligatia de a păstra confidentialitatea asupra faptelor, datelor și informatiilor aflate la dispozitia sa, in conformitate cu legislația specifică domeniului financiar-bancar, legislația specifică pieței de capital, precum și cu legislatia specifică prelucrării datelor cu caracter personal;

3. Faptul ca Furnizorul, reprezentantii, salariatii si colaboratorii Furnizorului, implicati in derularea Contractului, au acces in principal la date cu caracter confidential (denumite in continuare Informatii Confidentiale – vezi Glosar)

4. Protecția Sistemului de Informații și a Resurselor Informaționale ale BRD este un element esențial. Această protecție este responsabilitatea tuturor.

Următoarea Cartă confirmă dorința BRD de:

- A-si proteja Resursa Informațională și imaginea sa de marcă.
- A asigura o utilizare corectă și responsabilă a sistemului său de informații.

**Angajatul/colaboratorul/subcontractorul Furnizorului (denumit in continuare "Utilizatorul") ia la cunoștinţă si isi asuma prevederile prezentei Carte.**

**Obiective și domeniu de aplicare**

**Obiective**

BRD pune la dispoziția tuturor Utilizatorilor sistemului său IT un set de resurse IT, precum și informații și date necesare pentru îndeplinirea misiunii lor. În utilizarea acestor resurse, fiecarui Utilizator i se cere să respecte regulile BRD de utilizare și controalele efectuate pentru a permite BRD să se protejeze împotriva tuturor tipurilor de riscuri, cum ar fi frauda, divulgarea de informații, indisponibilitatea sistemului său de informații, criminalitatea informatică sau neconformitatea cu cerințele autorităților de reglementare.
Această Cartă stabilește regulile pentru a asigura securitatea și performanța sistemului IT, pentru a păstra confidențialitatea datelor în conformitate cu legislația în vigoare și cu drepturile și libertățile recunoscute Utilizatorilor. Exemplele menționate în această Cartă nu sunt exhaustive.
Carta se anexează la politicile interne și are același efect ca și acesta.
Datorită evoluției continue a tehnologiilor, această Cartă poate face obiectul unor modificări.

**Domeniul de aplicare**

Fiecare Utilizator al sistemului informațional sau care poate deține Resursele Informaționale ale BRD trebuie să respecte această Cartă.

**Modul de comunicare al Cartei**
Această cartă este opozabila fiecărui Utilizator al Sistemului de Informații sau al Resurselor Informaționale, prin asumarea acesteia prin semnatura, in mod individual.
Carta este comunicată, dacă este necesar, în momentul semnării Contractului. Furnizorul comunică această Cartă, inainte de inceperea activitatii si acordarii accesului, tuturor angajaților, colaboratorilor, reprezentantilor săi carora, în mod excepțional, urmeaza sa li se acorde acces de catre BRD la Sistemul IT sau la Resursele Informaționale ale BRD. Ulterior, Furnizorul transmite BRD Carta semnata de fiecare Utilizator, pe email, la adresa de email a responsabilului de contract din partea BRD.

- Pentru utilizatorii care au acces in mod direct, sau printr-o conexiune destinata angajatilor sau colaboratorilor la Sistemul IT al BRD:
  Utilizatorul declara ca a fost informat si recunoaste in mod expres faptul ca prevederile Cartei, ale reglementarilor si procedurilor BRD mentionate in Carta sunt disponibile in mod continuu in sistemul informatic al BRD la linkul https://intralegis.apps.brd.ro/intranet/ la care are access nerestrictionat, oricand, si nu poate invoca neprimirea vreunei informari regulate sau a versiunilor modificate ale acestora, asumandu-si obligatia de a le consulta periodic si de a se mentine informat la zi cu privire la continutul acestora.

- Pentru utilizatorii care au acces la prin intermediul unui VPN dedicat partenerilor terti la Sistemul IT BRD:
  BRD se angajează să informeze Utilizatorul, direct sau prin intermediul Furnizorului, cu privire la regulile cuprinse în Cartă, in cazul unor modificari semnificative, iar Utilizatorul se angajeaza sa le ia la cunostinta si sa remita documentul semnat catre BRD, la adresa de email a responsabilului de contract din partea BRD, direct sau prin intermediul Furnizorului, in termen de cel mult 5 zile de la comunicarea acestora de catre BRD.

**Reguli privind protecția informației și utilizarea resurselor IT**
**Respectarea confidențialității Informației**
**Clasificarea Informației**
Atunci când utilizează Sistemul IT al BRD, Utilizatorul trebuie să aplice principiile generale:
Păstrarea confidențialitatii asupra tuturor aspectelor legate de activitatea desfășurată în BRD, cu privire la clientii acesteia, precum si orice alte Informatii Confidentiale de care ia cunostinta în desfășurarea activității, în conformitate cu politica de confidențialitate a BRD.

- Respectarea secretului bancar.
- Protecția Datelor Personale.
- Protecția Informațiilor Privilegiate.

În acest scop, Utilizatorul se angajează să defineasca și să actualizeze nivelul de confidențialitate a informațiilor conținute în documentele/mesajele (date nestructurate) pe care trebuie să le creeze sau să le modifice, în conformitate cu scara pe patru niveluri: C0-Public; C1-Restricționat; C2-Confidențial; C3-Secret și să respecte regulile de utilizare aferente. Pentru nivelurile C2 si C3, exista o subsclasificare „Can Leave the Group/Cannot Leave the Group" (Pot părăsi Grupul sau Nu pot părăsi Grupul).
Clasificarea din punctul de vedere al confidențialității se realizeaza si pentru datele structurate (baze de date), ce pot fi accesate prin intermediul aplicațiilor IT puse la dispoziție de către BRD.

**Protecția datelor**
Utilizatorul se angajează să protejeze Resursele Informaționale ale Grupului, în special prin respectarea următoarelor reguli:

- La sediul BRD, prin eliberarea biroului și securizarea documentelor și a echipamentelor înainte de a le lăsa nesupravegheate (blocarea calculatorului, deconectarea sesiunii, cablu antifurt, dulap cu încuietoare etc.).

- Asigurarea faptului că informațiile confidențiale nu sunt lăsate în sălile de reuniune.
- Limitarea imprimării și utilizarea dispozitivelor în conformitate cu nivelul de confidențialitate (coșul de gunoi, containerul securizat, tocătorul etc.) pentru distrugerea acestora.
- În afara sediului BRD, prin utilizarea tuturor mijloacelor de prevenire a furtului (cablu antifurt, seifuri la hotel) și de protecție a informațiilor disponibile (blocarea calculatorului, deconectarea sesiunii, filtre de confidențialitate etc.), pentru a reduce probabilitatea furtului echipamentelor sau informației.
- Păstrarea vigilenței în ceea ce privește riscul divulgării informațiilor în locurile aglomerate (transport public, lifturi, restaurante etc.), prin adoptarea celei mai stricte discreții în ceea ce privește activitățile sale profesionale.
- Neparticiparea la reuniuni telefonice în locuri publice.
- Limitarea strictă a documentelor confidențiale pe suport de hârtie și a circulației acestora în afara sediilor BRD.
- La domiciliu (telemuncă sau in timpul exercitatii obligației de disponibilitate la apeluri de serviciu) sau într-o altă locație la distanță (exemplu de muncă de la sediul unui furnizor de servicii), prin luarea unor măsuri astfel incat informațiile confidențiale sau nepublice să nu fie văzute, audiate sau partajate cu externi neautorizați care pot fi prezenți, prin păstrarea vigilenței cu privire la prezența oricăror obiecte conectate (cameră de securitate, asistenți vocali conectați permanent etc.), în caz de absență, închiderea sesiunii de lucru și protejarea documentelor de văzul altora.
- Păstrarea vigilenței cu privire la orice cerere neobișnuită din partea unei surse nesigure (phishing, frauda telefonică a falsului președinte etc.) și contactarea corespondenților de securitate în caz de îndoială, respectiv efectuarea unui contra-apel pe numarul de telefon inregistrat in sistemele BRD al persoanei care v-a apelat.
- Respectarea procesului de însoțire a vizitatorilor în vigoare în incintele BRD.

**Protecția Datelor Cu Caracter Personal**

Regulamentul general privind protecția datelor cu caracter personal (GDPR) și Actele Normative emise la nivelul Băncii (N1D81, N1D81I1) definesc condițiile în care poate fi efectuată prelucrarea datelor personale și drepturile persoanelor vizate de prelucrare. Astfel, în contextul activității sale profesionale și al executării sarcinilor sale, Utilizatorul trebuie să acționeze în conformitate cu aceste politici și să respecte drepturile și libertățile fundamentale, precum și viața privată a persoanelor vizate, indiferent de prelucrarea pe care ar fi obligați să o realizeze.

Utilizatorul isi asuma faptul că datele cu caracter personal prelucrate in numele BRD nu sunt comunicate sau utilizate sub nicio formă în scopuri care sunt străine sau contrare sarcinii care i-a fost încredințată în temeiul Contractului, precum în scopuri personale sau în contextul activităților desfășurate în afara BRD.

În cazul unor nelămuriri referitoare la cadrul normativ specific, Utilizatorul este invitat să contacteze Celula Protecția Datelor Personale (PDPO) prin utilizarea adresei dedicate pdpo@brd.ro.

Presupunând că Utilizatorul este cauza unei încălcări a securității datelor cu caracter personal (pierderea disponibilității, integrității sau confidențialității datelor cu Caracter Personal), acesta trebuie să notifice cât mai curând incidentul conform procedurilor în vigoare în cadrul BRD (de ex. N1D81I1P1), pentru ca departamentele abilitate să poată informa, dacă este necesar, autoritățile de supraveghere în cauză, în termenul de 72 de ore de la data la care s-a luat cunoștință de producerea incidentului care vizează date cu caracter personal și, dacă este cazul, să informeze persoanele vizate de respectiva încălcare a securității datelor. Reguli generale pentru utilizarea sistemului IT al BRD.

**Reguli generale pentru utilizarea sistemului IT al BRD**

**Responsabilitatea Utilizatorului**

Accesul la resursele IT ale BRD este furnizat utilizatorilor în scopuri profesionale și în funcție de necesitățile BRD. Aceasta înseamnă că un mesaj trimis sau primit de la un echipament IT furnizat Utilizatorului are un caracter profesional, cu excepția cazului în care este utilizat în contextul sectiunii §2.2.3 „Utilizare privată/în scop personal”.

Fiecare Utilizator are obligatia de a se informa periodic cu privire la regulile aplicabile privind utilizarea sistemului IT și protecția informațiilor BRD, prin accesarea acestora directa, la linkul https://intralegis.apps.brd.ro/intranet/ .
Prin urmare, fiecare Utilizator este responsabil pentru folosirea resurselor IT care ii sunt încredințate.
În cazul deteriorării echipamentului și în absența oricărei neglijențe sau erori din partea Utilizatorului, BRD va suporta costul echipamentului.
Responsabilitatea Utilizatorului va fi angajată dacă acesta se face răspunzător de o utilizare neconformă. În acest sens, autentificarea și jurnalele sunt mijloace de dezvăluire a identității Utilizatorului.
Nerespectarea regulilor definite în prezenta Cartă poate duce la aplicarea de măsuri disciplinare pentru autorul său, într-un mod adecvat și proporțional, în conformitate cu amploarea sancțiunilor prevăzute în procedura aferentă regulamentului intern. Exemple de abateri de la reguli ce pot duce la aplicarea unor sancțiuni disciplinare:

a. Pentru toți Utilizatorii: divulgarea de informații sensibile (C2 sau C3), stocarea parolei în text clar, consultarea repetată a atașamentelor sau linkurilor suspecte, descărcarea și instalarea de pachete neaprobate sau ocolirea normelor de securitate pe echipament.
b. Pentru Utilizatorii IT (cu privilegii elevate), se adaugă, pe langa cele pentru toti utilizatorii: stocarea și partajarea parolelor sau secretelor administratorului/serviciului, utilizarea parolei contului administratorului/serviciului fără respectarea normelor interne, ocolirea procesului de securitate sau neimplementarea securității din proiectare.

Utilizatorul trebuie să contacteze corespondentul de securitate (CyberAlert@brd.ro) sau superiorul său ierarhic de îndată ce suspectează o încălcare a securității sau un posibil atac asupra sistemului IT al BRD. Acesta nu este responsabili de alertarea altor Utilizatori.

**Accesul la resursele BRD**

Fiecare Utilizator primește drepturi individuale de acces la Sistemele Informatice ale BRD/Grupului prin mijloace confidențiale de autentificare (coduri confidențiale, smartcards etc.). Acest drept de acces nu poate fi, în niciun fel, transmis, nici măcar temporar, unei terțe părți fără a angaja responsabilitatea Utilizatorului. Mijloacele de autentificare sunt strict personale și trebuie folosite numai pentru uzul Utilizatorului. Utilizatorul este responsabil pentru confidențialitatea acestora.
Prin urmare, Utilizatorul trebuie, în special:

- Să aleagă coduri confidențiale care să fie conforme cu politica BRD privind parolele, inclusiv privind complexitatea, să le păstreze secrete și să le actualizeze în funcție de frecvența stabilită de BRD sau imediat ce apare suspiciunea că a fost compromisă. (Atentie! Schimbarea de la distanta a parolei de acces in domeniu – parola de Windows – este posibila numai in intervalul de valabilitate al acesteia.)
- Să se angajeze să nu acorde utilizatorilor neautorizați acces la sistemele IT, prin intermediul materialelor pe care le utilizează.
- Să blocheze sesiunea software/sistem înainte de a lăsa echipamentul nesupravegheat.
- Să nu utilizeze sau să încerce să utilizeze un alt cont de utilizator decât cel propriu sau să încerce să-și ascundă adevărata identitate.
- Să nu evite/dezactiveze mijloacele de securitate și de monitorizare (de ex: screen-saver, setari de retea, instrumente de preventie a malware-ului, agenti EDR, DLP, AIP).
- Să nu își utilizeze dreptul de acces la sistemul IT în alte scopuri decât cele pentru care a fost acordat dreptul de acces.
- Să nu lase nesupravegheate smartcardul – pe care trebuie sa il aiba tot timpul asupra sa - si/sau telefonul unde este instalata aplicatia Mobile Phone Soft Token; sa nu comunice niciodata nimanui PIN-ul telefonului si PIN-ul aplicatiei OTP.
- Să nu conecteze la reteaua de date din sediile BRD alte dispozitive decât cele autorizate.
- Să utilizeze resursele sistemului IT în cadrul strict al activității sale profesionale, definit de funcția sa și în limitele atribuțiilor sale sau ale delegărilor care îi sunt acordate. Informațiile clasificate la orice nivel superior nivelului C0-Public pot fi folosite sau consultate exclusiv în scopuri comerciale

și în niciun caz nu trebuie utilizate sau consultate din motive personale sau pentru a-și satisface curiozitatea.

-

*1.1.1.1 Accesarea de la distanta a Sistemului IT BRD*

Pentru accesarea de la distanta a Sistemului Informatic BRD, se foloseste o solutie de VPN. In cazul in care se foloseste solutia VPN TMA pusa de dispozitie de catre Grupul SG, Utilizatorul primeste suplimentar un cont de acces in solutia Grupului SG.

*1.1.1.2 Reguli pentru accesarea de la distanta a Sistemului IT BRD*

i. Evitarea utilizarii punctelor publice de acces Internet (ex: free-WiFi, aeroport, restaurante, hoteluri, etc.).
ii. Utilizarea, legitima, a punctului de acces internet propriu, cu caracteristici de securitate superioare (ex. router WiFi minim WPA2/3 – cu parola complexă, hotspot de pe telefon mobil furnizat de **Furnizor/BRD**, setat cu parolă complexa). Evitarea partajarii echipamentului propriu WiFi cu alte persoane din vecinătate.
iii. Evitati utilizarea aparaturii de înregistrare foto-video, sau programe de inregistrare a ecranului pentru a extrage informaţii de pe dispozitivul de lucru.

Dreptul de acces al Utilizatorului încetează automat atunci când părăsește Furnizorul si/sau BRD (ieșirea din câmpul muncii, demisie sau încheierea contractului). De asemenea, acesta poate fi modificat ca urmare a schimbării felului muncii și/sau în conformitate cu cerințele comerciale.
Utilizatorului i se pot acorda drepturi de acces privilegiate la Sistemul IT pe care le poate exercita numai în scopul pentru care i-au fost acordate aceste drepturi. În cazul în care Utilizatorul detine drepturi de acces privilegiate, acesta trebuie sa respecte regulile specifice din sectiunea §2.4. Obligatii legate de utilizarea conturilor pentru accese privilegiate.

**Utilizare privată/în scop personal**

Utilizarea rezonabilă a sistemului IT în scop personal (accesarea site-urilor web, trimiterea de e-mailuri, stocarea fișierelor, telefonia, tipărirea, fotocopierea, scanarea etc.) este tolerată în cadrul nevoilor zilnice și al cadrului de viață al familiei. Această toleranță este condiționată de respectarea de către Utilizator a principiilor prevăzute în prezenta Cartă.
Utilizarea în scop personal trebuie să fie limitată, ca durată și frecvență, și nu trebuie să aibă impact asupra activității profesionale a Utilizatorului.
În contextul unei utilizări în scop personal a sistemelor informatice, Utilizatorului i se solicită următoarele:

- Dacă utilizează un director de fișiere, să identifice numele acestui director prin cuvântul cheie „[prv]” sau orice alt identificator clar și neechivoc al naturii private a informațiilor.
- Dacă se tipărește un document privat, să se identifice numele documentului cu cuvântul cheie „[prv]”.
- În cazul în care transmite e-mailuri sau orice altă formă de mesaj (de exemplu, sms), să menționeze în câmpul subiect cuvântul cheie „[prv]” (sau la începutul mesajului atunci când câmpul subiect nu există).
- În cazul în care doresc să primească e-mailuri sau orice altă formă de mesaje (de exemplu, sms), expeditorul trebuie să menționeze în linia de subiect cuvântul cheie „[prv]”[1] (sau la începutul mesajului atunci când câmpul de subiect nu există). Fiecare Utilizator trebuie să își informeze corespondenții atunci cand comunica adresa de e-mail profesional pentru utilizare în mod privat.

[1] *Indiferent de accente sau litere mici/majuscule; prin urmare, va fi acceptat, de exemplu "*

*[Prv], [pRV], ... "*

Aceste mesaje vor fi supuse acelorași proceduri de inspecție tehnică precum cele definite la sectiunea §3 „Măsuri de control și supraveghere”.

Nicio informație de natură profesională nu poate beneficia de cuvântul cheie [prv]. Ca atare, aceasta nu poate fi stocata în directorul de fișiere „[prv]”, nici imprimata, fotocopiata, scanata cu cuvântul cheie „[prv]”, nici trimisa sau primita de Utilizator prin e-mail sau prin orice altă formă de mesaj cu subiectul „[prv]”. BRD își rezervă dreptul de a bloca transmiterea unui mesaj sau a unui document marcat cu „[prv]” în cazul în care sunt detectate informații profesionale (a se vedea articolul §3 „Măsuri de control și supraveghere”). Utilizatorul va primi ulterior un e-mail prin care va fi informat cu privire la blocarea automată a trimiterii și se poate adresa la ierarhia sa pentru orice solicitare de deblocare a trimiterii mesajului respectiv.
Utilizarea în scop personal a Sistemelor IT este singura și întreaga responsabilitate a Utilizatorului. BRD nu va impune/aplica măsuri specifice de securitate pentru protecția conținutului privat.
În cazul în care se dovedește, prin indicații precise și consecvente, faptul că Utilizatorul folosește în mod abuziv sau malițios cuvântul cheie „[prv]” sau că are posibilitatea de a utiliza resursele BRD în scopuri personale, BRD va avea dreptul de a atrage toate consecințele disciplinare și, eventual, judiciare.
Utilizarea abuzivă a etichetei „[prv]” poate fi dedusă, de asemenea, din detectarea automată a conținutului, frecvența mesajelor primite sau trimise, volumul datelor schimbate, stocate sau imprimate, atașamente și durata conexiunii.
BRD va putea citi conținutul mesajelor și al dosarelor private pe baza respectării reglementărilor în vigoare și, în special, a secretului corespondenței.

**Reguli privind utilizarea echipamentelor și a instrumentelor digitale profesionale**
Instrumentele și conturile Utilizatorilor utilizate în contextul profesional trebuie să fie cele autorizate de BRD. Listă ne-exhaustivă de exemple:

- Schimburile de fișiere trebuie efectuate prin instrumente validate de BRD în conformitate cu regulile de confidențialitate. De exemplu, este descurajata utilizarea platformelor de tip „cloud” pentru transferul fisierelor de mari dimensiuni (ex. WeTransfer), fiind favorizata utlizarea solutiilor de Grup SG. Pentru transferul documentelor cu dimensiuni cuprinse intre 5MB si 2GB in intern/din extern BRD, trebuie folosite instrumentele puse la dispoziție de catre Banca: Secure Share. Pentru transmiterea in extern BRD, este necesara obtinerea unei autorizari din partea CISO. Pentru transferuri de volume mai mari, se recomanda utilizarea solutiei SecureHub.
- Folosirea mediilor de stocare externe (hard-discuri mobile, USB stick, carduri de memorie, CD/DVD, inscriptoare optice) reprezintă de asemenea un factor major de risc și este implicit interzisă (detalii în N10D1I5).
- Orice schimb de mesaje privind subiectele sensibile, strategice sau comerciale trebuie realizat prin instrumente validate de BRD, inclusiv cele aferente dispozitivelor mobile smartphone.
- Toți identificatorii profesionali (conturi) trebuie să fie utilizați într-un context strict profesional și nu trebuie să fie comunicați pe site-uri neautorizate de BRD.
- O adresă de e-mail personală (respectiv neprofesională) trebuie utilizată pentru înregistrarea pe site-uri externe (cu excepția activităților profesionale autorizate).
- Transferul automat al e-mailului de business în e-mailul personal (adică non-business) nu este permis. Transferul către e-mailul profesional al unui alt angajat sau către un e-mail profesional partajat poate fi realizat numai la inițiativa angajatului însuși. În cazul în care contextul profesional impune acest lucru și dacă transferul e-mailului nu este implementat, angajatul va trebui să își configureze e-mailul pentru a trimite un mesaj în care să desemneze persoana (persoanele) de contact în timpul absenței sale.
- Datorita riscurilor asociate cu transmiterea documentelor interne BRD catre adresa private de e-mail, acest lucru este implicit interzis.

**Reguli de utilizare a echipamentului**

Indiferent dacă este vorba de echipamente furnizate de BRD sau de echipamente personale utilizate în scopuri profesionale (BYOD), Utilizatorul se angajează să ia măsurile necesare pentru a garanta securitatea informațiilor profesionale și trebuie să respecte în special următoarele reguli:

- Păstrarea vigilenței în ceea ce privește accesarea Echipamentului de către terți.
- Respectarea configurației de bază a echipamentului, respectiv cea standard BRD, sau a soluției de securizare instalate pe echipament.
- Efectuarea întreținerii și aplicarea actualizărilor necesare.
- Notificarea suportului pentru utilizatori (MyIT_Support@brd.ro) și/sau a corespondentului său de securitate (CyberAlert@brd.ro) în cazul unei funcționări defectuoase, defecțiuni, alterări, furturi, pierderi sau încălcări de securitate ale terminalului (laptop sau smatphone).

În plus, în ceea ce privește echipamentele personale utilizate în scopuri profesionale, Utilizatorul se angajează, de asemenea, să respecte regulile privind dreptul de acces descrise la sectiunea §2.1.1 „Clasificarea informației", precum și regulile privind confidențialitatea menționate la sectiunea §2.1.2 „Protecția datelor".

Prin folosirea echipamentului personal in scopuri profesionale, Utilizatorul accepta si regulile de securitate asociate, respectiv :

i. instalarea de aplicatii de protectie impotriva amenintarilor cibernetice (ex. antivirus/anti-malware, tunel VPN, firewall aplicativ, containerizare etc.), actualizate la zi;
ii. sistemul de operare, precum si toate componentele software utilizate (browser, aplicatii software etc.), sa aiba patch-urile de securitate aplicate la zi;
iii. respectarea regulilor de la sectiunea §2.2.2 Accesul la resursele BRD

Anumite aplicații publice, negestionate sau neaprobate de către BRD pot fi accesibile utilizatorului. Aceste aplicații prezintă riscuri și, în special, pot colecta informații fără cunoștința Utilizatorului, cum ar fi date tehnice (tipul dispozitivului, versiunea sistemului de operare etc.), date de utilizare (data și ora instalării, utilizarea etc.), precum și anumite elemente de date cu caracter personal (geolocalizare, vârstă, preferințe etc.). Utilizarea sau descărcarea acestor aplicații în scopuri profesionale pe echipament se poate realiza numai după ce au fost validate anterior de echipele de securitate Acestea pot fi solicitate la MyIT_Support@brd.ro (daca echipamentul apartine BRD), acestea fiind instalate numai de catre tehnicianul de suport IT dupa ce au trecut prin circuitul de aprobare.

**Reguli de utilizare a internetului**

*1.1.1.3 Navigare pe internet*

BRD oferă acces la internet tuturor Utilizatorilor Sistemului său IT, în funcție de nevoile de business. E de așteptat ca Utilizatorii să consulte numai site-urile web care au o legătură directă și necesară cu activitatea profesională desfășurată. BRD își rezervă dreptul de a filtra în mod implicit categoriile de site-uri și de a bloca descărcările de pe anumite site-uri. Regulile și procesele asociate sunt reglementate de politica de filtrare a navigării pe internet.

Utilizatorul trebuie să fie deosebit de vigilent în ceea ce privește conținutul consultat, descărcat și schimbat pe site-uri, utilizând accesul la internet furnizat de BRD. În special, se interzice:

- Transmiterea sau publicarea de informații confidențiale sau nepublice despre BRD, filialele acesteia sau, în general, despre entitățile BRD sau din Grupul BRD, clienții sau partenerii acesteia sau despre forța de muncă a acesteia (cu excepția cazului în care este autorizată de ierarhie și protejată prin mijloace validate adecvate).
- Descărcarea, transmiterea sau stocarea conținutului de natură pornografică, pedofilă, rasistă, xenofobă, violentă sau defăimătoare, care conține orice incitare la ură, subminând respectul față de persoana umană și demnitatea, incitând la comiterea oricărei crime sau infracțiuni, promovând terorismul sau orice conținut care contravine ordinii publice sau ofensator sau care încalcă imaginea mărcii interne sau externe a BRD.
- Comiterea de acte reprobabile cu privire la legislația aplicabilă, în special în ceea ce privește respectarea drepturilor de proprietate intelectuală.
- Participarea la jocuri de noroc.

- Desfășurarea unei activități comerciale în nume propriu.
- Crearea sau administrarea de servicii de internet sau de comunicații electronice care nu au legătură cu necesitățile activității sale profesionale.
- Accesul la serviciile de e-mail externe (webmails), mesagerie instant (chat) externe și la rețelele sociale. Accesul la anumite retele sociale este acordat pe baza de derogare, pentru utilizare in scop profesional.

Descărcarea programelor este permisă numai persoanelor autorizate în mod explicit. Utilizatorul trebuie să aibă grijă să nu supraîncarce sistemul IT al BRD în mod abuziv, în special prin limitarea transferurilor de fișiere de mari dimensiuni sau a accesului la anumite resurse multimedia.

*1.1.1.4 Rețele sociale*

Ca parte a utilizării în scop profesional a rețelelor sociale, Utilizatorul se abține de la divulgarea de informații confidențiale cu privire la BRD, activitatea sa profesională, rolurile și responsabilitățile colegilor sau ale clienților săi și se angajează să respecte regulile de comunicare emise de BRD, în special în ceea ce privește respectarea confidențialității bancare si a secretului profesional. Utilizatorul nu trebuie să se angajeze în controverse care prezintă un risc pentru imaginea BRD.

În plus, sunt interzise mesajele ofensatoare, care denigrează sau care ar putea încălca viața privată, imaginea sau reputația angajaților și a Băncii. BRD va avea dreptul de a atrage toate consecințele disciplinare și eventual judiciare.

**Reguli privind utilizarea instrumentelor de mesagerie și de comunicare internă**

BRD pune la dispoziția utilizatorilor sistemului său IT un set de mijloace de comunicare (e-mail, mesagerie instant, comunități interne etc.).

Este interzisă transmiterea, retransmiterea sau publicarea mesajelor defăimătoare, abuzive, denigratoare sau care pot aduce atingere vieții private a persoanelor, imaginii, reputației sau considerației persoanelor și mesajelor care ar contraveni legislației în vigoare. Astfel de mesaje ar putea angaja responsabilitatea Utilizatorului și a BRD.

Utilizatorul nu trebuie să transmită mesaje precum alarme false sau zvonuri (informații neverificate care ar putea induce în eroare pe cineva).

Utilizatorul trebuie să depună eforturi pentru a limita numărul și dimensiunea atașamentelor pentru a evita supraîncărcarea rețelei. De asemenea, acesta trebuie să utilizeze cu înțelepciune listele de corespondență și să evite trimiterea de copii către un număr nejustificat de destinatari.

Pentru a primi/trimite informaţie sensibila (C2/C3, DP2/DP3) în intern BRD/Grup SG, Utilizatorul trebuie sa-si securizeze mesageria folosind un **certificat digital intern.** Certificatul digital intern permite folosirea funcţiei „Encrypt" pentru protejarea conţinutului mesajului și/sau atașamentelor acestuia trimise numai în intern BRD/Grup SG. Transmiterea informaţiei sensibile în extern BRD/Grup SG se face prin arhivare și parolare conform Ghidului pentru parolarea documentelor sensibile, folosind parole complexe.

In cazul in care Utilizatorul primeste un mesaj care ii ridica suspiciuni (utilizator necunoscut sau mesaj neobisnuit de la un utilizator cunoscut sau orice alte suspiciuni), acesta trebuie sa apese butonul « Mesaj suspect ».

**Obligatii legate de utilizarea conturilor pentru accese privilegiate**

*Pentru fiecare persoană care are un cont privilegiat pe o stație de lucru/server (fizic sau virtual)[2]*

*Un cont pentru acces privilegiat pe stația de lucru/server v-a fost furnizat ca parte a activității dvs. A detine un cont pentru accese privilegiate reprezintă o responsabilitate ridicata pentru protectia securitatii informatiei.*

*Reguli:*

- *Folosiți numai un cont dedicat, cvasi-nominal, pentru acțiunile de administrare;*

[2] *Ex. Windows: Administrator Domeniu, Administrator, Grup Administrator local; UNIX-like: root, sudo; conturi DBA si middleware etc.*

- *Atunci când definiți o parolă, asigurați-vă că aceasta este conformă cu politica de parole a Société Générale și/sau BRD (**Ghidul 50**). Parola trebuie să fie schimbată în mod regulat;*
- *Instalați numai aplicații de la o sursă de încredere (site-ul web al editorului trebuie să fie preferat), fără scopuri malițioase sau ilegale;*
- *Asigurați-vă că aplicația pe care doriți să o instalați nu este deja disponibilă în aplicatia "Service Catalog". În plus, asigurați-vă că respectați aspectele legate de licențiere;*
- *Păstrați aplicația actualizată și efectuați actualizarea de îndată ce editorul pune la dispoziție actualizarea;*
- *Solicitați un cont privilegiat numai atunci când această utilizare este strict necesară, și nu în mod sistematic;*
- *Nu divulgați nimănui credențialele dvs. de administrator;*
- *Nu vă păstrați parola în format text pe un suport fizic (de exemplu, un bilețel) sau logic (de exemplu, un fișier text).*

*Aceste acțiuni sunt interzise:*

- *Crearea sau mutarea unui utilizator în grupul de administratori;*
- *Modificarea altor Grupuri;*
- *Editarea privilegiilor de sistem sau a grupurilor utilizate de servicii;*
- *Editarea sau eliminarea parametrilor de securitate ai stației de lucru/serverului;*
- *Editarea sau modificarea caracteristicilor instrumentelor de securitate;*
- *Editarea configurației stației de lucru/serverului în orice scop, fără permisiunea scrisă expresă a CESI (proces de derogare – conform **Anexelor 4-12** din **N10D1I5**);*
- *Instalarea unui program (instrument, software, freeware, etc.) fără permisiunea scrisă expresă a managerului dvs. și a CESI (proces de derogare – conform **Anexelor 4-12** din **N10D1I5**).*

*Fiecare persoană care are un cont pentru acces privilegiat pentru a lucra pe stația de lucru/server (fizic sau virtual) trebuie să respecte regulile enumerate mai sus. Semnarea acestei anexe nu reprezintă o justificare pentru solicitarea dreptului de administrator local. Ea certifică faptul că sunteți conștient(ă) de obligațiile pe care le aveți în ceea ce privește utilizarea acestui tip de cont.*
*În plus, fiecare persoană vizată de acest document trebuie să acționeze în conformitate cu legislația națională, regulile si procedurile din cadrul BRD și bunele practici legate de activitatea sa. Nerespectarea celor de mai sus poate avea urmări legale.*

**Măsuri de control și supraveghere**

BRD își rezervă dreptul de a monitoriza utilizarea Resurselor IT și a Resurselor Informaționale, în conformitate cu cadrul juridic și cu viața privată a utilizatorilor, pentru:

- Asigurarea securității Sistemului IT și a Resurselor Informaționale.
- Asigurarea respectării regulilor definite în prezenta cartă.
- Îndeplinirea obligațiilor care decurg din actele cu putere de lege și reglementările care guvernează activitățile instituțiilor de credit și ale societăților de investiții.

**Măsuri de control și jurnale**

Prin urmare, se pot institui măsuri de control, ca de exemplu:

- Verificarea software-ului instalat pe stațiile de lucru furnizate de BRD, pentru a se asigura că niciun software rău intenționat nu compromite echipamentul Utilizatorului.
- Verificarea că mecanismele de protecție instituite de BRD pentru echipamentele profesionale și personale utilizate în contextul profesional nu sunt dezactivate.
- Verificarea conținutului e-mailurilor sau al oricăror alte forme de mesaje/fișiere/directoare/documente care sunt stocate/trimise/transferate/imprimate în software-ul și echipamentul furnizate de BRD pentru a asigura securitatea Sistemului IT si a Resurselor Informaționale.

Blocarea e-mailurilor care conțin documente identificate ca nefiind autorizate să părăsească Grupul BRD/BRD. Utilizatorii vor primi ulterior un e-mail prin care sunt informați cu privire la blocarea automată a acestei trimiteri și se pot referi la superiorul lor pentru orice solicitare de deblocare a trimiterii respectivului e-mail.

Filtrarea fluxurilor expuse la internet.

Blocarea accesului la site-uri neautorizate.

La un nivel mai general, orice măsură de control necesară pentru a menține securitatea Sistemului IT și a Resurselor Informaționale ale BRD poate fi pusă în aplicare.

Funcționarea măsurilor de control este responsabilitatea administratorilor de sistem a căror obligație de confidențialitate este prevăzută la punctul §3.3 „Obligația de confidențialitate a administratorilor de sistem" din prezenta cartă.

În conformitate cu principiile transparenței și proporționalității, se atrage atenția Utilizatorilor asupra faptului că dispozitivele de securitate informatică (firewall, sisteme de control al accesului etc.) instituite de BRD generează jurnale ale sistemelor care permit identificarea evenimentelor (autentificarea la o sesiune, ștergerea fișierelor, utilizarea aplicațiilor etc.). Aceste jurnale pot fi apoi corelate între ele pentru a investiga cauzele unui eveniment care are sau ar putea avea un impact asupra securității Sistemelor IT și a Resurselor Informaționale.

Jurnalele colectate de BRD includ următoarele informații (listă necompletă):

Mesaje trimise sau primite.

- Toate resursele accesate de Utilizator prin internet cu detalii, cum ar fi parametri tehnici de conectare (inclusiv ID-ul contului de utilizator, data și ora, volumul datelor transmise...).
- Autentificarea utilizatorului cu scopul accesării resurselor IT cu detalii, cum ar fi data și ora accesului.
- Lista parametrilor tehnici necesari pentru gestionarea serviciilor de e-mail (identificarea contului de utilizator, datele de contact ale destinatarului, data și ora, volumul, formatul și natura documentelor atașate etc.).

Pot fi păstrate jurnale în conformitate cu politicile interne relevante și cu reglementările aplicabile.

**Exploatarea jurnalelor**

În scopuri operaționale, se realizează o exploatare statistică a jurnalelor, în mod anonim. Acesta constă, în special, în stabilirea de statistici privind conexiunile și contactele efectuate.

Cu toate acestea, BRD poate efectua audituri nominale privind jurnalele, în urma unei defecțiuni, a unei alerte de securitate sau a prezumției de utilizare neconformă a resurselor informatice, respectând totodată confidențialitatea corespondenței private menționate la punctul §3.3 „Obligația de confidențialitate a administratorilor de sistem".

În acest caz, constatările materiale sunt destinate identificării diferitelor circumstanțe ce vor clarifica BRD cu privire la posibila realizare a unei utilizări neconforme și cu privire la identitatea autorului acesteia.

**Obligația de confidențialitate a administratorilor de sistem**

Administratorii de sistem asigură funcționarea normală și securitatea rețelelor și a sistemelor.

Prin urmare, prin funcțiile lor, aceștia pot avea acces la toate informațiile referitoare la utilizatori.

Aceștia au obligația de a respecta confidențialitatea și trebuie să respecte procesele și regulile legate de activitatea lor.

În acest context, Administratorii nu trebuie să divulge aceste informații în cazul în care acestea intră sub incidența confidențialității corespondenței private sau intră în sfera de confidențialitate a utilizatorilor și nu pun sub semnul întrebării funcționarea tehnică corespunzătoare a aplicațiilor, securitatea sau interesul BRD.

**Măsuri tehnice și administrative**
În scopuri tehnice sau administrative, accesul la resursele IT poate fi suspendat, restricționat sau eliminat, individual sau colectiv, dacă este necesar, în special pentru a menține disponibilitatea sau integritatea Sistemului Informațional al BRD și protecția Resurselor Informaționale ale BRD.

**Documente normative**
N1D41I2 - „Clasificarea și protecția Informației"
Ghid 50 – „Identificarea si autentificarea utilizatorilor in sistemul informatic BRD"
N10D1I5 – „Reguli de securitatea informatiei aplicabile dispozitivelor (fixe si mobile) de acces la SI BRD, mijloacelor de comunicare electronică și de lucru colaborativ si dispozitivelor externe de stocare. Gestiunea derogarilor (exceptiilor) InfoSec"
N1D81 - Asigurarea protecției datelor cu caracter personal
N1D81I1 - Prelucrarea, Protecţia și Securitatea Datelor cu Caracter Personal
N1D81I1P1 – Managementul încălcărilor de securitate a datelor cu caracter personal

**Glosar**
Informații confidențiale: toate informațiile care pot fi comunicate Utilizatorilor numai pe baza principiului necesității de a cunoaște și a căror divulgare ar avea un impact de nivel Ridicat asupra BRD si/sau a Grupului, a entităților acestuia sau a persoanei sau persoanelor în cauză. Informațiile privilegiate sunt incluse cel puțin în acest nivel de clasificare. Exemple de informatii confidentiale:

**a) informații referitoare la activitatea desfasurata de BRD** – in aceasta categorie sunt incluse, fara a se limita la, urmatoarele: informatii/date privind platforme si configuratii de sisteme informatice, know-how, munca de creatie sau experimentala, idei, concepte, tehnici, specificatii, planse, schite, diagrame, programe de calculator, codificari, coduri sursa, operatiuni legate de instalarea, utilizarea si/sau intretinerea de software/hardware, documente de licitatie, proiecte de produse noi, informatii comerciale, financiare, fiscale, tehnice privind activitatea BRD, baze de date privind furnizorii, informatii referitoare la relatia BRD cu furnizorii/Furnizorii sai, inclusiv informatiile de orice natura obtinute despre furnizori/Furnizori, informatii referitoare la relatia BRD cu entitatile din cadrul Grupului din care face parte, documente normative interne, note/minute/alte documente interne, procese-verbale privind desfasurarea sedintelor organelor statutare colective si/sau a comitetelor interne si/sau a altor entitati interne, decizii/hotarari ale organelor statutare/comitetelor interne/ale altor entitati interne, informatii care se incadreaza in categoria informatiilor privilegiate in conformitate cu reglementarile specifice pietelor de capital, baze de date privind clientii BRD etc.

**b) informatii referitoare la clientii BRD** - in aceasta categorie sunt incluse, fara a se limita la, urmatoarele: toate faptele, datele, informatiile care privesc persoana clientului (numele/denumirea clientilor, precum si orice alte date de identificare ale acestora) proprietatea, activitatea, afacerea, relatiile personale sau de afaceri ale clientilor (inclusiv situatii financiare ale clientilor, dosare de analiza), informatii referitoare la conturile clientilor – solduri, rulaje, operatiuni derulate – la serviciile prestate de BRD (produsele bancare utilizate de clienti) si/sau la contractele incheiate cu clientii, precum si orice alte informatii referitoare la relatia desfasurata de BRD cu clientii.

**c) informații privind personalul BRD** - în această categorie sunt incluse, fără a se limita la următoarele: orice informații referitoare la salariu, precum și alte drepturi salariale ale angajaților (inclusiv creșterea sau scăderea potențială a salariului), informații cu privire la posturile angajaților, deciziile de angajare, rezultatele testelor și examinărilor anterioare angajarii, informații cu privire la sănătatea și familia angajaților, informații cu privire la performanța angajaților, evaluări și instruire, cheltuieli/costuri pentru dezvoltarea profesională și pregătirea angajaților, conținutul contractului individual de muncă și a contractului colectiv de muncă, precum și orice informații primite direct sau indirect în timpul negocierii contractului colectiv de muncă etc.

**d) date cu caracter personal ale persoanelor fizice care intra in relatie cu BRD, fie in calitate de clienti, clienti prospecti, garanti si/sau imputerniciti ai clientilor persoane fizice, fie in calitate de reprezentanti/imputerniciti/ actionari/ asociati/ garanti ai clientilor persoane juridice -** in aceasta categorie sunt incluse, fara a se limita la, urmatoarele: numele si prenumele clientilor, sexul, data si locul nasterii, cetatenia, semnatura, date de stare civila, date din permisul de conducere, numar de telefon fix, numar de telefon mobil, numar de fax, adresa (domiciliu/resedinta), adresa de e-mail, profesie, loc de munca, formare profesionala - diplome, studii, situatie familiala, situatie economica si financiara, date bancare (ca de ex: numar de card, codul IBAN), imagine, numele de dinaintea casatoriei, etc.

Echipamente: Toate echipamentele puse la dispoziția Utilizatorului de către BRD sau echipamentele personale utilizate în scopuri profesionale (posturi de lucru, telefoane, tablete etc.).
Grup: Se referă la grupul format de Société Générale Persoană Juridică și filialele sale.
Resurse Informaționale: Reprezintă toate informațiile și/sau cunoștințele deținute de Grup (inclusiv informațiile despre clienți, datele cu caracter personal etc.).
Sistem IT: Toate elementele BRD care contribuie la crearea, prelucrarea, circulația și păstrarea informațiilor în cadrul societății (bază de date, software de aplicații, proceduri, documentație etc.), inclusiv sistemul IT propriu-zis (unitate centrală de prelucrare, periferice, sistem de operare etc.).
Informații privilegiate: Informațiile cu caracter precis care nu au fost făcute publice referitoare, în mod direct sau indirect, la emitenții sau instrumentele financiare enumerate pe piețele organizate din Spațiul Economic European (SEE) și care, dacă sunt făcute publice, ar putea avea un efect semnificativ asupra prețurilor instrumentelor financiare respective sau asupra prețului instrumentelor financiare derivate conexe.
Mesagerie instant: Aplicație care permite schimbul instantaneu de mesaje și fișiere între mai multe persoane.
Comunitatea internă: Grup de angajați care formează o comunitate virtuală în utilizarea instrumentelor de comunicare instituite de BRD.
Resurse IT: Se referă la toate elementele hardware ale BRD (posturi de lucru, smartphone-uri, tablete, imprimante, camere de supraveghere video etc.) și la programele informatice (instrumente colaborative, aplicații etc.) care permit Utilizatorului să prelucreze informații în format digital, analogic sau pe suport de hârtie.
Malware (cod malițios): produse software special concepute pentru a perturba, deteriora sau obține acces neautorizat la un sistem informatic, cum ar fi virusul, viermii informaticii, caii troieni sau orice alt cod sau instrucțiune. Acest software poate fi utilizat pentru:

- Infectarea sau afectarea oricărui program, software, date, fișiere, baze de date, calculator sau alte componente hardware sau componente.
- Deteriorarea, compromiterea integrității sau a confidențialității, întreruperea totală sau parțială a operațiunilor normale.
- Deturnarea sau permiterea deturnării integrale sau parțiale a sistemului IT de la utilizarea căreia îi este destinat.

Date cu caracter personal: Orice date sau informații referitoare, în mod direct sau indirect, la persoane identificate sau identificabile, indiferent de tipul de informații, constituie date cu caracter personal.
Aceasta se aplică nu numai prenumelor și numelor de familie, ci și tuturor informațiilor care, combinate cu alte date, pot fi utilizate pentru a identifica persoana (persoana vizată) sau pentru a-i atribui comportamentul unui grup identificat: numărul de contract, adresa, numărul de telefon, numărul de cont, segmentul, punctajul, e-mailul, imaginea, amprenta sau amprenta ADN, identificatorul conexiunii, adresa IP, numărul serial al unui dispozitiv electronic etc.
Caracterul public sau natura nesemnificativa a datelor, faptul că acestea nu permit identificarea directă a persoanelor fizice sau faptul că acestea nu au legătură cu viața lor privată nu exclud aplicarea legii, care acoperă toate informațiile referitoare la o persoană, indiferent de sensibilitatea sa.
Drepturi de acces privilegiate: Drepturi de acces acordate anumitor utilizatori care le permit accesul extins la resursele sistemului informațional, cum ar fi administratorii, managerii.

Corespondent de securitate: Interlocutor de securitate al utilizatorilor Sistemului IT. Releu care face posibilă multiplicarea locală a acțiunilor CISO.
Jurnale: Înregistrare memorată pentru toate evenimentele care au avut loc la nivel de sistem IT. Pot fi utilizate jurnale pentru monitorizarea tehnică a cererilor și pentru investigații în vederea combaterii divulgarilor de informații și a criminalității informatice. Înregistrarea jurnalelor constituie o pistă de audit.
Utilizatori: Se referă la următoarele persoane fizice care utilizează Sistemul IT al BRD:
Persoanele implicate într-un contract de servicii sau de parteneriat cu BRD precum si salariatii, colaboratorii, reprezentantii si/sau subcontractorii acestora.

In cazul in care nu voi respecta prevederile prezentului Angajament, cunosc faptul ca va fi atrasa raspunderea contractuala, patrimoniala si/sau penala.
Am citit, inteleg si respect cele mentionate mai sus,
**Furnizor:** _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
**Contract nr./data:** _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
**Nume si prenume:** _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
**Locul și Data:** _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
**Semnătură[3]:** _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

*[Prezenta Declaratie a fost incheiata la [data], in doua exemplare cu aceeasi putere juridica, unul pentru Banca si unul pentru angajat (utilizator).[4]]*
*[Prezenta Declaratie a fost semnata astazi, [data], prin folosirea mijloacelor de comunicare la distanta, intrand in vigoare la data semnarii acesteia.5]*

*[Prezenta Anexa a fost incheiata la [data], in doua exemplare cu aceeasi putere juridica, cate unul pentru fiecare dintre parti.[6]]*

*[Prezenta Anexa a fost semnata astazi, [data], prin folosirea mijloacelor de comunicare la distanta, intrand in vigoare la data semnarii acesteia.[7]]*

[3] Numai pentru semnatura olografa.

[4] *In cazul semnarii olografe*
[5] *In cazul semnarii digitale*
[6] *In cazul semnarii olografe*
[7] *In cazul semnarii digitale*