Anexa nr. 1
la ordinul ANI nr. 97 din 09.11.2020

CONCEPTUL
de creare a Registrului de stat al persoanelor care au interdicție de a ocupa o funcție publică sau de demnitate publică

INTRODUCERE

În conformitate cu Legea nr.132/2016 *cu privire la Autoritatea Națională de Integritate,* Autoritatea este o autoritate publică independentă faţă de alte organizații publice, faţă de alte persoane juridice de drept public sau privat și față de persoanele fizice, ce funcţionează la nivel naţional ca structură unică.

Din 1 ianuarie 2018, Autoritatea Naţională de Integritate gestionează Sistemul informațional automatizat „e-Integritate", care este destinat depunerii, arhivării, verificării și analizării automate a declarațiilor de avere și interese personale, înregistrării interdicțiilor de ocupare a funcțiilor publice sau funcțiilor de demnitate publică, sau, după caz, a funcției electorale și gestiunii ulterioare a acestor înregistrări, precum și facilitării accesului electronic al persoanelor și instituțiilor interesate la informațiile de interes public.

Autoritatea Naţională de Integritate, ca urmare a sesizărilor recepționate, inițiază procesul de control al averii și al intereselor personale, control privind respectarea regimului juridic al averii, al conflictelor de interese, al incompatibilităților și emite, în baza controlului, un act de constatare, care se publică pe pagina web oficială a ANI.

În condițiile legii, ca urmare a urmare a unui control realizat, finalizat printr-un act de constatare, subiectul declarării urmează a fi înscris în Registrul de stat al persoanelor care au interdicție de a ocupa o funcție publică sau de demnitate publică.

În acest context este necesară extinderea funcționalităților Sistemului informatic „e-Integritate" și elaborarea unei soluții informatice destinate gestiunii subiecților, care au interdicție de a ocupa o funcție publică sau de demnitate publică, sau, după caz, a funcției electorale. În acest sens, Registrul de stat al persoanelor care au interdicție de a ocupa o funcție publică sau de demnitate publică este o soluție de tip *BackEnd* la care dispun de acces utilizatorii autorizați din cadrul Autorității Naționale de Integritate.

Întru asigurarea accesului public la datele Registrului de stat al persoanelor care au interdicție de a ocupa o funcție publică sau de demnitate publică, sau, după caz, a funcției electorale este necesară integrarea acestuia cu pagina web oficială a ANI, unde utilizatorii cu acces anonim vor avea posibilitatea să exploreze datele cu caracter public din Registrul de stat al persoanelor care au interdicție de a ocupa o funcție publică sau de demnitate publică.

Printre beneficiarii direcți ai Registrului de stat al persoanelor care au interdicție de a ocupa o funcție publică sau de demnitate publică, ar putea fi enumerați:

- cetățenii Republicii Moldova, subiecți ai declarării averii și a intereselor personale;
- Autoritatea Națională de Integritate;
- autoritățile administrației publice centrale și locale.

Implementarea Registrul de stat al persoanelor care au interdicție de a ocupa o funcție publică sau de demnitate publică urmează să furnizeze următoarele categorii de beneficii așteptate:

a) Beneficii pentru cetățeni:

- accesul public la informația despre persoanele care au interdicție de a ocupa funcții publice sau de demnitate publică, sau, după caz, a funcției electorale;
- accesul public la informația statistică depersonalizată aferentă persoanelor care au interdicție de a ocupa funcții publice sau de demnitate publică, sau, după caz, a funcției electorale;

- asigurarea încrederii privind transparența și legalitatea proceselor de control efectuate de ANI.

b) Beneficii pentru Autoritatea Națională de Integritate:

- implementarea unor mecanisme moderne de control a respectării regimului juridic al averii, al conflictelor de interese, al incompatibilităților;
- eliminarea necesității interacțiunii directe a funcționarilor ANI cu potențialii solicitanți de informații privind interdicțiile de ocupare a funcțiilor publice sau de demnitate publică, sau, după caz, a funcției electorale;
- automatizarea proceselor de cooperare cu alte instituții în privința completării Registrului de stat al persoanelor care au interdicție de a ocupa o funcție publică sau de demnitate publică.

c) Beneficii pentru autoritățile publice centrale și locale:

- accesul public la informația despre persoanele care au interdicție de a ocupa funcții publice sau de demnitate publică, sau, după caz, a funcției electorale;
- reducerea termenului de obținere a datelor și documentelor privind persoanele cu interdicții de ocupare a funcțiilor publice sau de demnitate publică, sau, după caz, a funcției electorale.

d) Beneficii pentru Republica Moldova:

- asigurarea unor mecanisme eficiente de transparentizare a procesului de accedere a la funcții publice a persoanelor integre;
- asigurarea unui mediu favorabil de integritate a instituțiilor publice.

Capitolul I
DISPOZIȚII GENERALE

1. Registrul de stat al persoanelor care au interdicție de a ocupa o funcție publică sau de demnitate publică (în continuare - RSI) este o parte componentă a SIA „e-Integritate", care asigură automatizarea procesului de înregistrare a interdicțiilor aplicate persoanelor pentru ocuparea funcțiilor publice sau a funcțiilor de demnitate publică, sau, după caz, a funcției electorale, precum și gestiunea ulterioară a acestor înregistrări.

2. RSI constituie o soluție din categoria Guvern către Guvern (G2G) și Guvern către Cetățeni (G2C) și este îndreptată spre asigurarea tranziției de la modalitățile tradiționale de procesare manuală a documentelor pe suport de hârtie spre digitizarea totală și diminuare a intermediarilor procesului de interacțiune a cetățenilor, autorităților publice și instanțelor judecătorești cu Autoritatea Națională de Integritate.

3. Implementarea sistemului informatic va permite sporirea transparenței în activitatea ANI, va standardiza procesele de business și documentele în cadrul activității de control și constatare, va reduce timpul de interacțiune cu potențialii solicitanți de informații privind persoanele care au interdicții, va asigura mecanisme eficiente de transparentizare a procesului de accedere la funcțiile publice și funcțiile de demnitate publică, sau, după caz, a funcției electorale, a persoanelor integre.

4. Destinația RSI. RSI este o componentă informatică necesară implementării interacțiunii ANI cu entitățile externe (cetățeni, autorități publice instanțe judecătorești) în vederea asigurării accesului public la informația despre persoanele care au interdicție de a ocupa o funcție publică sau de demnitate publică, sau, după caz, o funcție electorală.

5. Destinația prioritară a RSI constă în dezvoltarea unui subsistem informatic al SIA „e-Integritate", prin intermediul căruia este asigurată gestionarea datelor cu privire la interdicțiile de ocupare a funcțiilor publice sau de demnitate publică, sau, după caz, a funcției electorale precum și să fie asigurat accesul la informația publică despre persoanele care au interdicție de a ocupa funcții publice sau de demnitate publică, sau, după caz, a funcției electorale.

6. RSI va interacționa direct, prin servicii informatice, cu pagina web oficială a ANI cu scopul publicării informațiilor relevante.

7. Pentru utilizatorii anonimi, RSI, va oferi o interfață a Web cu mecanism de căutare, care va permite accesul și vizualizarea informației publice privind persoanele care au interdicție de a ocupa funcții publice și funcții de demnitate publică, sau, după caz, a funcției electorale. Acest lucru urmează să sporească transparența proceselor de business în cadrul ANI și publicarea automatizată a datelor despre persoanele care au interdicție.

8. Noțiuni de bază și abrevieri.

În sensul prezentului Concept, abrevierile și acronimele utilizate semnifică următoarele:

- APC – autoritate publică centrală;
- APL – autoritate publică locală;
- BD – bază de date;
- ANI – Autoritatea Națională de Integritate;
- E-Gov – IP „Agenția de Guvernare Electronică”;
- RSP – Registrul de stat al populației;
- RSUD – Registrul de stat al unităților de drept;
- SGBD – Sistem de gestiune a bazelor de date;
- SI – sistem informatic;
- TI – Tehnologie informatică;
- TIC - Tehnologie informatică și de comunicare;
- TLS/SSL – protocoale criptografice care asigură comunicarea sigură între 2 noduri ale rețelei de calculatoare pentru acțiuni cum ar fi vizitarea paginilor Web, e-mail, Internet – fax, schimb de mesaje instantanee și alte transferuri de date.

9. Noțiunile și definițiile utilizate în cadrul prezentului Concept, semnifică următoarele:

1) bază de date – ansamblu de date organizate conform structurii conceptuale care descrie caracteristicile de bază și relația dintre entități;

2) credențiale – set de atribute ce stabilesc identitatea și autenticitatea utilizatorilor și sistemelor în cadrul sistemelor informaționale;

3) date – unități informaționale elementare despre persoane, subiecte, fapte evenimente, fenomene, procese obiecte, situații etc., prezentate într-o formă care permite, notificarea, comentarea și procesarea lor;

4) document electronic – informație în formă electronică, creată, structurată, prelucrată, păstrată, transmisă cu ajutorul computerului, altor dispozitive electronice sau mijloacelor software și hardware, semnată cu semnătura digitală;

5) instituție publică – persoană juridică cu statut de:

a) autoritate publică, autoritate administrativă centrală;

b) autoritate subordonată guvernului și structurile organizaționale din sfera lor de competență (autoritățile administrative din subordine, serviciile publice desconcentrate și cele aflate în subordine);

c) instituțiile publice în care ministerul, altă autoritate administrativă centrală are calitatea de fondator), autoritățile/instituțiile publice și organizațiile de stat autonome, subordonate sau înființate de Guvern;

d) Curtea Constituțională, instanța judecătorească, procuratura;

6) flux de lucru – proces administrativ al unei organizații în decursul căruia sarcini, proceduri și informații sunt prelucrate sau executate într-o anumită succesiune dictată de reguli prestabilite (norme procedurale) în scopul realizării unui produs sau furnizării unui serviciu;

7) integritatea datelor – stare a datelor, când acestea își păstrează conținutul și sunt interpretate univoc în caz de acțiuni aleatorii. Integritatea se consideră păstrată, dacă datele nu au fost alterate (șterse);

8) jurnalizare – funcție de înregistrare a informației despre evenimente. În cadrul sistemelor informaționale înregistrările despre evenimente includ detalii despre data și ora, utilizatorul acțiunea întreprinsă;

9) metadate – modalitatea de atribuire de valoare semantică datelor stocate în baza de date (date despre date);

10) obiect informațional – reprezentarea virtuală a entităților materiale și nemateriale existente;

11) resursă informațională – set de informații documentate în sistemul informatic, menținut în concordanță cu cerințele și legislația în vigoare;

12) sistem informatic – ansamblu de programe și echipamente care asigură prelucrarea autonomă a datelor (componenta automatizată a sistemului informațional);

13) sistem informațional – sistem de prelucrare a informației, împreună cu resursele informaționale asociate, cum ar fi resursele umane și tehnice, care furnizează și distribuie informația;

14) tehnologie informatică și de comunicație – termen comun care include toate tehnologiile utilizate pentru schimbul și manipularea informației;

15) veridicitatea datelor – nivel de corespundere a datelor, păstrate în memoria calculatorului sau în documente, stării reale a obiectelor din domeniul respectiv al sistemului, reflectate de aceste date.

10. Scopul creării RSI. Scopul elaborării RSI este asigurarea Autorității Naționale de Integritate cu o soluție informatică performantă pentru automatizarea procesului de înregistrare a interdicțiilor aplicate persoanelor pentru ocuparea funcțiilor publice sau funcțiilor de demnitate publică, sau, după caz, a funcției electorale și gestiunea ulterioară a acestor înregistrări. În acest scop, sistemul informatic prevede colectarea, stocarea, actualizarea și analiza datelor aferente proceselor specifice de gestiune a listei persoanelor cu interdicții.

11. Obiectivele de bază ale RSI. Reieșind din baza legislativă existentă și necesitățile obiective ale actorilor aferenți, pot fi menționate următoarele obiective ale sistemului informatic:

1) automatizarea proceselor de înregistrare automatizată, în urma procesului de constatare, a interdicțiilor de ocupare a funcțiilor publice și funcțiilor de demnitate publică, sau, după caz, a funcției electorale;

2) automatizarea proceselor de interacțiune a Autorității Naționale de Integritate cu actori externi în vederea asigurării accesului la informația conținută în RSI;

3) implementarea unui mediu de colaborare securizat și fiabil care oferă mijloace de integrare informațională pentru sisteme externe cu scopul realizării obiectivelor principale ale RSI;

4) integrarea RSI cu sistemele informatice externe ale autorităților publice și instituțiilor care dețin și gestionează date aferente aplicării interdicțiilor de ocupare a funcțiilor publice și funcțiilor de demnitate publică, sau, după caz, a funcției electorale;

5) furnizarea publicului interesat din Republica Moldova (cetățeni, APC, APL, societatea civilă) a informației veridice și operativă despre persoanele cu interdicții de ocupare a funcțiilor publice și funcțiilor de demnitate publică, sau, după caz, a funcției electorale;

6) sporirea transparenței activității și calității procesului de luare a deciziilor în cadrul instituțiilor publice la angajarea persoanelor în funcții publice și funcții de demnitate publică, sau, după caz, în funcție electorală;

7) furnizarea de informație autentică, veridică, curentă și consistentă tuturor actorilor implicați în procesele de business relevante RSI;

8) reducerea timpului de răspuns și asigurarea suportului informatic procesului decizional;

9) accesul rapid, garantat la date, indiferent de locația utilizatorului autorizat;

10) standardizarea datelor, mesajelor și acțiunilor entităților cu acces autorizat la RSI;

11) reducerea costurilor operaționale, sporirea calității și diversității mijloacelor de comunicare.

12. Implementarea RSI ca parte componentă a SIA „e-Integritate" va furniza ANI un instrument eficient de aplicare a interdicțiilor de ocupare a funcțiilor publice și funcțiilor de demnitate publică, sau, după caz, a funcției electorale, în urma procesului de instrumentare a dosarelor de control și elaborare a actelor de constatare.

13. Sarcinile principale ale RSI. Printre sarcinile principale înaintate sistemului informatic pot fi menționate:

1) furnizarea oportună a datelor relevante activităților de gestiune a interdicțiilor de ocupare a funcțiilor publice sau de demnitate publică, sau, după caz, a funcției electorale;

2) extinderea procesului de examinare a dosarelor de control privind integritatea persoanelor cu etapa de includere, în baza prevederilor actului de constatare, în RSI;

3) formalizarea și eficientizarea proceselor de gestiune a datelor cu privire la interdicțiile persoanelor de a ocupa funcții publice și funcții de demnitate publică, sau, după caz, a funcției electorale;

4) asigurarea și impulsionarea schimbului electronic de date cu terțe părți;

5) reducerea cheltuielilor de colectare și procesare a datelor disponibile prin intermediul platformei de interoperabilitate MConnect;

6) furnizarea cetățenilor a datelor rezultative, cu caracter public despre persoanele care au interdicție de a ocupa funcții publice și funcții de demnitate publică, sau, după caz, a funcției electorale.

14. Principiile de bază ale RSI sânt:

1) principiul legalității, care presupune crearea și exploatarea RSI în conformitate cu legislația națională;

2) principiul respectării drepturilor omului, care presupune exploatarea RSI în strictă conformitate cu legislația națională, tratatele și acordurile internaționale din domeniul drepturilor omului la care Republica Moldova este parte și, în special, cu dreptul la viața privată;

3) principiul integrității datelor, care constă în starea datelor, ce presupune păstrarea conținutului și interpretarea univocă, în condițiile unor acțiuni accidentale. Integritatea datelor se consideră a fi păstrată dacă datele nu au fost denaturate sau distruse (excluse din RSI);

4) principiul veridicității datelor, care presupune introducerea datelor în RSI în baza documentelor autentice, precum și asigurarea unui grad înalt de corespundere a datelor stocate în RSI cu starea reală a obiectelor reprezentate de acestea într-un domeniu concret;

5) principiul plenitudinii datelor, prin care se înțelege asigurarea volumului complet al informației colectate în conformitate cu actele normative;

6) principiul identificării de stat a obiectelor înregistrării, care prevede existența unui cod de identificare unic pentru fiecare obiect;

7) principiul transparenței, care presupune accesul cetățenilor la o serie de informații cu caracter public;

8) principiul controlului formării și utilizării RSI, ce reprezintă totalitatea de măsuri organizatorice și tehnice de program care asigură calitatea înaltă a resurselor informaționale, fiabilitatea înaltă a păstrării lor și corectitudinea utilizării în conformitate cu legislația, precum și care mențin accesul la informație operativ și comod pentru utilizator, conform nivelului de acces;

9) principiul confidențialității informației, care constă în restricționarea accesului persoanelor neautorizate la informația cu accesibilitate limitată în conformitate cu legislația, în scopul neadmiterii ingerinței în viața intimă, familială și privată a subiecților datelor cu caracter personal sau cauzării prejudiciilor persoanei juridice;

10) principiul securității informaționale, care prevede asigurarea nivelului integrității, exclusivității, accesibilității și eficienței protecției datelor împotriva pierderii, alterării, denaturării

și atacurilor, protecția caracterului secret al informației, a integrității și pregătirea pentru lucru atât la nivel de sistem, cât și la nivel de date prezentate în această informație;

11) principiul modularității și scalabilității, ce reprezintă posibilitatea de a dezvolta RSI fără modificarea componentelor create anterior;

12) principiul conformității prelucrării datelor cu caracter personal, care presupune prelucrarea datelor cu caracter personal ale subiectului declarării și ale persoanelor care au interdicție de a ocupa o funcție publică sau de demnitate publică, sau, după caz, a funcției electorale, în conformitate cu prevederile art. 4 din Legea nr. 133/2011 *privind protecția datelor cu caracter personal*;

13) principiul compatibilității RSI, care presupune compatibilitatea RSI cu alte module ale SIA „e-Integritate", precum și cu alte sisteme informaționale publice.

Capitolul II
CADRUL NORMATIV- JURIDIC AL RSI

15. Cadrul normativ-juridic al RSI include legislația națională şi tratatele internaționale la care Republica Moldova este parte.

16. Crearea și funcționarea RSI este reglementată, în particular, de următoarele acte normative și documente de politici:

1) Constituția Republicii Moldova din 29 iulie 1994;
2) Legea nr. 982/2000 privind accesul la informație;
3) Legea nr. 1069/2000 cu privire la informatică;
4) Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat;
5) Legea nr. 71/2007 cu privire la registre;
6) Legea nr. 133/2011 privind protecția datelor cu caracter personal;
7) Legea nr. 91/2014 privind semnătura electronică și documentul electronic;
8) Legea nr. 132/2016 cu privire la Autoritatea Națională de Integritate;
9) Legea nr. 133/2016 privind declararea averii și a intereselor personale;
10) Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate;
11) Decretul Președintelui Republicii Moldova nr. 1743/2004 privind edificarea societății informaționale în Republica Moldova;
12) Hotărârea Guvernului nr. 1140/2017 pentru aprobarea Regulamentului privind activitatea prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice;
13) Hotărârea Guvernului nr. 1141/2017 pentru aprobarea Regulamentului privind modalitatea de aplicare a semnăturii electronice pe documentele electronice de către funcționarii persoanelor juridice de drept public în cadrul circulației electronice ale acestora;
14) Hotărârea Guvernului nr. 562/2006 cu privire la crearea sistemelor și resurselor informaționale automatizate de stat;
15) Hotărârea Guvernului nr. 1123/2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal;
16) Hotărârea Guvernului nr. 710/2011 cu privire la aprobarea Programului strategic de modernizare tehnologică a guvernării (e-Transformare);
17) Hotărârea Guvernului nr. 656/2012 cu privire la aprobarea Programului privind Cadrul de Interoperabilitate;
18) Hotărârea Guvernului nr. 1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);
19) Hotărârea Guvernului nr. 405/2014 privind serviciul electronic guvernamental integrat

de semnătură electronică (MSign);

20) Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog).

21) Hotărârea Guvernului nr. 183/2019 cu privire la aprobarea Conceptului tehnic al Sistemului informațional automatizat „e-Integritate”;

22) Hotărârea Guvernului nr. 228/2020 pentru aprobarea Regulamentului cu privire la organizarea și funcționarea Sistemului informațional automatizat „e-Integritate”.

17. La elaborarea și implementarea RSI trebuie respectate standardele tehnice în materie de dezvoltare a soluțiilor informatice, printre care:

1) Standardul Republicii Moldova SM ISO/CEI 27002:2014 „Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației”;

2) Standardul Republicii Moldova SM ISO/CEI 12207:2014 „Ingineria sistemelor și software-ului. Procesele ciclului de viață al software-ului”;

3) Standardul Republicii Moldova SM ISO/CEI/IEEE 15288:2015 „Ingineria sistemelor și software-ului. Procesele ciclului de viață al sistemului”.

Capitolul III
SPAȚIUL FUNCȚIONAL AL RSI

18. RSI asigură îndeplinirea funcțiilor de bază ale sistemului informațional-tip, precum și îndeplinirea unor funcții specifice, determinate de destinația sistemului, după cum urmează:

1) înregistrarea interdicțiilor de a ocupa funcții publice sau de demnitate publică, sau, după caz, a funcției electorale, ca urmare a constatării încălcărilor în procesul de control privind respectarea regimului juridic al averii, conflictelor de interese și al incompatibilităților, rectificarea și radierea interdicțiilor din RSI;

2) explorarea informațiilor publice despre interdicții, vizualizarea statisticilor publice pe portalul public al ANI;

3) căutarea și vizualizarea autorizată de către utilizatorii SIA „e-Integritate” a informațiilor despre interdicțiile de a ocupa o funcție publică sau de demnitate publică, sau, după caz, a funcției electorale;

4) generarea și exportul de rapoarte în formate predefinite, conform necesităților Autorității;

5) jurnalizarea evenimentelor din RSI privind interdicțiile de a ocupa funcții publice sau de demnitate publică, , sau, după caz, a funcției electorale, atât prin mecanisme interne (integrate în cadrul SIA „e-Integritate”), cât și prin integrarea mecanismelor externe de jurnalizare a evenimentelor de business critice (serviciul electronic guvernamental de jurnalizare - MLog).

19. Funcțiile RSI pot fi dezvoltate prin atribuirea de noi sarcini, ținând cont de prevederile normelor legale din domeniul integrității.

20. Interfața de utilizator a RSI. RSI trebuie să ofere o interfață ergonomică, intuitivă și accesibilă tuturor tipurilor de utilizatori prin intermediul unui explorator web. Registrul trebuie să posede un design grafic inedit, agreabil, echilibrat și distinct resposiv pentru totalitatea dispozitivelor utilizate.

21. În dependență de categoriile utilizatorilor (drepturilor și rolurile acestora), sistemul informatic va furniza o interfață personalizată fiecărei categorii de utilizator.

22. Utilizatorii vor dispune de minim 5 nivele de acces la interfața de utilizator și date:

nivel acces utilizator internet – nivel caracteristic tuturor utilizatorilor internet care dispun de acces la funcționalitățile specifice de afișare a informațiilor cu caracter public furnizate de RSI prin intermediul paginii web a ANI (ww.ani.md);

nivel acces decident ANI – nivel de acces asigurat persoanei cu funcții decidente în cadrul ANI cu rol decident, care va asigura acces la totalitatea funcționalităților de vizualizare a colecției

de date, extragere a rapoartelor și statisticilor, monitorizare și aprobarea/respingerea formularelor electronice perfectate de inspectorii ANI, destinate rectificării/anulării înregistrărilor privind interdicțiile conținute în RSI;

nivel acces inspector de integritate – nivel de acces asigurat inspectorilor de integritate, care va asigura acces la totalitatea funcționalităților necesare vizualizării datelor din RSI, în cadrul procedurilor/dosarelor de control atribuite în gestiune, generare de rapoarte specifice și perfectare a formularelor electronice destinate rectificării/anulării înregistrărilor privind interdicțiile conținute în RSI;

nivel acces administrator de sistem – nivel caracteristic utilizatorului cu cel mai înalt nivel de acces la resursele sistemului informatic. Acest nivel, dat fiind rolul său de a administra buna funcționare a soluției informatice, va asigura acces la toate funcționalitățile interfeței de utilizator și conținutul bazei de date livrate de interfața de utilizator;

nivel acces sistem informatic extern – nivel caracteristic sistemelor informatice externe cu care va sincroniza datele RSI.

23. RSI va furniza interfață bilingvă în limbile română (implicită) și rusă. Procedurile de regăsire a informației și înregistrărilor vor fi realizate prin intermediul unor căutări simple (specificarea unor șiruri de căutare) sau a unor căutări de complexitate mai ridicată, prin intermediul cărora se poate realiza o filtrare mai exactă a informației (formulare QBE). Indiferent de natura informației căutate utilizatorul va utiliza aceeași metodă de interogare și regăsire a informației pentru oricare compartiment al produsului informatic.

24. Adițional la modulul de căutare realizat pe baza principiului QBE, care va da posibilitatea de a afișa rezultatele căutării prin asigurarea posibilității filtrării datelor în lista cu rezultatele căutării.

25. Interfața de utilizator a RSI va asigura un mecanism de filtrare a înregistrărilor ce corespund criteriului de căutare, prezentat utilizatorilor în funcție de drepturile lor de acces.

26. Mărimile indexate (valori din clasificatoare, nomenclatoare) vor putea fi filtrate prin alegerea valorii din liste predefinite. Pentru câmpurile de tip numeric sau dată calendaristică va exista posibilitatea filtrării după valoarea exactă a caracteristicii căutate.

27. Interfața de utilizator a RSI va oferi posibilitatea filtrării rezultatelor după mască, care va permite afișarea înregistrărilor unde toate valorile câmpului filtrat încep cu șirul de caractere specificat, toate valorile câmpului filtrat sfârșesc cu șirul de caractere specificat și toate valorile câmpului filtrat conțin șirul de caractere specificat.

28. Conținutul oricărui tabel cu rezultate sau formă electronică, în funcție de natura informației conținute, urmează să poată fi exportat în formatele: CSV, RTF și PDF.

29. RSI va avea următoarele componente asociate funcționalităților de bază:

1) Gestionarea RSI:

a) Înregistrarea interdicției de ocupare a funcției publice sau de demnitate publică, sau, după caz, a funcției electorale, ca urmare a procesului de control și a prevederilor actului de constatare (conține toate etapele de la perfectarea actului de constatare care prevede interdicție până la marcarea actului de constatare ca definitiv și sincronizarea datelor despre interdicții pe pagina oficială a ANI);

b) procesarea solicitărilor de rectificare/radiere a interdicțiilor (angajatul ANI accesează și completează formularul de adăugare a unei solicitări de rectificare/radiere a interdicției, cu mecanism de atașare a documentelor justificative);

c) aprobarea/respingerea solicitării de rectificare/radiere a interdicțiilor – totalitatea funcționalităților necesare gestiunii procesului de coordonare a solicitării de rectificare/radiere a interdicției cu persoana decidentă din cadrul ANI;

d) căutarea și vizualizarea autorizată a datelor despre interdicții – totalitatea funcționalităților necesare utilizatorilor autorizați ai ANI pentru căutarea informației relevante,

prin completarea formularelor speciale de căutare după o secvență de text, cu opțiuni avansate de căutare în baza regulilor de reducere a arealului de căutare utilizând valorile metadatelor RSI.

2) Publicarea datelor despre interdicții, statistici și indicatorilor cheie de performanță – livrează totalitatea funcționalităților necesare generării, exportării și publicării informației statistice cu caracter public privind activitatea RSI:

a) rapoarte statistice furnizate automatizat de sistem pentru a fi publicate pe pagina web oficială a ANI;

b) date publice detaliate despre interdicții;

c) valori ale indicatorilor de performanță ale ANI.

3) Sincronizarea datelor despre interdicții pe pagina oficială a ANI – funcționalitate automatizată prin intermediul căreia RSI comunică cu pagina web oficială a ANI cu scopul de a publica date privind interdicțiile de ocupare a funcțiilor publice sau de demnitate publică, sau, după caz, a funcției electorale;

4) Rapoarte și statistici – funcționalitate accesibilă persoanelor cu rol decident din cadrul ANI, care permite generarea rapoartelor predefinite și ad-hoc privind conținutul informațional al RSI;

5) Administrarea sistemului – totalitatea funcționalităților de gestiune a clasificatoarelor, nomenclatoarelor, constantelor, variabilelor de sistem necesare pentru buna funcționare a RSI;

6) Jurnalizarea evenimentelor, care include totalitatea funcționalităților de configurare a principiilor de funcționare și generare a evenimentelor care vor fi jurnalizate și de definire a strategiilor de colectare a evenimentelor jurnalizate. Funcționalitatea include atât mecanismul de jurnalizare internă (integrate în cadrul SIA „e-Integritate"), cât și integrarea mecanismelor externe de jurnalizare a evenimentelor de business critice (MLog) .

30. RSI include următoarele contururi funcționale de bază:

1) conturul Autorității:

a) înregistrarea interdicțiilor de a ocupa funcții publice sau de demnitate publică, sau, după caz, a funcției electorale, ca urmare a constatării încălcărilor în procesul de control privind respectarea regimului juridic al averii, al conflictelor de interese și al incompatibilităților;

b) rectificarea și radierea interdicțiilor din RSI;

c) administrarea RSI;

2) portalul public al RSI:

a) publicarea datelor detaliate cu privire la persoanele care au interdicție de a ocupa o funcție publică sau de demnitate publică, sau, după caz, a funcției electorale;

b) căutarea interdicțiilor în baza unor criterii de filtrare prestabilite;

3) audit, rapoarte și statistici.

Capitolul IV
STRUCTURA ORGANIZAȚIONALĂ A SISTEMULUI INFORMATIC

31. Posesorul RSI este Autoritatea. Rolul de posesor al sistemului informatic reflectă aspectul administrativ ce ține de competențele totale deținute de ANI, necesare creării, administrării și dezvoltării continue a sistemului informatic. În această calitate, ANI asigură achiziționarea sistemului din sursele bugetare disponibile pentru astfel de activități. ANI, în calitate de implementator, asigură suportul organizațional și metodologic întru automatizarea funcțiilor business necesare atingerii obiectivelor sistemului informatic.

32. Deținătorul RSI din punct de vedere informațional este Autoritatea, care asigură crearea și exploatarea RSI. Administratorul tehnic al soluției informatice este IP „Serviciul Tehnologia

Informației și Securitate Cibernetică", care furnizează infrastructura tehnică care va găzdui RSI în conformitate cu cerințele față de sistemele informatice de importanță statală.

33. Administratorul de sistem este angajatul Autorității sau o organizație – persoană subcontractată de Autoritate, care acordă suportul tehnic de administrare a RSI.

34. Registratorii RSI sunt totalitatea inspectorilor de integritate ai ANI, care vor crea înregistrările în RSI în cadrul proceselor de business de examinare a sesizărilor parvenite în adresa ANI și perfectarea actelor de constatare în urma verificărilor efectuate.

35. Utilizatorii RSI sunt:

1) *utilizator internet* - actor uman care dispune de acces la funcționalitățile specifice de afișare a informațiilor cu caracter public furnizate de RSI prin intermediul paginii WEB a ANI (ww.ani.md).

2) *inspector de integritate* – actor uman, angajat al ANI cu atribuții de perfectare a formularelor destinate modificării conținutului RSI. Acești utilizatori vor perfecta cea mai mare parte a datelor aferente interdicțiilor de ocupare a funcțiilor publice și funcțiilor de demnitate publică, sau, după caz, a funcției electorale.

3) *decident ANI* – actor uman, angajat al ANI cu acces absolut la conținutul informațional și avansat la funcționalitățile furnizate de RSI, care dispune de rol de decident în fluxurile de lucru aferente înregistrării/modificării datelor privind statutul angajatului organizației publice.

4) *administrator de sistem* – actor uman, abilitat cu administrarea RSI. Dacă mediul tehnologic include capabilități suficiente pentru îndeplinirea lucrărilor de administrare apoi implementarea acestora în sistem este opțională.

5) *administrator tehnic* - actor uman, care monitorizează infrastructura tehnică ce găzduiește RSI, asigură mentenanța și securitatea informațională a RSI.

Capitolul V
DOCUMENTELE SISTEMULUI INFORMATIC

36. Documentele de intrare ale sistemului informatic. RSI va stoca un șir de documente de intrare prezentate de actorii ANI implicați în procesele de business privind exercitarea controlului asupra respectării regimului juridic de declarare a averii și intereselor personale. Din categoria documentelor de intrare pot fi menționate:

1) sesizarea privind încălcarea regimului juridic al averii, al conflictelor de interese și al incompatibilităților;

2) actul de constatare emis în urma controlului efectuat de ANI;

3) solicitarea de rectificare sau radiere a datelor despre interdicție.

37. Documente de ieșire ale sistemului informatic. RSI va genera și prezenta un șir de documente de ieșire aferente proceselor de înregistrare și gestiunea ulterioară a datelor despre interdicții:

1) tranzacția de înregistrare a interdicției;

2) extrase din RSI, liste ale persoanelor cu interdicții de ocupare a funcțiilor publice și funcțiilor de demnitate publică, sau, după caz, a funcției electorale;

3) rapoarte statistice vizând interdicțiile de ocupare a funcțiilor publice și funcțiilor de demnitate publică, sau, după caz, a funcției electorale.

38. Documente tehnologice ale sistemului informatic. La categoria documentelor tehnologice create și procesate în cadrul RSI pot fi menționate:

- înregistrări ale fișierelor log privind interacțiunea RSI cu sistemele informatice externe;
- înregistrări ale fișierelor log privind activitatea utilizatorilor autorizați în cadrul RSI;

- înregistrări ale fișierelor log privind evenimentele de gestiune a înregistrărilor interdicțiilor.

Capitolul VI
SPAȚIUL INFORMAȚIONAL AL SISTEMULUI INFORMATIC

39. Totalitatea obiectelor informaționale, care reprezintă resursa informațională a RSI, este determinată de destinația sistemului și include următoarele obiecte:

1) interdicție;

2) act de constatare;

3) solicitare de rectificare/radiere interdicție;

4) eveniment de gestiune a înregistrării.

40. Identificarea obiectelor în cadrul RSI se efectuează prin utilizarea numărului de identificare unic.

1) pentru „interdicții" – numărul de identificare unic generat de sistem;

2) pentru „acte de constatare" – numărul de identificare unic furnizat de SIA „e-Management";

3) pentru „solicitare de rectificare/radiere interdicție" – numărul de identificare unic furnizat de SIA „e-Management";

4) pentru „Eveniment de gestiune a înregistrării (eveniment)" - numărul de identificare unic generat de sistem.

41. Datele Sistemului informatic. Datele prezentului Sistem reprezintă totalitatea de atribute ale obiectelor informaționale și includ:

1) Interdicție:

a) Numărul unic de identificare a interdicției în RSI;

b) Date despre actul de constatare:

- numărul unic de identificare a actului de constatare;
- data emiterii actului de constatare;
- mențiuni despre statutul actului de constatare (în termen (pasibil) de contestare, contestat, definitiv, anulat);

c) Date despre subiectul declarării:

- IDNP subiectului;
- numele, prenumele subiectului;
- denumirea organizației, IDNO;
- funcția deținută.

d) Date despre perioada pentru care este aplicată interdicția:

- statutul interdicției, determinat de statutul actului de constatare (preventivă, definitivă, contestată, anulată);
- termenul de aplicare a interdicției (luni);
- data intrării în vigoare a interdicției;
- data încetării interdicției;

e) Alte mențiuni speciale:

- publicată pe pagina WEB a ANI (da/nu).

2) Act de constatare:

a) numărul unic de identificare a actului de constatare;

b) data emiterii actului de constatare;

c) tipul actului de constatare (de încetare, de constatare a încălcării);

d) date despre tipul încălcării (01- avere; 02 - conflict de interese; 03-incompatibilități).

e) date despre operatorul inspector care a elaborat actul de constatare:
- identificatorul unic al inspectorului ANI în SIA „e-Integritate”;

f) date despre subiectul declarării pentru care a fost examinat cazul de încălcare;
- IDNP subiectului;
- numele, prenumele subiectului;
- denumirea organizației, IDNO;
- funcția deținută;

g) date despre interdicție:
- numărul unic de identificare a interdicției în RSI;
- termenul de aplicare a interdicției (luni).

3) Solicitare de rectificare/radiere interdicție:
a) numărul unic de identificare a solicitării de rectificare;
b) numărul unic de identificare a interdicției în RSI;
c) numele, prenumele, IDNP al subiectului declarării pentru care a fost adăugată interdicția;
d) nota informativă despre datele care trebuie rectificate.

4) Eveniment de gestiune a înregistrării:
a) numărul unic de identificare al evenimentului;
b) tipul evenimentului;
c) data și ora evenimentului.

Capitolul VII
SPAȚIUL TEHNOLOGIC AL SISTEMULUI INFORMATIC

42. RSI va fi elaborat în baza unei interfețe web accesibile prin intermediul unui explorator de internet de largă utilizare (MS Edge/MS Internet Explorer, Mozilla FireFox, Opera, Google Chrome sau Safari).

43. RSI ca parte componentă a SIA „e-Integritate” nu este o soluție izolată, ci interacționează cu soluții informatice externe și trebuie să furnizeze facilități pentru integrarea cu alte sisteme informatice.

44. La baza modulelor funcționale ale RSI trebuie utilizată o arhitectură client-server multi-nivel (care exclude interacțiunea directă a aplicației cu baza de date) bazată pe tehnologiile web moderne adecvate.

45. Întru asigurarea unui nivel adecvat al securității informaționale aplicația trebuie să funcționeze doar în baza conexiunilor securizate între stațiile client și serverul de aplicație (prin intermediul canalelor VPN și a sesiunilor TLS/SSL).

46. Reieșind din arhitectura SIA „e-Integritate”, exploatarea RSI constă din cooperarea a 3 categorii de noduri distincte:

- Infrastructura TIC a ANI – infrastructura TIC a ANI în Mcloud, care găzduiește SIA „e-Integritate”, Portalul public al SIA „e-Integritate” și Pagina WEB oficială a ANI;
- Mcloud – infrastructura TIC a platformei tehnologice guvernamentale comune care formează cloud-ul guvernamental (MCloud) unde sunt găzduite un șir de sisteme informatice cu care interacționează SIA „e-Integritate” sau serviciile cărora sunt consumate de SIA „e-Integritate”. În cadrul SIA „e-Integritate” sunt reutilizate următoarele servicii de platformă Mcloud (MPass - pentru autentificarea utilizatorilor prin intermediul semnăturii electronice sau mobile;

MSign – pentru aplicarea semnăturii electronice; MNotify – pentru notificarea utilizatorilor; MLog – pentru jurnalizarea evenimentelor de business critice).

- Calculatoare client – calculatoarele, de la care sunt accesate de către utilizatori (în funcție de drepturi și roluri) funcționalitățile SIA „e-Integritate”.

47. Interfața și funcționalitățile livrate fiecărui utilizator în parte depind de nivelul utilizatorului, drepturile și rolurile acestuia. Indiferent de nivelul de acces al utilizatorilor toate conexiunile utilizatorilor la SIA „e-Integritate” sunt efectuate prin intermediul conexiunilor sigure (VPN sau TLS/SSL).

48. RSI constă din următoarele componente funcționale:

a) dashboard-ul utilizatorului autorizat – care furnizează un tablou de bord pentru accesarea rapidă a evenimentelor de business aferente atribuțiilor de serviciu ale utilizatorilor autorizați ai RSI;

b) importul de date în format tipizat (opțional) – care asigură posibilitatea importului de interdicții de ocupare a funcțiilor publice și funcțiilor de demnitate publică, sau, după caz, a funcției electorale, parvenite de la instituțiile terțe. Acestea vor parveni în format tipizat și vor fi importate de administratorul de sistem;

c) completarea solicitării de rectificare – care furnizează formularul electronic necesar modificării datelor privind interdicțiile de ocupare a funcțiilor publice și funcțiilor de demnitate publică, sau, după caz, a funcției electorale (pentru perfectarea tranzacțiilor de modificare a datelor conținute în RSI);

d) aprobarea solicitării de rectificare – care furnizează funcționalitatea de aprobare/respingere a formularului electronic de modificare a datelor privind interdicțiile de ocupare a funcțiilor publice și funcțiilor de demnitate publică, sau, după caz, a funcției electorale;

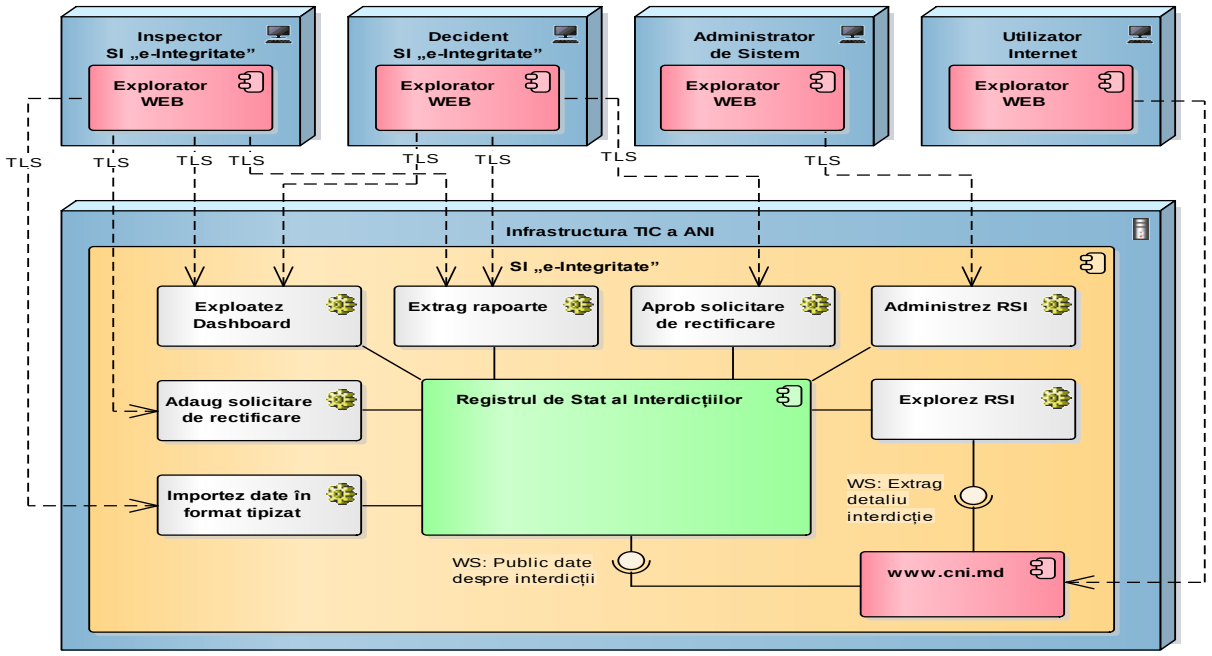
e) explorare registru – care furnizează funcționalitatea de explorare a conținutului RSI (căutare/filtrare date, extragere date, vizualizare interdicții și detaliile acestora etc.);

f) componenta de generare a rapoartelor – care furnizează funcționalități destinate prelucrării și prezentării datelor sub formă de indicatori de performanță, statistici și rapoarte analitice;

g) componenta de administrare a registrului – furnizează funcționalități destinate gestiunii și configurării sistemului informatic, atribuirii drepturilor de acces, gestiunii nomenclatoarelor/clasificatoarelor, monitorizării parametrilor de funcționare optima a sistemului informatic, alte funcționalități destinate administrării sistemului;

h) portalul public „e-Integritate” (accesibil prin intermediul paginii WEB oficiale a ANI) – care asigură accesul publicului larg la informația cu caracter public furnizat de RSI. Registrul va furniza interfața de publicare a datelor publice relevante.

Arhitectura logică a RSI este prezentată în figura de mai jos.



Capitolul VIII
ASIGURAREA SECURITĂȚII INFORMAȚIONALE

49. Asigurarea securității informaționale. Sistemul complex al securității informaționale reprezintă totalitatea normelor juridice în domeniu, măsurilor organizatorice şi economice, precum şi a mijloacelor tehnologice şi a metodelor de protecţie criptografică şi software-hardware a informaţiei, care sânt orientate spre asigurarea nivelului necesar al integrităţii, confidenţialităţii şi accesibilităţii resurselor informaţionale.

50. Sarcina de bază a securităţii informaţionale este asigurarea:

a) confidenţialităţii informației – protecţia împotriva accesului sau a dezvăluirii neautorizate de date;

b) integrităţii logice a datelor – protecţia împotriva introducerii, actualizării și ștergerii nesancționate a informației sau introducerea datelor denaturate;

c) asigurarea securității infrastructurii informaționale de tentative de a defecta sau de a modifica funcționarea acestuia.

51. Mecanismele principale de securitate informațională utilizate vor fi:

a) autentificarea și autorizarea accesului la date;

b) administrarea accesului la date;

c) înregistrarea de audit a acțiunilor utilizatorilor sistemului informatic;

d) criptarea datelor, după caz;

e) auditul informatic;

f) procedurile de restabilire în caz de dezastru.

52. Veriga cea mai sensibilă la risc în sistemul de securitate este factorul uman. Din aceste considerente, instruirea personalului la capitolul însușirii metodicii rezistenței la amenințări informatice este un element foarte important.

53. În procesul de elaborarea a RSI pentru asigurarea securității informaționale se va ține cont de algoritmii și protocoalele existente pe piață cu respectarea cadrului legal al Republicii Moldova.

54. Adițional este binevenită elaborarea unor acțiuni organizatorice, tehnologice și de program de asigurarea a securității informaționale în conformitate cu standardele internaționale agreate în Republica Moldova:

- SM ISO/CEI 15408-1:2014 „Tehnologia informației. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informației. Partea 1: Introducere și model general";
- SM ISO/CEI 15408-2:2014 „Tehnologia informaţiei. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informaţiei. Partea 2: Cerinţe funcţionale de securitate";
- SM ISO/CEI 15408-3:2014 „Tehnologia informaţiei. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informației. Partea 3: Cerințe de asigurare a securităţii";
- SM SR ISO/CEI 27002:2017 "Tehnologia informației; Tehnici de securitate; Sisteme de management al securității informaționale. Cerințe;
- SM ISO/CEI 27002:2017 "Tehnologia informației; Tehnici de securitate; Cod de bună practică pentru managementul securității informației."

55. Reieșind din cele expuse, accesul la RSI trebuie să fie asigurat și autorizat prin intermediul semnăturii electronice. Utilizatorii vor poseda drepturi distincte de acces în dependență de nivelul de securitate căruia îi corespund. Pentru fiecare categorie de acces trebuie să existe posibilitatea de a defini rolurile și drepturile utilizatorilor (inclusiv nivelul de acces la interfața accesibil utilizatorilor).

56. Accesul la informația bazei de date trebuie să fie limitată în dependență de drepturile și rolurile specifice grupurilor de acces. În acest caz, fiecare grup de utilizatori va avea acces la o interfață personalizată (diferită de cea a altor grupuri) pentru vizualizarea și gestionarea informației bazei de date, precum și de manipulare cu datele.

57. Indiferent de nivelul de acces al utilizatorului (inspector de integritate, administrator de sistem, administrator tehnic), nici un grup de acces nu va poseda dreptul de a suprima direct înregistrările bazei de date. Sistemul informatic va permite aplicarea de modificări prin inserarea unor înregistrări suplimentare care anulează sau modifică înregistrările sau statuturile curente. În acest caz nu se va admite modificarea directă a datelor bazei de date. Toate inserările și actualizările de date în baza de date se vor face exclusiv prin intermediul unor formulare electronice specializate, cu parcurgerea completă a unor fluxuri de lucru implementate în cadrul RSI.

58. Orice modificare: modificarea informației unei înregistrări, schimbare statut, adăugarea unor înregistrări noi etc., trebuie să fie documentată în registre electronice speciale (fișiere log) indicând momentul de timp și utilizatorul care a efectuat modificarea potențial periculoasă. Pentru fiecare modificare, RSI va salva în evenimentul jurnalizat modificarea efectuată. În consecință, sistemul informatic proiectat va dispune de un instrument eficient de analiză a comportamentului utilizatorilor (sau a productivității lor).

59. La nivel fizic, politica de asigurare a securității informaționale trebuie să fie realizate prin intermediul unor module automate de generare a copiilor de rezervă a fișierelor și bazelor de date aflate în producere. Administratorii RSI trebuie să dispună de posibilitatea de a-și defini politica de generare automată a copiilor de rezervă.

60. Întru asigurarea unui nivel adecvat al securității informaționale a RSI, se consideră binevenită elaborarea și implementarea unei politici de asigurare a securității informaționale. Această politică va detalia totalitatea compartimentelor de securitate, rolurile, drepturile și obligațiile fiecărui actor al sistemului informatic.

61. Politica de securitate va fi adusă la cunoștința fiecărui utilizator contra semnătura. Fiecare utilizator va cunoaște obligațiile de serviciu în materie de respectare securității informaționale și totalitatea procedurilor formale pe care trebuie să le respecte în strictă concordanță cu politica de securitate.

62. Pentru asigurarea veridicității informației, se va crea o politică care va defini mecanismele de validare a datelor introduse în cadrul RSI sau extrase din acesta.

63. ANI va dispune sau va contracta personal calificat pentru efectuarea auditului securității informaționale, verificării și instruirii continue în materie de asigurare a securității informaționale.

64. La momentul acceptării RSI, se vor verifica următoarele cerințe caracteristice procedurilor de asigurare a securității informaționale:

1) sistemul informatic garantează păstrarea completă și integritatea tuturor înregistrărilor RSI;

2) accesul la RSI se face în mod controlat;

3) accesul la funcțiile oferite utilizatorilor autorizați se face cu autentificarea acestora;

4) schimbul de date în sistem se realizează doar pe canale securizate;

5) acțiunile utilizatorilor sunt înregistrate în jurnale electronice;

6) sistemul emite un semnal periodic care indică starea sa funcțională;

7) sistemul autentifică utilizatorii exclusiv prin semnătură electronică prin intermediul Mpass.

65. Securitatea informațională presupune protecția RSI, la toate etapele proceselor de creare, procesare, stocare și transmitere a datelor, de acțiuni accidentale sau intenționate cu caracter artificial sau natural, care au ca rezultat cauzarea prejudiciului posesorului și utilizatorilor resurselor informaționale și infrastructurii informaționale.

66. Sarcina de bază a securității informaționale este asigurarea integrității și confidențialității informației.

67. Exportul de date din RSI are loc în condițiile legislației, cu autorizarea Centrului Național pentru Protecția Datelor cu Caracter Personal și doar în cazul în care beneficiarul asigură un nivel adecvat de protecție a drepturilor subiecților datelor cu caracter personal și a datelor destinate transmiterii.