Anexa nr. 1
la ordinul ANI nr. 80 din 26.08.2020

CONCEPTUL DE CREARE
a Registrului electronic al subiecților declarării averii și a intereselor personale

INTRODUCERE

În conformitate cu Legea nr.132/2016 cu privire la Autoritatea Națională de Integritate, Autoritatea este o autoritate publică independentă faţă de alte organizaţii 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 și gestiunii ulterioare a acestor înregistrări, precum și facilitării accesului electronic al persoanelor și instituțiilor interesate la informațiile de interes public.

La art.3 alin.(1) din Legea nr.133/2016 *privind declararea averii şi a intereselor personale* sunt enumerați subiecții declarării averii și intereselor personale:

- persoanele care deţin funcţiile de demnitate publică prevăzute în anexa la Legea nr. 199 din 16 iulie 2010 cu privire la statutul persoanelor cu funcţii de demnitate publică;
- membrii Consiliului de observatori al instituţiei publice naţionale a audiovizualului Compania „Teleradio-Moldova" , Compania Teleradio-Găgăuzia; consilierii consiliilor săteşti (comunale), orăşeneşti (municipale), raionale; deputaţii Adunării Populare a unităţii teritoriale autonome Găgăuzia;
- membrii Consiliului Superior al Magistraturii şi ai Consiliului Superior al Procurorilor din rândul profesorilor, precum și membrii organelor care funcționează în subordinea Consiliului Superior al Magistraturii și a Consiliului Superior al Procurorilor;
- membrii nepermanenți ai Comisiei Electorale Centrale;
- conducătorii organizațiilor publice şi adjuncţii acestora;
- membrii Consiliului de supraveghere, ai Comitetului executiv și angajații Băncii Naționale a Moldovei, membrii și angajații Comisiei Naționale a Pieței Financiare, cu excepția angajaților care desfășoară activități auxiliare – de secretariat, de protocol, administrative, tehnice;
- personalul din cabinetele persoanelor cu funcţii de demnitate publică;
- funcționarii publici, inclusiv cei cu statut special;
- membrii Consiliului de Integritate;
- membrii colegiilor/comisiilor de admitere în profesie, de evaluare, disciplinare și/sau de etică a profesiilor conexe justiției.

Potrivit normei precitate, subiecţii prevăzuţi la alin. (1) sunt incluşi în Registrul electronic al subiecţilor declarării averii şi a intereselor personale, ţinut de Autoritatea Națională de Integritate.

Subsecvent, în entităţile în care activează persoane care, conform prezentei legi, au obligaţia de a depune declaraţii sunt desemnate persoane din cadrul serviciului resurse umane responsabile de actualizarea permanentă a Registrului electronic al subiecţilor declarării averii şi a intereselor personale.

Astfel, înregistrarea subiectului în Registrul electronic al subiecţilor declarării averii şi a intereselor personale, este o condiție indispensabilă în scopul acordării acestuia posibilității de a depune declarația de avere și interese personale în format electronic, utilizând semnătura electronică. De asemenea, această înregistrare permite Autorității Naționale de Integritate de a implementa proceduri de verificare și analiză a declarațiilor de avere și interese personale.

Potrivit pct. 57 din Conceptul tehnic al SIA „e-Integritate”, acesta include ca parte componentă Registrul electronic al subiecților declarării averii și a intereselor personale, care este completat și actualizat de furnizorii datelor din cadrul organizațiilor publice în care activează subiecții declarării

Printre beneficiarii direcți ai Registrului electronic al subiecților declarării averii și a intereselor personale, 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 Registrului electronic al subiecților declarării averii și a intereselor personale urmează să furnizeze următoarele categrorii de beneficii așteptate:

Beneficii pentru cetățeni, subiecți ai declarării averii și a intereselor personale:

- Informarea oportună cu privire la obligația de a depune declarația în baza unui dintre următoarele temeiuri: a) declarația anuală, b) declarația în cazul angajării, al validării mandatului ori al numirii în funcţie; c) declarația după încetarea mandatului sau a raporturilor de muncă ori de serviciu;
- Reducerea setului de date ce urmează a fi completate, datorită completării unui șir de date date personale și despre familie, de către persoanele responsabile din cadrul serviciului resurse umane al organizației, unde activează subiectul;
- Obținerea automatizată (la adresa indicată a poștei electronice) a dovezii de depunere a declarației de avere și interese personale
- Asigurarea încrederii privind transparența și legalitatea proceselor de control efectuate de ANI.

Beneficii pentru Autoritatea Națională de Integritate:

- Implementarea unor mecanisme moderne de control a respectării regimului juridic al declarării averii și intereselor personale, al conflictelor de interese, al incompatibilităților, restricțiilor și limitărilor;
- Eliminarea necesității interacțiunii directe și automatizarea proceselor de cooperare între funcționarii ANI cu persoanele responsabile din cadrul serviciului resurse

umane ale organizațiilor publice, responsabile de evidența subiecţilor declarării averii şi a intereselor personale.

Beneficii pentru Autoritățile publice centrale și locale:

- Automatizarea proceselor de evidență a angajaților, subiecţi ai declarării averii şi a intereselor personale;
- Scutirea de obligația de colectare de la subiecții declarării, cu excepțiile prevăzute de Legea nr.133/2016 (art.7^1), a declarațiilor de avere și interese personale, acestea fiind completate și depuse de către subiecții înșiși în format electronic.

Beneficii pentru Republica Moldova:

- Asigurarea unui mediu favorabil de integritate a instituțiilor publice;
- Asigurarea unor mecanisme eficiente de transparentizare a procesului de depunere și control a declarațiilor de avere și interese personale.

Conceptul tehnic stabilește cerințele de bază pentru implementarea noilor tehnologii informaționale în procesul de depunere, de verificare și analiză a declarațiilor de avere și interese personale.

Capitolul I
DISPOZIȚII GENERALE

1. Registrul electronic al subiecților declarării averii și a intereselor personale (în continuare - RSD) este o parte componentă a SIA „e-Integritate", care asigură funcționalitatea de management al resurselor umane din cadrul organizațiilor publice în care activează subiecții declarării, monitorizarea termenelor specificate în legislație de depunere a declarațiilor și notificarea subiecților declarării prin intermediul serviciului electronic guvernamental de notificare (MNotify).

2. RSD 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 procesului de interacțiune a cetățenilor și autorităților publice 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, creează baza informatică necesară pentru depunerea de către subiecți în format electronic a declarației de avere și interese personale, utilizând semnătura electronică. De asemenea, realizarea RSD, creează premisele necesare pentru monitorizează încontinuu a fluxului subiecților înregistrați și notificarea acestora privind termenele și temeiurile specificate în legislație de depunere a declarațiilor de avere și interese personale.

4. Destinația RSD.

Registrul electronic al subiecților declarării averii și a intereselor personale este o componentă informatică necesară implementării interacțiunii ANI cu entitățile externe (cetățeni și autorități publice) în vederea formării resursei informaţionale despre subiecții declarării din cadrul organizațiilor publice, în vederea creării suportului necesar pentru depunerea declarației în format electronic și monitorizării termenelor specificate în legislație de depunere a declarațiilor.

Destinația prioritară a RSD constă în dezvoltarea unui subsistem informatic al SIA „e-Integritate", prin intermediul căruia este asigurată gestionarea datelor cu privire la organizațiile publice și angajații acestora cu statut de subiecți ai declarării averii și intereselor personale prin colectarea, stocarea, actualizarea şi analiza datelor despre funcţiile publice şi personalul din autorităţile administraţiei publice centrale şi locale. RSD este destinat, de asemenea, pentru asigurarea unui management eficient al procesului de control asupra respectării regimului personalului şi prezentarea informaţiei organelor abilitate.

5. Noțiuni de bază și abrevieri.

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

1) APC – Autoritate Publică Centrală;
2) APL – Autoritate Publică Locală;
3) BD – bază de date;
4) ANI – Autoritatea Națională de Integritate;
5) E-Gov – IP „Agenția de Guvernare Electronică";
6) RSP – Registrul de stat al populației;
7) RSUD – Registrul de stat al unităților de drept;
8) SGBD – Sistem de gestiune a bazelor de date;
9) SI – sistem informatic;
10) TI – Tehnologie informatică.

6. 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 subordonate 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, instanță judecătorească, procuratură.

6) Flux de lucru – proces administrativ al unei organizații în decursul căruia sarcini, proceduri ș 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 i 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 informație 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 informație documentată 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 (componentă 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.

7. Scopul creării RSD.

Scopul elaborării RSD constă în formarea resursei informaționale despre subiecții declarării din cadrul organizațiilor publice, precum și implementarea mecanismelor de depunere a declarațiilor, de verificare a averilor, intereselor personale și conflictelor de interese, a incompatibilităților, restricțiilor și limitărilor, în conformitate cu prevederile Legii nr. 132/2016 cu privire la Autoritatea Națională de Integritate și ale Legii nr. 133/2016 privind declararea averii și a intereselor personale.

8. Sarcinile de bază ale RSD.

Implementarea RSD ca parte componentă a SIA „e-Integritate” va furniza ANI un instrument eficient de monitorizare a respectării regimului juridic al declarării averii și intereselor personale, al conflictelor de interese, al incompatibilităților, restricțiilor și limitărilor. Printre sarcinile principale înaintate sistemului informatic pot fi menționate:

1) furnizarea oportună a datelor relevante cu privire la evenimentele de angajare/numire/alegere în funcție, precum și de demisie/eliberare din funcție a subiecților declarării și obligațiile apărute privind depunerea declarației;

2) formalizarea și eficientizarea proceselor de gestiune a datelor cu privire la subiecții declarării și notificarea acestora la apariția obligațiilor privind depunerea declarației;

3) asigurarea și impulsionarea schimbului electronic de date cu organizațiile publice și terțe părți;

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

5) facilitarea procesului de depunere de către subiecții declarării a declarațiilor în format electronic.

9. Principiile de bază ale RSD sânt:

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

2) principiul respectării drepturilor omului, care presupune exploatarea RSD 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 RSD);

4) principiul veridicității datelor, care presupune introducerea datelor în RSD în baza documentelor autentice, precum și asigurarea unui grad înalt de corespundere a datelor stocate în RSD 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 RSD, 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 şi 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 RSD 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 în conformitate cu prevederile art. 4 din Legea nr. 133/2011 privind protecția datelor cu caracter personal;

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

Capitolul II
CADRUL NORMATIV JURIDIC AL RSD

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

11. Crearea și funcționarea RSD 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. 183/2019 cu privire la aprobarea Conceptului tehnic al Sistemului informațional automatizat „e-Integritate”;
13) Hotărârea Guvernului nr. 228/2020 pentru aprobarea Regulamentului cu privire la organizarea și funcționarea Sistemului informațional automatizat „e-Integritate”;

14) Hotărârea Guvernului nr. 1140/2017 pentru aprobarea Regulamentului privind activitatea prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice;

15) 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;

16) Hotărârea Guvernului nr. 562/2006 cu privire la crearea sistemelor și resurselor informaționale automatizate de stat;

17) 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;

18) Hotărârea Guvernului nr. 710/2011 cu privire la aprobarea Programului strategic de modernizare tehnologică a guvernării (e-Transformare);

19) Hotărârea Guvernului nr. 656/2012 cu privire la aprobarea Programului privind Cadrul de Interoperabilitate;

20) Hotărârea Guvernului nr. 1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);

21) Hotărârea Guvernului nr. 405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);

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

12. La elaborarea și implementarea RSD 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 RSD

13. RSD asigură îndeplinirea funcțiilor de bază ale sistemului informațional-tip, precum și îndeplinirea unor funcții specifice (ilustrate în figura *Interconexiunile RSD*), determinate de destinația sistemului, după cum urmează:

1) completarea și actualizarea informațiilor cu privire la organizațiile publice în cadrul cărora activează subiecți ai declarării, inclusiv importarea datelor din RSUD prin intermediul platformei guvernamentale de interoperabilitate MConnect;

2) completarea și actualizarea informațiilor cu privire la subiecții declarării ce activează în cadrul organizațiilor publice distincte, inclusiv importarea datelor din RSP prin intermediul platformei MConnect;

3) monitorizarea evenimentelor de angajare/numire/alegere în funcție, precum și de demisie/eliberare din funcție a subiecților declarării și obligațiilor apărute privind depunerea declarației;

4) notificarea subiecților declarării cu privire la obligațiile apărute privind depunerea declarației prin intermediul serviciului electronic guvernamental de notificare (MNotify);

5) monitorizarea termenilor legali de depunere a declaraţiei, și furnizarea automatizată a datelor către SIA „e-Integritate”, în caz de nedepunere a declarațiilor în termenul stabilit, spre includere în lista subiecților declarării pasibili de declanşarea din oficiu a procedurii de control ;

6) furnizarea datelor pentru precompletarea formularului electronic al declarației de avere și interese personale, destinat subiectului declarării;

7) schimbul de date cu alte module ale SIA „e-Integritate”, în vederea completării și actualizării resursei informaționale a sistemului;

8) generarea și exportul de rapoarte în formate predefinite, conform necesităților ANI privind conținutul informațional al RSD;

9) jurnalizarea evenimentelor din RSD privind înregistrarea și actualizarea datelor despre subiecții declarării și organizațiile publice, în care activează aceștea, 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).

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

15. Interfața de utilizator a RSD.

RSD 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 accesibil pentru totalitatea dispozitivelor utilizate.

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

17. Utilizatorii vor dispune de minim 3 nivele de acces la interfața de utilizator și date:

1) Nivel acces inspector ANI – nivel de acces asigurat angajaților ANI, care va asigura acces la totalitatea funcționalităților necesare vizualizării datelor din RSD, în cadrul procedurilor/dosarelor de control atribuite în gestiune, generare de rapoarte specifice și perfectare a formularelor electronice privind actele de constatare emise în privința subiecților declarării;

2) Nivel acces operator resurse umane – nivel de acces asigurat persoanelor responsabile din cadrul serviciilor resurse umane ale organizațiilor publice, în care activează subiecți ai declarării, care va asigura acces la totalitatea funcționalităților necesare introducerii, actualizării și vizualizării datelor din RSD, în cadrul procedurilor de personal legate de angajare/numire/alegere în funcție, precum și de demisie/eliberare din funcție a subiecților declarării;

3) 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.

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

5) 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.

6) Interfața de utilizator a RSD 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.

18. 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.

19.RSD va avea următoarele componente asociate funcționalităților de bază:

1) Gestionarea Registrului electronic al subiecților declarării averii și a intereselor personale:

a) Înregistrarea subiectului declarării la angajare/numire/alegere în funcție;

b) Modificarea statutului subiectului declarării la demisie/transfer;

2) monitorizarea evenimentelor de angajare/numire/alegere în funcție, precum și de demisie/eliberare din funcție a subiecților declarării și obligațiilor apărute privind depunerea declarației:

a) notificarea subiecților declarării, expedierea notificărilor utilizând serviciul electronic guvernamental de notificare (MNotify) cu privire la obligațiile apărute privind depunerea declarației;

b) furnizarea automatizată a datelor către SIA „e-Integritate”, în caz de nedepunere a declarației în termenul stabilit, spre includere în lista subiecților declarării pasibili de declanșarea din oficiu a procedurii de control;

3) Audit, rapoarte și statistici:

a) generarea rapoartelor;

b) exportul rapoartelor;

c) jurnalizarea evenimentelor din sistem.

20.RSD „e-Integritate” include următoarele contururi funcționale de bază:

1) conturul organizațiilor publice:

a) înregistrarea subiecților declarării în Registrul electronic al subiecților declarării averii și a intereselor personale;

b) modificarea statutului subiecților declarării în Registrul electronic al subiecților declarării averii și a intereselor personale;

2) conturul Autorității:

a) gestionarea utilizatorilor;

b) gestionarea Registrului electronic al subiecților declarării averii și a intereselor personale;

3) audit, rapoarte și statistici.

Capitolul IV.
STRUCTURA ORGANIZAȚIONALĂ
A SISTEMULUI INFORMATIC

21. Posesorul RSD 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.

22. Deținătorul RSD din punct de vedere informațional este Autoritatea, care asigură crearea și exploatarea RSD. Administratorul tehnic al soluției informatice este IP „STISC”, care furnizează infrastructura tehnică care va găzdui RSD în conformitate cu cerințele față de sistemele informatice de importanță statală.

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

24. Registratorii RSD sânt persoanele responsabile (operator resurse umane) din cadrul organizațiilor publice în care activează subiecții declarării. La angajarea în câmpul muncii a subiecților declarațiilor, persoana responsabilă din cadrul direcției/secției resurse umane al organizației va înregistra/modifica (în cazul când persoana se regăsește în baza de date) statutul angajatului organizației publice.

25. Utilizatorii RSD sânt:

1) *operator resurse umane* - actor uman atribuit persoanelor responsabile din cadrul organizațiilor publice în care activează subiecții declarării, care completează Registrul

electronic al subiecților declarării averilor și a intereselor personale (IDNP/IDNO, nume, prenume, funcția, actul juridic, data emiterii acestuia, adresa etc.) în modul stabilit de legislație. Este o categorie de de utilizatori ai RSD care vor perfecta cea mai mare parte a datelor aferente angajaților organizațiilor publice, care au statut de subiect al declarării averii și intereselor personale. Actorii în cauză dispun de acces la următoarele funcționalități:

a) utilizarea Dashboard-ului pentru recepționarea și accesarea notificărilor privind evenimentele de business care-l vizează;

b) formularea interogărilor de căutare în conținutul BD a RSD;

c) înregistrarea informației cu privire la datele personale și de familie ale angajaților, evenimentele de angajare/numire/alegere în funcție, actele administrative aferente, precum și de demisie/eliberare din funcție în conținutul BD a RSD;

d) generarea și extragerea rapoartelor/statisticilor relevante drepturilor sale de acces la date;

e) recepționarea notificărilor de sistem;

2) *inspector de integritate* – actor uman, angajat al ANI cu atribuții de vizualizare a datelor din RSD, în cadrul procedurilor/dosarelor de control atribuite în gestiune, generare de rapoarte specifice și perfectare a formularelor electronice privind actele de constatare emise în privința subiecților declarării. Actorii în cauză dispun de acces la următoarele funcționalități:

a) utilizarea Dashboard-ului pentru recepționarea și accesarea notificărilor privind evenimentele de business care-l vizează;

b) formularea interogărilor de căutare în conținutul BD a RSD;

c) înregistrarea informației cu privire la datele personale și de familie ale angajaților, evenimentele de angajare/numire/alegere în funcție, actele administrative aferente, precum și de demisie/eliberare din funcție în conținutul BD a RSD;

d) generarea și extragerea rapoartelor/statisticilor relevante drepturilor sale de acces la date;

e) recepționarea notificărilor de sistem;

3) *administrator de sistem* – actor uman, abilitat cu administrarea RSD. Dacă mediul tehnologic include capabilități suficiente pentru îndeplinirea lucrărilor de administrare apoi implementarea acestora în sistem este opțională. Această categorie de actori are acces la următoarele funcționalități:

a) Folosește necondiționat toate funcționalitățile sistemului informatic, cu excepția modificării fișierelor de evenimente;

b) Vizualizează orice înregistrare din baza de date;

c) Generează rapoarte aferente auditului RSD și conținutului informațional al Bazei de date;

d) Administrează sistemul de nomenclatoare;

e) Recepționează notificări de sistem.

4) *administrator tehnic* - actor uman, abilitat cu administrarea RSD. Dacă mediul tehnologic include capabilități suficiente pentru îndeplinirea lucrărilor de administrare apoi

implementarea acestora în sistem este opțională. Această categorie de actori are acces la următoarele funcționalități:

a) Folosește necondiționat toate funcționalitățile sistemului informatic, cu excepția modificării fișierelor de evenimente;
b) Vizualizează orice înregistrare din baza de date;
c) Administrează serverul de aplicații ;
d) Administrează baza de date în producție;
e) Administrează profilurile utilizatorilor;
f) Generează rapoarte aferente auditului RSD și conținutului informațional al Bazei de date;
g) Administrează sistemul de nomenclatoare;
h) Recepționează notificări de sistem;
i) Efectuează copii de rezervă a bazei de date.

Capitolul V
DOCUMENTELE SISTEMULUI INFORMATIC

20. Documentele de intrare ale sistemului informatic.

RSD va stoca un șir de documente de intrare prezentate de cetățeni, decidenți ai AP, precum și a actorilor 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) Acte de identitate ale sistemului național de pașapoarte – buletine de identitate, pașapoarte ale cetățeanului Republicii Moldova;
2) Acte de stare civilă – adeverințe de naștere, adeverințe de căsătorie/de divorț;
3) Acte administrative emise de organizațiile publice cu privire la angajare/numire/alegere în funcție, actele administrative aferente, precum și de demisie/eliberare din funcție.

21. Documente de ieșire ale sistemului informatic.

RSD va genera și prezenta un șir de documente de ieșire aferente proceselor de înregistrare a angajaților organizațiilor publice cu statut de subiect al declarării, precum și de exercitare a controlului asupra respectării regimului juridic de declarare a averii și intereselor personale. Din categoria documentelor de ieșire pot fi menționate:

1) Extrase din RSD, liste ale persoanelor – subiecți ai declarării care nu și-au onorat obligația de depunere a declarației de avere și interese personale în termen legal;
2) Rapoarte statistice vizând numărul de subiecți ai declarării în diverse organizații publice.

22. Documente tehnologice ale sistemului informatic.

La categoria documentelor tehnologice create și procesate în cadrul RSD pot fi menționate:

1) Înregistrări ale fișierelor log privind interacțiunea RSD cu sistemele informatice externe;

2) Înregistrări ale fișierelor log privind activitatea utilizatorilor autorizați în cadrul RSD;

3) Înregistrări ale fișierelor log privind evenimentele de gestiune a evenimentelor aferente înregistrării/modificării datelor privind statutul angajatului organizației publice subiecții declarării.

Capitolul VI
SPAȚIUL INFORMAȚIONAL AL SISTEMULUI INFORMATIC

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

1) Profilul persoanei (subiect al declarării);
2) Organizația;
3) Subdiviziunea organizației;
4) Activitatea angajatului;
5) Eveniment de gestiune a înregistrării.

24. Identificarea obiectelor în cadrul RSD se efectuează prin utilizarea numărului de identificare unic.

1) pentru „subiecții declarării averii și intereselor personale” – cheia combinată „denumirea organizației publice și IDNO-ul organizației publice”, „numele/prenumele și IDNP-ul persoanei fizice”;

2) pentru organizații – cheia combinată „denumirea organizației publice și IDNO-ul organizației publice”;

3) pentru subdiviziunile organizației – cheia combinată „denumirea organizației publice și IDNO-ul organizației publice”+„denumirea subdiviziunii”;

4) activitatea angajatului – „numele/prenumele și IDNP-ul persoanei fizice”+„denumirea funcției”+„actul ce atestă numirea în funcție”;

5) Eveniment de gestiune a înregistrării (eveniment) - cheia combinată „numele/prenumele și IDNP-ul persoanei fizice”+ „tipul evenimentului” +„data evenimentului”.

25. Datele Sistemului informatic.

Datele prezentului Sistem reprezintă totalitatea de atribute ale obiectelor informaţionale şi includ:

1) date privind obiectul informaţional „profilul persoanei”:

a) Numele și prenumele
b) IDNP persoana
c) Seria, nr. buletinului de identitate
d) Viza de reședință
e) Starea civilă
f) Soț/Soție:
- Numele și prenumele
- IDNP
g) Copii minori
- Numele și prenumele
- Data și anul nașterii
- IDNP
h) Persoane aflate la întreținere
- Numele și prenumele
- Data și anul nașterii
- IDNP
i) Sex
j) Telefon fix
k) Telefon mobil
l) Email
m) Data creării
n) Data actualizării

2) date privind obiectul informaţional „Organizația”:

a) IDNO Organizației;
b) Denumirea Organizației;
c) Descrierea organizației
d) Date de contact;
e) Adresa;
f) Rechizite bancare;
g) Data creării;
h) Data actualizării.

3) date privind obiectul informaţional „Subdiviziunea Organizației”:

a) IDNO Organizației;
b) Denumirea Organizației;
c) Descrierea organizației
d) Denumirea Subdiviziunii;
e) Filiala;
f) Date de contact;
g) Adresa;
h) Rechizite bancare;

i) Data creării;
j) Data actualizării.

4) date privind obiectul informaţional „activitatea angajatului”:
a) Numele și prenumele
b) IDNP
c) Data angajării
d) IDNO Organizației;
e) Denumirea Organizației;
f) Subdiviziunea Organizației;
g) Funcția
h) Actul ce atestă numirea în funcție
i) Modificarea raportului de muncă
j) Data eliberării
k) Actul ce atestă eliberarea din funcție
l) Statutul angajatului în organizație
m) Transferat de la (IDNO Organizației)

5) date privind obiectul informaţional „eveniment”:
a) Evenimentul angajare/numire/alegere în funcție:
- IDNP al subiectului declarațiilor
- Data angajării
- Funcția
- Organizația
- Ordinul de angajare

b) Evenimentul demisie/eliberare din funcție:
- IDNP al subiectului declarațiilor
- Data eliberării din funcție
- Funcția
- Organizația
- Ordinul de eliberare

26. Scenarii de bază.

Scenariul de bază include o listă a evenimentelor ce se produc cu obiectul informaţional şi se ţin la evidenţă în Sistem. În RSD sânt ţinute la evidenţă următoarele evenimente:

1) *pentru obiectul informațional „Profilul persoanei”:*

a) Punerea primară în evidenţă se efectuează la angajare/numire/alegere în funcție și emiterea actului administrativ cu privire la angajarea în funcție a persoanei. Completarea automată a unui șir de date despre persoană poate fi realizată prin importul de date din Registrul de stat al populației.

2) *Actualizarea datelor privind „Profilul persoanei” se efectuează:*

a) la survenirea modificărilor în datele personale sau de familie ale persoanei;

b) la emiterea actului administrativ cu privire la transferul persoanei în altă funcție în cadrul aceleiași organizații.

3) *Radierea datelor*, prin aplicarea mențiunii „eliberat" în câmpul „statutul angajatului", se efectuează la emiterea actului administrativ cu privire la eliberarea din funcție.

4) *Popularea RSD se va implementa prin trei metode:*

a) La ingerarea declarațiilor digitizate și pe baza metadatele aferente lor, SI "E-Integritate" va popula registrul cu subiecți noi;

b) Actualizarea datelor din profilul persoanei (subiectului declarării) prin interfața de utilizator specifică, la depunerea declarațiilor prin metoda on-line;

c) La modificarea statutului subiectului, managerii resurselor umane vor introduce date referitor la subiect în registrul subiecților declarațiilor prin intermediul interfeței de utilizator specifice.

5) *Pentru obiectul informaţional „Organizaţia" și „Subdiviziunea organizației":*

a) Punerea primară în evidenţă se efectuează la înregistrarea Organizației la organele de înregistrare (Camera Înregistrării de Stat, Ministerul Justiției etc.), în care activează angajați cu statut de subiect al declarării. Completarea automată a unui șir de date despre Organizație poate fi realizată prin importul de date din Registrul de stat al unităților de drept.

b) Actualizarea datelor privind „Organizația" se efectuează la modificarea datelor de evidență a acesteia, precum denumirea, adresa, rechizitele bancare etc.

c) Radierea datelor, cu transferarea datelor în arhivă are loc în cazul lichidării sau reorganizării Organizației prin absorbirea ei de către altă organizație.

6) *Pentru obiectul informational „ Activitatea angajatului":*

a) Punerea primară în evidenţă se efectuează la angajare/numire/alegere în funcție și emiterea actului administrativ cu privire la angajarea în funcție a angajatului.

b) Actualizarea datelor privind activitatea angajatului se efectuează la emiterea actului administrativ cu privire la suspendarea raporturilor de muncă, eliberarea din funcție sau la transferul persoanei în altă funcție în cadrul aceleiași organizații.

7) *Pentru obiectul informational „Eveniment":*

a) Punerea primară în evidenţă se efectuează la înregistrarea evenimentului. Scoaterea din evidenţă se efectuează la anularea evenimentului sau după expirarea actualităţii informaţiei cu privire la eveniment.

27. Clasificatoarele și nomenclatoarele sistemului informatic.

În scopul asigurării veridicităţii şi asigurării interoperabilităţii RSD cu sisteme informatice terțe, reducerii volumului de informaţie stocată, se vor utiliza clasificatoare și nomenclatoare care pot fi divizate în 4 grupuri:

1) internaţionale (valorile cărora sunt standardizate și acceptate la nivel internațional);

2) naţionale (CUATM, FOJ, CFP etc.);

3) de interoperabilitate (valorile cărora sunt utilizate la interacțiune cu sisteme informatice terțe);

4) intrasistemice (variabile de system, parametri ai interfeței de utilizator, parametri de configurare a sistemului informatic, roluri, categoriile de documente, tipuri de încălcări, funcții publice).

28. Clasificatoarele intrasistemice se elaborează şi se utilizează în cadrul RSD doar în lipsa clasificatoarelor/nomenclatoarele internaţionale şi naţionale aprobate.

29. Interacțiunea cu alte sisteme informatice.

Pentru asigurarea funcționalității în condiții optime a RSD, este necesară realizarea interacțiunii cu alte sisteme informatice. În special, este prioritară integrarea cu următoarele servicii de platformă MCloud:

1) MPass - pentru autentificarea și controlul accesului;
2) MSign – pentru aplicarea și validarea semnăturii electronice;
3) MLog – pentru juranilizarea evenimentelor de business critice;
4) MNotify – pentru notificarea utilizatorilor.

30. Interacțiunea cu platforma de interoperabilitate MConnect va fi utilizată pentru interacțiunea RSD cu alte sisteme informatice, care aparțin autorităților publice ale Republicii Moldova (Registrul de stat al populației, Registrul de stat al unităților de drept).

Capitolul VII
SPAȚIUL TEHNOLOGIC AL SISTEMULUI INFORMATIC

31. RSD 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).

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

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

34. 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).

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

1) 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.

2) Mcloud – infrastructura TIC a platformei tehnologice guvernamentale comune care formează colud-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 RSD 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 jurnilizarea evenimentelor de business critice).

3) Calculatoare client – calculatoarele, de la care sunt accesate de către utilizatori (în funcție de drepturi și roluri) funcționalitățile RSD.

36. 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 RSD sunt efectuate prin intermediul conexiunilor sigure (VPN sau TLS/SSL).

37. RSD constă din următoarele componente funcționale:

1) 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 RSD.

2) Importul de date în format tipizat – care asigură posibilitatea importului de date din alte sisteme informatice (Registrul de stat al populației, Registrul de stat al unităților de drept) prin intermediul platformei de interoperabilitate MConnect.

3) Explorare Registru – care furnizează funcționalitatea de exploare a conținutului RSD (căutare/filtrare date, extragere date etc.).

4) Componenta de generare a rapoartelor – care furnizează funcționalități destinate prelucrării și prezentării datelor sub formă de indicatori de performanță, statisitici și rapoarte analitice;

5) 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.

Capitolul VIII
ASIGURAREA SECURITĂȚII INFORMAȚIONALE

38. Asigurarea securității informaționale.

Sistemul complex al securităţii informaționale reprezintă totalitatea normelor juridice în domeniu, măsurilor organizatorice şi economice, precum şi a mijloacelor tehnologice şi a metodelor de protecție criptografică şi software-hardware a informaţiei, care sânt orientate

spre asigurarea nivelului necesar al integrităţii, confidenţialităţii şi accesibilităţii resurselor informaţionale.

39. Sarcina de bază a securităţii informaţionale este asigurarea:

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

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

3) Asigurarea securității infrastructurii informaționale de tentative de a defecta sau de a modifica funcționarea acestuia.

40. Mecanismele principale de securitate informațională utilizate vor fi:

1) Autentificarea și autorizarea accesului la date;
2) Administrarea accesului la date;
3) Înregistrarea de audit a acțiunilor utilizatorilor sistemului informatic;
4) Criptarea datelor, după caz;
5) Auditul informatic;
6) Procedurile de restabilire în caz de dezastru.

41. 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.

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

43. 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:

1) SM ISO/CEI 15408-1:2014 „Tehnologia informaţiei. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informaţiei. Partea 1: Introducere şi model general”;

2) SM ISO/CEI 15408-2:2014 „Tehnologia informaţiei. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informaţiei. Partea 2: Cerinţe funcţionale de securitate”;

3) SM ISO/CEI 15408-3:2014 „Tehnologia informaţiei. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informaţiei. Partea 3: Cerinţe de asigurare a securităţii”;

4) SM SR ISO/CEI 27002:2017 “Tehnologia informației; Tehnici de securitate; Sisteme de management al securității informaționale. Cerințe;

5) SM ISO/CEI 27002:2017 “Tehnologia informației; Tehnici de securitate; Cod de bună practică pentru managementul securității informației.”

44. Reieșind din cele expuse, accesul la RSD 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).

45. 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.

46. Indiferent de nivelul de acces al utilizatorului (operator SRU, 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 va permite aplicarea de modificări prin inserarea unor înregistrări suplimentare care anulează sau modifică înregistrările sau starturile 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 RSD.

47. 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, RSD 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).

48. 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 RSD trebuie să dispună de posibilitatea de a-și defini politica de generare automată a copiilor de rezervă.

49. Întru asigurarea unui nivel adecvat al securității informaționale a RSD, în organizațiile publice, în care activează subiecții declarării 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.

50. Politica de securitate va fi adusă la cunoștința fiecărui utilizator contra semnătură. 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.

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

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

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

1) Sistemul informatic garantează păstrarea completă și integritatea tuturor înregistrărilor RSD;
2) Accesul la RSD 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.

54. Securitatea informațională presupune protecția RSD, 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.

55. Sarcina de bază a securității informaționale este asigurarea integrității și confidențialității informației. Exportul de date din RSD 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.