

**Specificații tehnice**

[Acest tabel va fi completat de către ofertant în coloanele 2, 3, 4, 6, 7,  
iar de către BNM – în coloanele 1, 5,]

Numărul procedurii de achiziție nr. <a href="#">ocds-b3wdp1-MD-1683180299953</a> din <b>26 mai 2023</b>
Obiectul achiziției: <b>Licențe și menținere pentru soluții de securitate</b>

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
<b>Lot 1: Extinderea sistemului de clasificare și marcare a documentelor și a mesageriei electronice</b>						
Licență pentru 100 utilizatori pentru sistemul de clasificare și marcare a documentelor și mesageriei electronice	TITUS	SUA	FORTRA	<p><b>Tip:</b> Extinderea licenței TITUS CLASSIFICATION cu 100 utilizatori sau echivalentul, inclusiv 12 luni de suport standard de la producător.</p> <p><b>Cantitate:</b> 1 licență pentru 100 utilizatori.</p> <p><b>Notă:</b> Luând în considerație că în BNM este deja în exploatare licență pentru 400 utilizatori, în caz de oferire a altui produs decât TITUS, Ofertantul trebuie să acopere cu licență pentru toți 500 utilizatori (100 noi + 400 existente deja exploatare în cadrul sistemului informațional al BNM). Totodată, Furnizorul va fi responsabil pentru livrarea, instalarea, configurarea (inclusiv configurarea politicilor inițiale) și punerea în funcțiune a soluției și pentru asigurarea suportului la definirea/configurarea și exploatarea soluției pentru primul an de exploatare a acesteia.</p>	<p><b>Tip:</b> Extinderea licenței TITUS CLASSIFICATION (Message Classification, Classification for Office, Classification for Desktop Standard Bundle) cu 100 utilizatori, inclusiv 12 luni de suport standard de la producător.</p> <p><b>Cantitate:</b> 1 licență Titus Message Classification, Classification for Office, Classification for Desktop Standard Bundle pentru 100 utilizatori, part number TMCTCOTCD-S-VOL1 .</p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p><b>Caracteristici:</b>  <i>Soluția trebuie să ofere următoarele funcționalități minime pentru un număr de 100 utilizatori:</i></p> <ul style="list-style-type: none"> <li>- <i>Selectarea consecventă forțată a etichetelor de clasificare.</i></li> <li>- <i>Aplicarea unor marcaje specifice vizuale asupra mesajelor de e-mail și documente.</i></li> <li>- <i>Punerea în aplicare a controalelor de securitate care pot fi declanșate pe bază etichetelor de clasificare selectate.</i></li> </ul> <p style="text-align: center;"><b>• Interfața cu utilizatorul:</b></p> <p><i>Soluția trebuie să permită selectarea unei etichete de clasificare, prin intermediul butonului de pe toolbar și a panoului de selecție.</i></p> <p><i>Soluția trebuie să solicite automat și obligatoriu utilizatorului selectarea unei etichete de clasificare prin intermediul unei ferestre de dialog (de selecție).</i></p> <p><i>Soluția trebuie să afișeze clasificarea unui e-mail primit în bara de instrumente și în panoul de selecție.</i></p> <p><i>Soluția trebuie să afișeze clasificare a unui document în bara de instrumente și în panoul de selecție.</i></p> <p><i>Soluția trebuie să furnizeze o metodă de sensibilă la context pentru a ghida (sugera) clasificarea.</i></p> <p><i>Soluția trebuie să permită utilizatorilor să clasifice un e-mail cu un singur click de mouse (sa permită one-click classification).</i></p> <p><i>Soluția trebuie să permită utilizatorilor să clasifice un document cu un singur click de mouse (să permită one-click classification).</i></p>	<p><b>Caracteristici:</b>  <i>Soluția oferă următoarele funcționalități minime pentru un număr de 100 utilizatori:</i></p> <ul style="list-style-type: none"> <li>- <i>Selectarea consecventă forțată a etichetelor de clasificare.</i></li> <li>- <i>Aplicarea unor marcaje specifice vizuale asupra mesajelor de e-mail și documente.</i></li> <li>- <i>Punerea în aplicare a controalelor de securitate care pot fi declanșate pe bază etichetelor de clasificare selectate.</i></li> </ul> <p style="text-align: center;"><b>• Interfața cu utilizatorul:</b></p> <p><i>Soluția permite selectarea unei etichete de clasificare, prin intermediul butonului de pe toolbar și a panoului de selecție.</i></p> <p><i>Soluția solicită automat și obligatoriu utilizatorului selectarea unei etichete de clasificare prin intermediul unei ferestre de dialog (de selecție).</i></p> <p><i>Soluția afișează clasificarea unui e-mail primit în bara de instrumente și în panoul de selecție.</i></p> <p><i>Soluția afișează clasificare a unui document în bara de instrumente și în panoul de selecție.</i></p> <p><i>Soluția furnizează o metodă de sensibilă la context pentru a ghida (sugera) clasificarea.</i></p> <p><i>Soluția permite utilizatorilor să clasifice un e-mail cu un singur click de mouse (permite one-click classification).</i></p> <p><i>Soluția permite utilizatorilor să clasifice un document cu un singur click de mouse (permite one-click classification).</i></p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p><i>Soluția trebuie să poată furniza un număr de nivele ale etichetelor de clasificare, care să poată defini politica de confidențialitate a instituției. Etichetele trebuie să fie personalizabile în Outlook și Office (aplicații existente în cadrul instituției).</i></p> <p><i>Soluția trebuie să ofere abilitatea de a stabili o selecție implicită pentru orice clasificare.</i></p> <p><i>Soluția trebuie să ofere abilitatea de a solicita utilizatorilor să modifice valorile de clasificare în cazul în care este detectat conținut sensibil documentele Office.</i></p> <p><i>Soluția trebuie să ofere abilitatea de a forța o selecție la orice nivel de clasificare.</i></p> <p><i>Soluția trebuie să furnizeze capacitatea de a suporta un număr de cel puțin 7 nivele de clasificare în Outlook.</i></p> <p><i>Soluția trebuie să furnizeze capacitatea de a suporta un număr de cel puțin 7 nivele de clasificare în suita de aplicații MS Office: Word, Excel, PowerPoint (aplicații existente în cadrul instituției).</i></p> <p><i>Soluția trebuie să furnizeze mai multe tipuri de controale de clasificare: liste de tip select, liste tip multi-select, calendare și casetele de text.</i></p> <p><i>Soluția trebuie să furnizeze Ajutor personalizabil HTML pentru a oferi suport în aplicație utilizatorilor.</i></p> <p><i>Soluția trebuie să furnizeze ajutor contextual, personalizabil, pentru clasificarea în Office (aplicație existent în cadrul instituției).</i></p> <p><i>Soluția trebuie să furnizeze ajutor contextual, personalizabil, pentru clasificarea în Outlook.</i></p>	<p><i>Soluția poate furniza un număr de nivele ale etichetelor de clasificare, care poate defini politica de confidențialitate a instituției. Etichetele sunt personalizabile în Outlook și Office (aplicații existente în cadrul instituției).</i></p> <p><i>Soluția oferă abilitatea de a stabili o selecție implicită pentru orice clasificare.</i></p> <p><i>Soluția oferă abilitatea de a solicita utilizatorilor să modifice valorile de clasificare în cazul în care este detectat conținut sensibil documentele Office.</i></p> <p><i>Soluția oferă abilitatea de a forța o selecție la orice nivel de clasificare.</i></p> <p><i>Soluția furnizează capacitatea de a suporta un număr de cel puțin 7 nivele de clasificare în Outlook.</i></p> <p><i>Soluția furnizează capacitatea de a suporta un număr de cel puțin 7 nivele de clasificare în suita de aplicații MS Office: Word, Excel, PowerPoint (aplicații existente în cadrul instituției).</i></p> <p><i>Soluția furnizează mai multe tipuri de controale de clasificare: liste de tip select, liste tip multi-select, calendare și casetele de text.</i></p> <p><i>Soluția furnizează ajutor personalizabil HTML pentru a oferi suport în aplicație utilizatorilor.</i></p> <p><i>Soluția furnizează ajutor contextual, personalizabil, pentru clasificarea în Office (aplicație existent în cadrul instituției).</i></p> <p><i>Soluția furnizează ajutor contextual, personalizabil, pentru clasificarea în Outlook.</i></p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p><i>Soluția trebuie să furnizeze avertismente, mesaje de avertisment sau eroare personalizabile, specifice politicii de clasificare a organizației.</i></p> <p><i>Soluția trebuie să ofere sprijin pentru clasificarea de rezervări din calendar și sarcini în Outlook.</i></p> <p><i>Sortarea, filtrarea și căutarea în Outlook trebuie să fie capabilă să folosească clasificarea furnizată de soluție drept criteriu.</i></p> <p><i>Soluția trebuie să ofere posibilitatea de a prezenta opțiuni suplimentare de clasificări în Outlook utilizatorului, în concordanță cu rolul lui în organizație.</i></p> <p><i>Soluția trebuie să ofere selecții de clasificare în Outlook, care pot fi afișate sau ascunse în funcție de proprietățile Active Directory.</i></p> <p><i>Soluția trebuie să ofere sprijin pentru perioadele de păstrare a datelor și declasificare folosind un câmp dată.</i></p> <p><i>Soluția trebuie să ofere sprijin pentru auto-completarea categoriei din Outlook bazat pe clasificare.</i></p> <p><i>Soluția trebuie să ofere posibilitatea de a obliga utilizatorul să introducă motive și justificări în cazul unui mesaj de tip avertizare sau prevenție.</i></p> <p><i>Soluția trebuie să ofere sprijin pentru marcarea (clasificarea) pe porțiuni (paragrafe) în documentele MS Office.</i></p> <p><i>Soluția trebuie să ofere sprijin pentru clasificarea mesajelor de e-mail primite în Outlook.</i></p>	<p><i>Soluția furnizează avertismente, mesaje de avertisment sau eroare personalizabile, specifice politicii de clasificare a organizației.</i></p> <p><i>Soluția oferă sprijin pentru clasificarea de rezervări din calendar și sarcini în Outlook.</i></p> <p><i>Sortarea, filtrarea și căutarea în Outlook sunt capabile să folosească clasificarea furnizată de soluție drept criteriu.</i></p> <p><i>Soluția oferă posibilitatea de a prezenta opțiuni suplimentare de clasificări în Outlook utilizatorului, în concordanță cu rolul lui în organizație.</i></p> <p><i>Soluția oferă selecții de clasificare în Outlook, care pot fi afișate sau ascunse în funcție de proprietățile Active Directory.</i></p> <p><i>Soluția oferă sprijin pentru perioadele de păstrare a datelor și declasificare folosind un câmp dată.</i></p> <p><i>Soluția oferă sprijin pentru auto-completarea categoriei din Outlook bazat pe clasificare.</i></p> <p><i>Soluția oferă posibilitatea de a obliga utilizatorul să introducă motive și justificări în cazul unui mesaj de tip avertizare sau prevenție.</i></p> <p><i>Soluția oferă sprijin pentru marcarea (clasificarea) pe porțiuni (paragrafe) în documentele MS Office.</i></p> <p><i>Soluția oferă sprijin pentru clasificarea mesajelor de e-mail primite în Outlook.</i></p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p><i>Soluția trebuie să ofere sprijin pentru afișarea clasificării mesajul în limba preferată a utilizatorului în Outlook.</i></p> <p><i>Soluția trebuie să ofere sprijin pentru interoperabilitatea în mediul multi-limbă în Outlook.</i></p> <p><i>Soluția trebuie să poată fi personalizată complet (inclusiv butoanele) în limba română.</i></p> <ul style="list-style-type: none"> <li>• <b>Marcaje vizuale:</b></li> </ul> <p><i>Soluția trebuie să ofere capacitatea de a insera etichete vizuale, în prima linie a unui mesaj de e-mail.</i></p> <p><i>Soluția trebuie să ofere capacitatea de a insera etichete vizuale în ultimul rând al unui mesaj de e-mail.</i></p> <p><i>Soluția trebuie să permită ca etichetele vizuale în prima linie și ultima de mesaj să fie diferite una de alta.</i></p> <p><i>Soluția trebuie să ofere posibilitatea de adăugare de eticheta-text vizuală specifică clasificării.</i></p> <p><i>Soluția trebuie să ofere posibilitatea formatării etichetei vizuale specifică clasificării.</i></p> <p><i>Soluția trebuie să ofere posibilitatea de introducere de etichete vizuale de clasificare în linia de subiect a unui mesaj de e-mail ca un prefix sau sufix la textul subiect.</i></p> <p><i>Soluția trebuie să ofere capacitatea de a insera abrevieri ale clasificării în linia de subiect a unui mesaj de e-mail.</i></p> <p><i>Soluția trebuie să ofere în mod automat adăugarea user-ului și a textului de semnătura specifică clasificării pentru un mesaj de e-mail.</i></p>	<p><i>Soluția oferă sprijin pentru afișarea clasificării mesajul în limba preferată a utilizatorului în Outlook.</i></p> <p><i>Soluția oferă sprijin pentru interoperabilitatea în mediul multi-limbă în Outlook.</i></p> <p><i>Soluția poate fi personalizată complet (inclusiv butoanele) în limba română.</i></p> <ul style="list-style-type: none"> <li>• <b>Marcaje vizuale:</b></li> </ul> <p><i>Soluția oferă capacitatea de a insera etichete vizuale, în prima linie a unui mesaj de e-mail.</i></p> <p><i>Soluția oferă capacitatea de a insera etichete vizuale în ultimul rând al unui mesaj de e-mail.</i></p> <p><i>Soluția permite ca etichetele vizuale în prima linie și ultima de mesaj să fie diferite una de alta.</i></p> <p><i>Soluția oferă posibilitatea de adăugare de eticheta-text vizuală specifică clasificării.</i></p> <p><i>Soluția oferă posibilitatea formatării etichetei vizuale specifică clasificării.</i></p> <p><i>Soluția oferă posibilitatea de introducere de etichete vizuale de clasificare în linia de subiect a unui mesaj de e-mail ca un prefix sau sufix la textul subiect.</i></p> <p><i>Soluția oferă capacitatea de a insera abrevieri ale clasificării în linia de subiect a unui mesaj de e-mail.</i></p> <p><i>Soluția oferă în mod automat adăugarea user-ului și a textului de semnătura specifică clasificării pentru un mesaj de e-mail.</i></p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p><i>Soluția trebuie să suporte adăugarea valorilor dinamice la etichete vizuale într-un mesaj de e-mail, care includ Clasificarea, Subiect, numele expeditorului, E-mail expeditor, Data Expediere, Ora Expediere, lista de atașamente și lista de destinatari.</i></p> <p><i>Soluția trebuie să accepte formatarea vizuală a etichetelor vizuale: font, dimensiunea și culoarea în HTML sau formate RTF mesaj.</i></p> <p><i>Soluția trebuie să suporte introducerea de etichete vizuale specifice clasificării în antetul și subsolul a documentului.</i></p> <p><i>Soluția trebuie să sprijine adăugarea valorilor dinamice pentru etichete vizuale în antet și subsol a unui document care include clasificarea și numele de utilizator.</i></p> <p><i>Soluția trebuie să accepte formatarea vizuală a etichetei: font, dimensiunea, culoarea și locația în antet și subsoluri ale unui document.</i></p> <p><i>Soluția trebuie să sprijine introducerea unei inscripționări de tip watermark specifică unei clasificări, într-un document Word, Excel, PowerPoint (aplicații existente în cadrul instituției).</i></p> <p><i>Soluția trebuie să sprijine introducerea numelui utilizatorului curent într-o inscripționare de tip watermark într-un document în Word, Excel, PowerPoint.</i></p> <ul style="list-style-type: none"> <li>• <b>Securitate:</b></li> </ul> <p><i>Soluția trebuie să permită o varietate de politici de clasificare a fi asociate cu orice selecție de clasificare.</i></p>	<p><i>Soluția suportă adăugarea valorilor dinamice la etichete vizuale într-un mesaj de e-mail, care includ Clasificarea, Subiect, numele expeditorului, E-mail expeditor, Data Expediere, Ora Expediere, lista de atașamente și lista de destinatari.</i></p> <p><i>Soluția acceptă formatarea vizuală a etichetelor vizuale: font, dimensiunea și culoarea în HTML sau formate RTF mesaj.</i></p> <p><i>Soluția suportă introducerea de etichete vizuale specifice clasificării în antetul și subsolul a documentului.</i></p> <p><i>Soluția sprijină adăugarea valorilor dinamice pentru etichete vizuale în antet și subsol a unui document care include clasificarea și numele de utilizator.</i></p> <p><i>Soluția acceptă formatarea vizuală a etichetei: font, dimensiunea, culoarea și locația în antet și subsoluri ale unui document.</i></p> <p><i>Soluția sprijină introducerea unei inscripționări de tip watermark specifică unei clasificări, într-un document Word, Excel, PowerPoint (aplicații existente în cadrul instituției).</i></p> <p><i>Soluția sprijină introducerea numelui utilizatorului curent într-o inscripționare de tip watermark într-un document în Word, Excel, PowerPoint.</i></p> <ul style="list-style-type: none"> <li>• <b>Securitate:</b></li> </ul> <p><i>Soluția permite o varietate de politici de clasificare a fi asociate cu orice selecție de clasificare.</i></p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p><i>Soluția trebuie să suporte capacitatea de a restricționa destinatarul unui mesaj e-mail în Outlook pe bază atât a clasificării mesajului cât și a valorilor atributului destinatar sau calității de membru în grupul Active Directory.</i></p> <p><i>Soluția trebuie să suporte capacitatea de a prezenta avertismente de clasificare specifice la trimiterea unui mesaj de e-mail.</i></p> <p><i>Soluția trebuie să ofere capacitatea de a forța clasificarea documentului înainte de a-l salva sau imprima.</i></p> <p><i>Soluția trebuie să ofere capacitatea de a forța clasificarea mesajului înainte de a-l salva, trimite sau imprima.</i></p> <p><i>Soluția trebuie să ofere capacitatea de a prezenta avertismentele și, opțional, a preveni trimiterea unui mesaj de e-mail, bazat atât pe clasificare cât și pe numărul de destinatari.</i></p> <p><i>Soluția trebuie să ofere capacitatea de a controla trimiterea de e-mail-uri bazate pe domenii de destinatari: în acest caz domeniile pot fi descrise ca domenii permise sau refuzate.</i></p> <p><i>Soluția trebuie să stocheze metadatele de clasificare ca proprietăți MAPI ale unui mesaj de e-mail.</i></p> <p><i>Soluția trebuie să poată insera metadatele de clasificare în proprietățile particularizate ale documentului.</i></p> <p><i>Soluția trebuie să poată introduce metadatele de clasificare în antetul SMTP X al mesajului e-mail.</i></p>	<p><i>Soluția suportă capacitatea de a restricționa destinatarul unui mesaj e-mail în Outlook pe bază atât a clasificării mesajului cât și a valorilor atributului destinatar sau calității de membru în grupul Active Directory.</i></p> <p><i>Soluția suportă capacitatea de a prezenta avertismente de clasificare specifice la trimiterea unui mesaj de e-mail.</i></p> <p><i>Soluția oferă capacitatea de a forța clasificarea documentului înainte de a-l salva sau imprima.</i></p> <p><i>Soluția oferă capacitatea de a forța clasificarea mesajului înainte de a-l salva, trimite sau imprima.</i></p> <p><i>Soluția oferă capacitatea de a prezenta avertismentele și, opțional, a preveni trimiterea unui mesaj de e-mail, bazat atât pe clasificare cât și pe numărul de destinatari.</i></p> <p><i>Soluția oferă capacitatea de a controla trimiterea de e-mail-uri bazate pe domenii de destinatari: în acest caz domeniile pot fi descrise ca domenii permise sau refuzate.</i></p> <p><i>Soluția stochează metadatele de clasificare ca proprietăți MAPI ale unui mesaj de e-mail.</i></p> <p><i>Soluția poate insera metadatele de clasificare în proprietățile particularizate ale documentului.</i></p> <p><i>Soluția poate introduce metadatele de clasificare în antetul SMTP X al mesajului e-mail.</i></p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Produ cătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p><i>Soluția trebuie să ofere capacitatea de a forța selecția pentru orice set de clasificări ale unui mesaj e-mail înainte de a fi transmis.</i></p> <p><i>Soluția trebuie să ofere capacitatea de a forța în mod automat, transparent și consecvent aplicarea drepturilor Management Services (RMS) conform template-urilor RMS existente, unui mesaj de e-mail în Outlook, pe bază clasificările specifice, înainte de a fi transmis.</i></p> <p><i>Soluția trebuie să ofere capacitatea de a aplica criptare S / MIME și semnătură digitală unui mesaj de e-mail bazat pe clasificarea mesajului.</i></p> <p><i>Soluția trebuie să ofere capacitatea de a avertiza și, opțional, a preveni trimiterea unui mesaj de e-mail în cazul în care clasificarea este downgraded la momentul de Reply sau Forward.</i></p> <p><i>Soluția trebuie să ofere capacitatea de a avertiza și, opțional, împiedica expedierea în cazul în care clasificarea este schimbată la momentul de Reply sau Forward în Outlook.</i></p> <p><i>Soluția trebuie să ofere capacitatea de a pune în BCC o adresă de mail specifică, în bază clasificării mesajului în Outlook.</i></p> <p><i>Soluția trebuie să ofere capacitatea de a înregistra toate acțiunile de clasificare la jurnalul de evenimente Windows (acțiune, inclusiv motiv acțiune și justificare acțiune). Jurnalizarea să poată fi personalizată (ex. doar pentru mesaje de tip avertizare sau prevenție).</i></p> <p><i>Soluția trebuie să accepte verificarea atașamentelor, utilizând metadatele atașamentului create la</i></p>	<p><i>Soluția oferă capacitatea de a forța selecția pentru orice set de clasificări ale unui mesaj e-mail înainte de a fi transmis.</i></p> <p><i>Soluția oferă capacitatea de a forța în mod automat, transparent și consecvent aplicarea drepturilor Management Services (RMS) conform template-urilor RMS existente, unui mesaj de e-mail în Outlook, pe bază clasificările specifice, înainte de a fi transmis.</i></p> <p><i>Soluția oferă capacitatea de a aplica criptare S / MIME și semnătură digitală unui mesaj de e-mail bazat pe clasificarea mesajului.</i></p> <p><i>Soluția oferă capacitatea de a avertiza și, opțional, a preveni trimiterea unui mesaj de e-mail în cazul în care clasificarea este downgraded la momentul de Reply sau Forward.</i></p> <p><i>Soluția oferă capacitatea de a avertiza și, opțional, împiedica expedierea în cazul în care clasificarea este schimbată la momentul de Reply sau Forward în Outlook.</i></p> <p><i>Soluția oferă capacitatea de a pune în BCC o adresă de mail specifică, în bază clasificării mesajului în Outlook.</i></p> <p><i>Soluția oferă capacitatea de a înregistra toate acțiunile de clasificare la jurnalul de evenimente Windows (acțiune, inclusiv motiv acțiune și justificare acțiune). Jurnalizarea poate fi personalizată (ex. doar pentru mesaje de tip avertizare sau prevenție).</i></p> <p><i>Soluția acceptă verificarea atașamentelor, utilizând metadatele atașamentului create la clasificare</i></p>	



Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p><i>clasificare pentru document, precum și, clasificarea încorporată în e-mail. De exemplu, dacă un document este clasificat ca, de exemplu, "Secret" și este atașat la un e-mail, soluția să poată asigura că e-mail este clasificat cel puțin la același nivel, dacă nu, să avertizeze sau să prevină, în funcție de setările din sistem.</i></p> <p><i>Soluția trebuie să ofere capacitatea de a avertiza și de a preveni, opțional, utilizatorii la trimiterea de e-mailuri, cu o linie de subiect cu caractere prea puține în Outlook.</i></p> <p><i>Soluția trebuie să includă o funcție de scanare de conținut care poate scana un mesaj de e-mail și documentele anexate în bază unor expresii de text și modele de expresie regulate configurate în prealabil înainte de a trimite și apoi de a avertiza utilizatorii și, opțional, a preveni trimiterea dacă este detectat conținut sensibil.</i></p> <p><i>Soluția trebuie să includă o funcție de revizuire de conținut ce scoate în evidență vizual conținutul considerat sensibil într-un e-mail, astfel încât utilizatorii să poată remedia orice încălcări ale politicilor, înainte ca e-mail-ul să părăsească desktop, în Outlook.</i></p> <p><i>Soluția trebuie să includă o caracteristică redactare care permite utilizatorilor de a redacta în mod automat (adică înnegrit) conținutul sensibil într-un e-mail în Outlook.</i></p> <p><i>Soluția să ofere facilități sporite de redactare interactivă de tip „do it yourself” – care permite utilizatorilor să evidențieze rapid și să ”înnegrască”</i></p>	<p><i>pentru document, precum și, clasificarea încorporată în e-mail. De exemplu, dacă un document este clasificat ca, de exemplu, "Secret" și este atașat la un e-mail, soluția să poată asigura că e-mail este clasificat cel puțin la același nivel, dacă nu, să avertizeze sau să prevină, în funcție de setările din sistem.</i></p> <p><i>Soluția oferă capacitatea de a avertiza și de a preveni, opțional, utilizatorii la trimiterea de e-mailuri, cu o linie de subiect cu caractere prea puține în Outlook.</i></p> <p><i>Soluția include o funcție de scanare de conținut care poate scana un mesaj de e-mail și documentele anexate în bază unor expresii de text și modele de expresie regulate configurate în prealabil înainte de a trimite și apoi de a avertiza utilizatorii și, opțional, a preveni trimiterea dacă este detectat conținut sensibil.</i></p> <p><i>Soluția include o funcție de revizuire de conținut ce scoate în evidență vizual conținutul considerat sensibil într-un e-mail, astfel încât utilizatorii să poată remedia orice încălcări ale politicilor, înainte ca e-mail-ul să părăsească desktop, în Outlook.</i></p> <p><i>Soluția include o caracteristică redactare care permite utilizatorilor de a redacta în mod automat (adică înnegrit) conținutul sensibil într-un e-mail în Outlook.</i></p> <p><i>Soluția oferă facilități sporite de redactare interactivă de tip „do it yourself” – care permite utilizatorilor să evidențieze rapid și să</i></p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p><i>textul pe care doresc să îl redacteze (elimine din vizualizare) în cadrul e-mail-urilor.</i></p> <p><i>Soluția trebuie să ofere facilități îmbunătățite de validare de conținut: să permită administratorilor de a combina mai multe norme privind controalele avansate de politici. De exemplu, se pot verifica atât atașamentele, precum și adresele e-mail ale destinatarilor pentru orice încălcări ale politicilor, pentru a permite verificarea tipului de fișier care se trimite și cui se trimite.</i></p> <p><i>Soluția trebuie să ofere interoperabilitate cu soluțiile de clasificare ale altor tipuri de documente decât documentele de tip Office: inclusiv PDF, CAD, video, imagini și alte fișiere – pentru a se verifica ca nu sunt clasificate la un nivel mai ridicat decât e-mail.</i></p> <p><i>Soluția trebuie să ofere capacitatea de a forța în mod automat aplicarea drepturilor din template-urile Management Services (RMS), pe un document bazat, pe clasificările specifice.</i></p> <p><i>Soluția trebuie să includă capacitatea de a avertiza și de a preveni, opțional, salvarea și imprimarea dacă orice clasificare este downgrad-ată în Office existent.</i></p> <p><i>Soluția trebuie să interopereze cu conversia de document Office - PDF, prin salvarea valorilor de clasificare proprietățile fișierului PDF creat.</i></p> <p><i>Soluția trebuie să ofere capacitatea de a scana documentul și sugestia utilizatorului atunci când un cuvânt sau o frază poate fi inadecvată pentru clasificarea actuală.</i></p>	<p><i>”înnegrească” textul pe care doresc să îl redacteze (elimine din vizualizare) în cadrul e-mail-urilor.</i></p> <p><i>Soluția trebuie să ofere facilități îmbunătățite de validare de conținut: să permită administratorilor de a combina mai multe norme privind controalele avansate de politici. De exemplu, se pot verifica atât atașamentele, precum și adresele e-mail ale destinatarilor pentru orice încălcări ale politicilor, pentru a permite verificarea tipului de fișier care se trimite și cui se trimite.</i></p> <p><i>Soluția oferă interoperabilitate cu soluțiile de clasificare ale altor tipuri de documente decât documentele de tip Office: inclusiv PDF, CAD, video, imagini și alte fișiere – pentru a se verifica ca nu sunt clasificate la un nivel mai ridicat decât e-mail.</i></p> <p><i>Soluția oferă capacitatea de a forța în mod automat aplicarea drepturilor din template-urile Management Services (RMS), pe un document bazat, pe clasificările specifice.</i></p> <p><i>Soluția include capacitatea de a avertiza și de a preveni, opțional, salvarea și imprimarea dacă orice clasificare este downgrad-ată în Office existent.</i></p> <p><i>Soluția interoperează cu conversia de document Office - PDF, prin salvarea valorilor de clasificare proprietățile fișierului PDF creat.</i></p> <p><i>Soluția oferă capacitatea de a scana documentul și sugestia utilizatorului atunci când un cuvânt sau o frază poate fi inadecvată pentru clasificarea actuală.</i></p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p><i>Soluția trebuie să ofere capacitatea, bazată pe clasificare, de a elimina automat conținutul potențial sensibil și a informațiilor din documentele Word, inclusiv Comentarii, revizuirii, versiunile, Informații personale, Antet e-mail, Routing Slip, Trimitere pentru revizuire, Document Properties, Template, Document Workspace, Adnotări, Proprietăți Document Server, Policy Management ale documentului, tipul de conținut, Custom XML, anteturi și subsoluri, și textul ascuns, prin intermediul inspectorilor de document.</i></p> <p><i>Soluția trebuie să fie în măsură a preveni vizualizarea mesajelor e-mail sensibile atunci când se accesează Inbox-ul prin intermediul Outlook Web Access.</i></p> <ul style="list-style-type: none"> <li>• <b>Interoperabilitate:</b></li> </ul> <p><i>Soluția trebuie să ofere posibilitatea de a atașa metadate la documentele Office, astfel încât aceste metadate de clasificare să poată fi utilizate de alte soluții terțe precum DLP (Data Loss Prevention) pentru a proteja informațiile din organizație.</i></p> <p><i>Soluția trebuie să ofere posibilitatea de a atașa metadate la documentele Office astfel încât să poată fi refolosite de soluția SharePoint existentă care oferă securitate sporită documentelor, etichetare a documentelor și conversie automată în PDF.</i></p> <p><i>Soluția trebuie să permită aplicarea unor politici de arhivare a mesajelor e-mail în bază clasificărilor atașate mesajelor e-mail.</i></p> <p><i>Soluția trebuie să permită refolosirea clasificării e-mail-urilor de soluțiile e-Discovery.</i></p>	<p><i>Soluția oferă capacitatea, bazată pe clasificare, de a elimina automat conținutul potențial sensibil și a informațiilor din documentele Word, inclusiv Comentarii, revizuirii, versiunile, Informații personale, Antet e-mail, Routing Slip, Trimitere pentru revizuire, Document Properties, Template, Document Workspace, Adnotări, Proprietăți Document Server, Policy Management ale documentului, tipul de conținut, Custom XML, anteturi și subsoluri, și textul ascuns, prin intermediul inspectorilor de document.</i></p> <p><i>Soluția este în măsură a preveni vizualizarea mesajelor e-mail sensibile atunci când se accesează Inbox-ul prin intermediul Outlook Web Access.</i></p> <ul style="list-style-type: none"> <li>• <b>Interoperabilitate:</b></li> </ul> <p><i>Soluția oferă posibilitatea de a atașa metadate la documentele Office, astfel încât aceste metadate de clasificare să poată fi utilizate de alte soluții terțe precum DLP (Data Loss Prevention) pentru a proteja informațiile din organizație.</i></p> <p><i>Soluția oferă posibilitatea de a atașa metadate la documentele Office astfel încât să poată fi refolosite de soluția SharePoint existentă care oferă securitate sporită documentelor, etichetare a documentelor și conversie automată în PDF.</i></p> <p><i>Soluția permite aplicarea unor politici de arhivare a mesajelor e-mail în bază clasificărilor atașate mesajelor e-mail.</i></p> <p><i>Soluția permite refolosirea clasificării e-mail-urilor de soluțiile e-Discovery.</i></p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p><i>Soluția trebuie să furnizeze date cuprinzătoare referitoare la acțiunile utilizatorului, astfel încât să poată fi refolosite de o varietate largă de soluții de raportare logg-uri.</i></p> <p><i>Soluția trebuie să ofere capacitatea de a interopera cu soluția de managementul documentelor, cu soluția de arhivare precum și cu alte tipuri de soluții cum ar fi:</i></p> <ul style="list-style-type: none"> <li>- soluții SIEM (Sistem integrat de management al evenimentelor)</li> <li>- soluții de management al drepturilor asupra documentelor</li> <li>- soluții de criptare</li> <li>- soluții de e-discovery</li> <li>- soluții de Data Loss Prevention</li> </ul> <p><b>• Implementare, compatibilitate și configurare:</b></p> <p><i>Soluția trebuie să lucreze cu MS Office Professional Plus 2016/2021, Microsoft 365 E3.</i></p> <p><i>Soluția trebuie să ofere posibilitatea de a configura schema de clasificare, de a adăuga sau a modifica etichetele de la o locație centrală, fără a necesita modificări pe fiecare stație de lucru individuală.</i></p> <ul style="list-style-type: none"> <li>• <b>Cerințe față de serviciile de suport:</b> <ul style="list-style-type: none"> <li>- Product updates/upgrade;</li> <li>- Access your Account Information;</li> <li>- Contact Technical Support Team (Create New Cases, obtain the status of current cases);</li> <li>- Search the Knowledge Database;</li> </ul> </li> </ul> <p><i>Obtain Product Documentation (admin guides).</i></p>	<p><i>Soluția furnizează date cuprinzătoare referitoare la acțiunile utilizatorului, astfel încât să poată fi refolosite de o varietate largă de soluții de raportare logg-uri.</i></p> <p><i>Soluția oferă capacitatea de a interopera cu soluția de managementul documentelor, cu soluția de arhivare precum și cu alte tipuri de soluții cum ar fi:</i></p> <ul style="list-style-type: none"> <li>- soluții SIEM (Sistem integrat de management al evenimentelor)</li> <li>- soluții de management al drepturilor asupra documentelor</li> <li>- soluții de criptare</li> <li>- soluții de e-discovery</li> <li>- soluții de Data Loss Prevention</li> </ul> <p><b>• Implementare, compatibilitate și configurare:</b></p> <p><i>Soluția lucrează cu MS Office Professional Plus 2010/2013/2016/2019/2021, Microsoft 365 E3, E5.</i></p> <p><i>Soluția oferă posibilitatea de a configura schema de clasificare, de a adăuga sau a modifica etichetele de la o locație centrală, fără a necesita modificări pe fiecare stație de lucru individuală.</i></p> <ul style="list-style-type: none"> <li>• <b>Cerințe față de serviciile de suport:</b> <ul style="list-style-type: none"> <li>- Product updates/upgrade;</li> <li>- Access your Account Information;</li> <li>- Contact Technical Support Team (Create New Cases, obtain the status of current cases);</li> <li>- Search the Knowledge Database;</li> </ul> </li> </ul> <p><i>Obtain Product Documentation (admin guides).</i></p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
<b>Lot 2: Extinderea soluția de prevenire a scurgerii de informație</b>						
Licență pentru 100 utilizatori pentru soluția de prevenire a scurgerii de informație	Trellix (McAfee) Total Protection	SUA	Trellix	<p><b>Tip:</b> Extinderea licenței pentru soluția de prevenire a scurgerii de informație McAfee Total Protection For Data Loss Prevention Appliance Software cu 100 utilizatori, inclusiv 12 luni de suport standard de la producător, care va include control pentru:</p> <ul style="list-style-type: none"> <li>- Stații de lucru (endpoint)</li> <li>- Serviciul proxy (iCap)</li> <li>- Serviciul de poștă electronică (SMTP)</li> <li>- Monitorizarea rețelei (Network monitor).</li> </ul> <p><b>Cantitate:</b> 1 licență pentru 100 utilizatori.</p> <p><i>Notă: Luând în considerație că în BNM este deja în exploatare licență pentru 400 utilizatori, în caz de oferire a altui produs decât McAfee DLP, Ofertantul trebuie să acopere cu licență pentru toți 500 utilizatori (100 noi + 400 existente deja exploatate în cadrul sistemului informațional al BNM). Totodată, va fi responsabil pentru livrarea, instalarea, configurarea (inclusiv configurarea politicilor inițiale) și punerea în funcțiune a soluției și pentru asigurarea suportului la definirea/configurarea și exploatarea soluției pentru primul an de exploatare a acesteia.</i></p> <p><b>Caracteristici:</b></p> <ul style="list-style-type: none"> <li>• <b><u>Protecție Endpoint:</u></b></li> <li>- să suporte sistemele de operare: Microsoft Windows 10, Microsoft Windows 11.</li> <li>- să identifice conținutul chiar dacă acesta este arhivat (minimum 10 niveluri de arhivare).</li> </ul>	<p><b>Tip:</b> Extinderea licenței pentru soluția de prevenire a scurgerii de informație McAfee (Trellix) Total Protection For Data Loss Prevention Appliance Software cu 100 utilizatori, inclusiv 12 luni de suport standard de la producător, care va include control pentru:</p> <ul style="list-style-type: none"> <li>- Stații de lucru (endpoint)</li> <li>- Serviciul proxy (iCap)</li> <li>- Serviciul de poștă electronică (SMTP)</li> <li>- Monitorizarea rețelei (Network monitor).</li> </ul> <p><b>Cantitate:</b> 1 licență (Trellix (McAfee) Total Protection for Data Loss Prevention Appliance Software) pentru 100 utilizatori.</p> <p><b>Caracteristici:</b></p> <ul style="list-style-type: none"> <li>• <b><u>Protecție Endpoint:</u></b></li> <li>- suportă sistemele de operare: Microsoft Windows 10, Microsoft Windows 11.</li> <li>- identifică conținutul chiar dacă acesta este arhivat (minimum 10 niveluri de arhivare).</li> </ul>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<ul style="list-style-type: none"> <li>- să poată aplica politici bazate pe conținut confidențial pentru cel puțin 300 de tipuri de fișiere.</li> <li>- să poată detecta documentele ce au fost clasificate deja (fie prin intermeniul unui instrument de clasificare a documentelor prin înscrierea în Metadate și/sau prin aplicare de marcări vizuale, fie prin faptul că documentul dat conține careva marcaje vizuale cu privire la clasa căreia aparține (ex. mențiuni în header/footer pentru documente word) sau în funcție de sursa documentului - aplicația prin intermediul căreia a fost creat).</li> <li>- agentul soluției să poată proteja minim 100.000 de documente indiferent dacă stația este Online sau Offline;</li> <li>- analiza conținutului să nu fie limitată la limba utilizată;</li> <li>- soluția trebuie să permită parametrizarea nivelului de utilizare a resurselor utilizate (procesor, RAM);</li> <li>- să protejeze informația confidențială la: <ul style="list-style-type: none"> <li>- scrierea pe suporturi de stocare mobile (memorii USB, optice etc.);</li> <li>- trimisă prin intermediul serviciilor de poștă electronică;</li> <li>- încărcată pe web;</li> <li>- copiată cu ajutorul clipboard-ului;</li> <li>- printată în fișier sau pe imprimantă;</li> <li>- scrisă pe un share în rețea;</li> <li>- folosită în aplicațiile network-based;</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>- poate aplica politici bazate pe conținut confidențial pentru cel puțin 300 de tipuri de fișiere.</li> <li>- poate detecta documentele ce au fost clasificate deja (fie prin intermeniul unui instrument de clasificare a documentelor prin înscrierea în Metadate și/sau prin aplicare de marcări vizuale, fie prin faptul că documentul dat conține careva marcaje vizuale cu privire la clasa căreia aparține (ex. mențiuni în header/footer pentru documente word) sau în funcție de sursa documentului - aplicația prin intermediul căreia a fost creat).</li> <li>- agentul soluției poate proteja minim 100.000 de documente indiferent dacă stația este Online sau Offline;</li> <li>- analiza conținutului nu este limitată la limba utilizată;</li> <li>- soluția permite parametrizarea nivelului de utilizare a resurselor utilizate (procesor, RAM);</li> <li>- protejează informația confidențială la: <ul style="list-style-type: none"> <li>- scrierea pe suporturi de stocare mobile (memorii USB, optice etc.);</li> <li>- trimisă prin intermediul serviciilor de poștă electronică;</li> <li>- încărcată pe web;</li> <li>- copiată cu ajutorul clipboard-ului;</li> <li>- printată în fișier sau pe imprimantă;</li> <li>- scrisă pe un share în rețea;</li> <li>- folosită în aplicațiile network-based;</li> </ul> </li> </ul>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Produ cătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<ul style="list-style-type: none"> <li>- la efectuarea screenshot-ului ecranului.</li> <li>- să mențină înregistrări de audit privind activitatea agentului de endpoint;</li> <li>- să mențină înregistrări de audit privind activitatea agentului de endpoint;</li> <li>- soluția trebuie să dispună de mecanisme proprii de instalare a agenților pe stațiile de lucru sau alte sisteme, sau să permită integrarea cu Directory Services;</li> <li>- agentul de endpoint trebuie să fie compatibil, determinat prin testări, cu soluții de antivirus, firewall, criptare, backup și antispypware third-party;</li> <li>- agentul de endpoint trebuie să permită aplicarea politicilor folosind conținut înregistrat/ amprentat;</li> <li>- agentul de endpoint trebuie să aibă opțiunea de blocare a activității pentru situațiile de încălcare a politicii de securitate prestabilită (ex. - se încearcă upload-area de documente considerate confidențiale; - copierea pe SD card, USB flash drive / memory stick; - crearea de noi documente pe baza celor originale; - crearea de arhive și upload-area ulterioară a acestora (sau copierea pe USB flash);</li> <li>- construirea regulilor de protecție trebuie să se poată face și în funcție de cuvinte-cheie, expresii regulate și amprente (hash-uri);</li> <li>- construcția regulilor trebuie să includă suport pentru logica booleana incluzând AND, OR, sau alte declarații logice;</li> </ul>	<ul style="list-style-type: none"> <li>- la efectuarea screenshot-ului ecranului.</li> <li>- menține înregistrări de audit privind activitatea agentului de endpoint;</li> <li>- menține înregistrări de audit privind activitatea agentului de endpoint;</li> <li>- soluția dispune de mecanisme proprii de instalare a agenților pe stațiile de lucru sau alte sisteme, sau să permită integrarea cu Directory Services;</li> <li>- agentul de endpoint este compatibil, determinat prin testări, cu soluții de antivirus, firewall, criptare, backup și antispypware third-party;</li> <li>- agentul de endpoint permite aplicarea politicilor folosind conținut înregistrat/ amprentat;</li> <li>- agentul de endpoint are opțiunea de blocare a activității pentru situațiile de încălcare a politicii de securitate prestabilită (ex. - se încearcă upload-area de documente considerate confidențiale; - copierea pe SD card, USB flash drive / memory stick; - crearea de noi documente pe baza celor originale; - crearea de arhive și upload-area ulterioară a acestora (sau copierea pe USB flash);</li> <li>- construirea regulilor de protecție se poate face și în funcție de cuvinte-cheie, expresii regulate și amprente (hash-uri);</li> <li>- construcția regulilor include suport pentru logica booleana incluzând AND, OR, sau alte declarații logice;</li> </ul>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p>- soluția trebuie să aibă abilitatea de a identifica fișierele bazându-se pe conceptul de true file type și nu doar pe extensia fișierelor;</p> <p>- trebuie să poată scana stația și să identifice documentele ce conțin informații clasificate (funcții de tipul descoperă - discovery);</p> <p>- să permită efectuarea de notificări personalizate;</p> <p>- trebuie să fie capabilă să identifice nivelul de clasificare a documentelor din marcajele vizuale și să aplice regulile de protecție pe aceste documente.;</p> <p>- trebuie să fie capabilă să protejeze documente nemarcate ce au conținut ce provine din documente clasificate cu marcaje vizuale.</p> <p>- soluția trebuie să permită crearea de politici în mod granular de permitere / blocare a dispozitivelor periferice pe baza informațiilor despre:</p> <p>a. ID Producător</p> <p>b. ID Model Dispozitiv Periferic</p> <p>c. Tipul de dispozitiv</p> <p>d. Clasa dispozitivului detectat de sistemul de operare</p> <p>e. BUS Conectare (USB, S-ATA, ETC.)</p> <p>f. Numele Dispozitivului</p> <p>g. Tipul sistemului de fișiere (NTFS/FAT/FAT32)</p> <p>h. Numele Volumului / Partiției (în cazul dispozitivelor de stocare date)</p> <p>- soluția trebuie să poată lua următoarele acțiuni la conectarea unui dispozitiv periferic:</p>	<p>- soluția are abilitatea de a identifica fișierele bazându-se pe conceptul de true file type și nu doar pe extensia fișierelor;</p> <p>- poate scana stația și să identifice documentele ce conțin informații clasificate (funcții de tipul descoperă - discovery);</p> <p>- permite efectuarea de notificări personalizate;</p> <p>- capabil să identifice nivelul de clasificare a documentelor din marcajele vizuale și să aplice regulile de protecție pe aceste documente.;</p> <p>- capabil să protejeze documente nemarcate ce au conținut ce provine din documente clasificate cu marcaje vizuale.</p> <p>- soluția permite crearea de politici în mod granular de permitere / blocare a dispozitivelor periferice pe baza informațiilor despre:</p> <p>a. ID Producător</p> <p>b. ID Model Dispozitiv Periferic</p> <p>c. Tipul de dispozitiv</p> <p>d. Clasa dispozitivului detectat de sistemul de operare</p> <p>e. BUS Conectare (USB, S-ATA, ETC.)</p> <p>f. Numele Dispozitivului</p> <p>g. Tipul sistemului de fișiere (NTFS/FAT/FAT32)</p> <p>h. Numele Volumului / Partiției (în cazul dispozitivelor de stocare date)</p> <p>- soluția poate lua următoarele acțiuni la conectarea unui dispozitiv periferic:</p>	



Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p>a. <i>blocare</i>: să nu permită instalarea acestuia;</p> <p>b. <i>monitorizare</i>: să genereze un eveniment ce conține detalii despre dispozitiv;</p> <p>c. <i>forțare mod utilizare ReadOnly</i>: în cazul dispozitivelor de stocare date, acestea se vor utiliza doar pentru citirea datelor de pe ele.</p> <p>d. <i>soluția trebuie să poată prevenii executarea de cod și aplicații direct de pe dispozitive externe. De asemenea, trebuie să vină și cu un mecanism de macare a aplicațiilor permise.</i></p> <p>- <i>soluția trebuie să permită aplicarea de politici diferite în funcție de locația utilizatorului (ex: să nu poată conecta imprimante atunci când nu se află în perimetrul rețelei).</i></p> <p>- <i>soluția trebuie să ofere un mecanism de dezactivare a restricțiilor pentru utilizatorii ce nu au conectivitate cu severul de administrare.</i></p> <p>- <i>soluția trebuie să permită construirea unei liste de dispozitive permise și corelarea acestei liste la utilizatori / grupuri de utilizatori din Directory Services, astfel încât aceștia să poată utiliza dispozitivele indiferent de calculatorul la care se afla.</i></p> <p>- <i>soluția trebuie să permită alertarea administratorului atunci când sunt copiate informații pe dispozitive externe de stocare date. Pentru situații în care stația de lucru este offline, soluția va stoca informația respectivă local, iar la prima conectare on-line, va asigura alertarea administratorului.</i></p>	<p>a. <i>blocare</i>: să nu permită instalarea acestuia;</p> <p>b. <i>monitorizare</i>: să genereze un eveniment ce conține detalii despre dispozitiv;</p> <p>c. <i>forțare mod utilizare ReadOnly</i>: în cazul dispozitivelor de stocare date, acestea se vor utiliza doar pentru citirea datelor de pe ele.</p> <p>d. <i>soluția poate prevenii executarea de cod și aplicații direct de pe dispozitive externe. De asemenea, vine și cu un mecanism de macare a aplicațiilor permise.</i></p> <p>- <i>soluția permite aplicarea de politici diferite în funcție de locația utilizatorului (ex: să nu poată conecta imprimante atunci când nu se află în perimetrul rețelei).</i></p> <p>- <i>soluția oferă un mecanism de dezactivare a restricțiilor pentru utilizatorii ce nu au conectivitate cu severul de administrare.</i></p> <p>- <i>soluția permite construirea unei liste de dispozitive permise și corelarea acestei liste la utilizatori / grupuri de utilizatori din Directory Services, astfel încât aceștia să poată utiliza dispozitivele indiferent de calculatorul la care se afla.</i></p> <p>- <i>soluția permite alertarea administratorului atunci când sunt copiate informații pe dispozitive externe de stocare date. Pentru situații în care stația de lucru este offline, soluția va stoca informația respectivă local, iar la prima conectare on-line, va asigura alertarea administratorului.</i></p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p>- soluția trebuie să permită filtrarea fișierelor ce sunt copiate pe dispozitive externe de stocare date după extensie și /sau tip de fișier. Tipul de fișier trebuie identificat indiferent de extensia acestuia. (ex: blocarea copierii fișierelor Microsoft Office Word, Adobe Reader PDF).</p> <p>- soluția trebuie să nu poată fi oprită (stopată activitatea) de utilizator chiar dacă acesta are dreptul de administrator local.</p> <p>- soluția trebuie să permită crearea unei reguli de shadowing(duplicare) a fișierelor copiate pe dispozitive externe atunci când anumite criterii sunt indeplinite (Ex: un anumit utilizator, grup de utilizatori, tipul fișierului, extensia fișierului). Duplicatul fișierului trebuie să poată fi accesat numai de cei ce au acest drept în consola de administrare.</p> <ul style="list-style-type: none"> <li>• <b><u>Protecția resurselor de rețea:</u></b></li> </ul> <p>- să poată efectua descoperirea, indexarea și înregistrarea datelor din baze de date de tipul MySQL, Oracle.</p> <p>- pentru fișierele ce trebuie protejate să poată preveni upload-ul efectuat direct din consolă.</p> <p>- soluția trebuie să asigure accesul la interfața de administrare prin intermediul unui portal web securizat SSL.</p> <p>- să permită aplicarea de filtre în procesul de descoperire a datelor (spre exemplu, excluderea fișierelor mai mari de X MB).</p> <p>- să poată efectua extragerea de informații din arhive cu peste 10 niveluri.</p>	<p>- soluția permite filtrarea fișierelor ce sunt copiate pe dispozitive externe de stocare date după extensie și /sau tip de fișier. Tipul de fișier este identificat indiferent de extensia acestuia. (ex: blocarea copierii fișierelor Microsoft Office Word, Adobe Reader PDF).</p> <p>- soluția nu poate fi oprită (stopată activitatea) de utilizator chiar dacă acesta are dreptul de administrator local.</p> <p>- soluția permite crearea unei reguli de shadowing(duplicare) a fișierelor copiate pe dispozitive externe atunci când anumite criterii sunt indeplinite (Ex: un anumit utilizator, grup de utilizatori, tipul fișierului, extensia fișierului). Duplicatul fișierului poate fi accesat numai de cei ce au acest drept în consola de administrare.</p> <ul style="list-style-type: none"> <li>• <b><u>Protecția resurselor de rețea:</u></b></li> </ul> <p>- poate efectua descoperirea, indexarea și înregistrarea datelor din baze de date de tipul MySQL, Oracle.</p> <p>- pentru fișierele ce trebuie protejate poate preveni upload-ul efectuat direct din consolă.</p> <p>- soluția asigură accesul la interfața de administrare prin intermediul unui portal web securizat SSL.</p> <p>- permite aplicarea de filtre în procesul de descoperire a datelor (spre exemplu, excluderea fișierelor mai mari de X MB).</p> <p>- poate efectua extragerea de informații din arhive cu peste 10 niveluri.</p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Produ cătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p>- să permită setarea nivelului de resurse pe care în consumă (ex. lățimea de bandă la scanare).</p> <p>- soluția trebuie să scaneze incremental în CIFS, NFS, FTP.</p> <ul style="list-style-type: none"> <li>• <b><u>Protecție Proxy:</u></b> soluția trebuie să fie capabilă să se integreze cu serviciul de proxy al BNM (McAfee WebGateway) și trebuie să protejeze împotriva transmiterii neautorizate de date și informații prin protocoalele de rețea HTTP, HTTP/S și FTP.</li> <li>• <b><u>Protecție Email:</u></b> soluția trebuie să fie capabilă să se integreze cu serviciul de email al BNM (Microsoft Exchange 2016 și alte versiuni ulterioare, MS Outlook).</li> <li>• <b><u>Network monitor:</u></b> <ul style="list-style-type: none"> <li>- soluția trebuie să fie capabilă să scaneze, analizeze și să clasifice în timp real traficul de ieșire din/în rețeaua Internet/BNM pentru majoritatea protocoalelor de rețea (HTTP, SMTP, IMAP, POP3, FTP, Telnet, Rlogin, SSH, webmail, Yahoo! Chat, AOL Chat, MSN Chat, ICY, TSP, SOCKS, PCAnywhere, RDP, VNC, SMB, Citrix, Skype, IRC, LDAP, DASL, NTLM, Kazaa, BitTorrent, eDonkey, Gnutella, DirectConnect, MP2P, WinMX, Sherlock, eMule, and more);</li> <li>- soluția trebuie să fie capabilă să se integreze pasiv cu echipamentul de rețea utilizând SPAN port sau “physically inline network tap” (optional);</li> <li>- soluția trebuie să asigure vizualizarea rapoartelor de incident.</li> </ul> </li> </ul> <ul style="list-style-type: none"> <li>• <b><u>Cerințe privind administrarea:</u></b></li> </ul>	<p>- permite setarea nivelului de resurse pe care le consumă (ex. lățimea de bandă la scanare).</p> <p>- soluția scanează incremental în CIFS, NFS, FTP.</p> <ul style="list-style-type: none"> <li>• <b><u>Protecție Proxy:</u></b> soluția este capabilă să se integreze cu serviciul de proxy al BNM (McAfee WebGateway) și trebuie să protejeze împotriva transmiterii neautorizate de date și informații prin protocoalele de rețea HTTP, HTTP/S și FTP.</li> <li>• <b><u>Protecție Email:</u></b> soluția este capabilă să se integreze cu serviciul de email al BNM (Microsoft Exchange 2016 și alte versiuni ulterioare, MS Outlook).</li> <li>• <b><u>Network monitor:</u></b> <ul style="list-style-type: none"> <li>- soluția este capabilă să scaneze, analizeze și să clasifice în timp real traficul de ieșire din/în rețeaua Internet/BNM pentru majoritatea protocoalelor de rețea (HTTP, SMTP, IMAP, POP3, FTP, Telnet, Rlogin, SSH, webmail, Yahoo! Chat, AOL Chat, MSN Chat, ICY, TSP, SOCKS, PCAnywhere, RDP, VNC, SMB, Citrix, Skype, IRC, LDAP, DASL, NTLM, Kazaa, BitTorrent, eDonkey, Gnutella, DirectConnect, MP2P, WinMX, Sherlock, eMule, and more);</li> <li>- soluția este capabilă să se integreze pasiv cu echipamentul de rețea utilizând SPAN port sau “physically inline network tap” (optional);</li> <li>- soluția asigură vizualizarea rapoartelor de incident.</li> </ul> </li> </ul> <ul style="list-style-type: none"> <li>• <b><u>Cerințe privind administrarea:</u></b></li> </ul>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p>- consola trebuie să permită atribuirea automată a politicilor pe stații și servere în funcție de specificațiile sistemului (ex: Platforma desktop/server, Subnet, tip procesor, sistem de operare).</p> <p>- sincronizarea dintre server și client trebuie să se facă dinspre client către server.</p> <p>- administrarea componentelor de data loss prevention și de control al dispozitivelor externe trebuie să se poată face dintr-o singură consola.</p> <p>- consola de administrare trebuie să poată fi instalată într-un mediu virtual.</p> <p>- soluția trebuie să poată filtra evenimentele ce sunt generate de componentele aflate pe stațiile de lucru astfel încât baza de date să nu se încarce cu informații considerate inutile.</p> <p>- soluția trebuie să permită configurarea de mesaje în funcție de tipul evenimentului.</p> <p>- accesul în consola de administrare să poată fi făcut pe baza credențialelor din Directory Services.</p> <p>- consola de administrare trebuie să permită crearea de roluri în mod granular pentru cei ce o administrează.</p> <p>- soluția trebuie să ducă loguri (înregistrări de audit) cu privire la acțiunile utilizatorilor în consolă.</p> <p>- consola trebuie să permită construirea unei liste de contacte în vederea folosirii acestora pentru notificări prin mesagerie electronică (E-mail).</p>	<p>- consola permite atribuirea automată a politicilor pe stații și servere în funcție de specificațiile sistemului (ex: Platforma desktop/server, Subnet, tip procesor, sistem de operare).</p> <p>- sincronizarea dintre server și client se face dinspre client către server.</p> <p>- administrarea componentelor de data loss prevention și de control al dispozitivelor externe se pot face dintr-o singură consola.</p> <p>- consola de administrare poate fi instalată într-un mediu virtual.</p> <p>- soluția poate filtra evenimentele ce sunt generate de componentele aflate pe stațiile de lucru astfel încât baza de date să nu se încarce cu informații considerate inutile.</p> <p>- soluția permite configurarea de mesaje în funcție de tipul evenimentului.</p> <p>- accesul în consola de administrare poate fi făcut pe baza credențialelor din Directory Services.</p> <p>- consola de administrare permite crearea de roluri în mod granular pentru cei ce o administrează.</p> <p>- soluția duce/colectează loguri (înregistrări de audit) cu privire la acțiunile utilizatorilor în consolă.</p> <p>- consola permite construirea unei liste de contacte în vederea folosirii acestora pentru notificări prin mesagerie electronică (E-mail).</p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p>- consola de administrare trebuie să poată fi accesată de pe orice computer din rețea în mod securizat, fără necesitatea instalării de software adițional.</p> <p>- dacă serverul de administrare este accesat prin intermediul unei interfețe web, trebuie să fie posibil importul unui certificat ssl generat de o autoritate locală, înlocuindu-l astfel pe cel auto-generat.</p> <p>- sistemul trebuie să permită setarea periodicității de sincronizare dintre server și componente.</p> <p>- sistemul trebuie să permită setarea periodicității de transmitere a evenimentelor de pe client pe server.</p> <p>- sistemul trebuie să poată / permită automatizarea de sarcini de instalare / dezinstalare a componentelor pe stațiile de lucru, de rulare a rapoartelor și de transmiterea de notificări de prin mesagerie electronică.</p> <p>- sistemul (serverul) trebuie să fie capabil să declanșeze acțiuni automate atunci când anumite condiții sunt îndeplinite (ex: generarea unui eveniment pe server, pe o stație de lucru, detectarea unui nou sistem pe rețea).</p> <p>- soluția trebuie să permită aplicarea de politici diferite pentru sisteme pe: a. sisteme individuale; b. grupuri de sisteme; c. sisteme din Directory Services ce aparțin aceleiași OU.</p> <p>- soluția trebuie să permită accesarea logurilor componente de sincronizare de pe sisteme în timp real prin intermediul unui serviciu web.</p>	<p>- consola de administrare poate fi accesată de pe orice computer din rețea în mod securizat, fără necesitatea instalării de software adițional.</p> <p>- dacă serverul de administrare este accesat prin intermediul unei interfețe web, este posibil importul unui certificat ssl generat de o autoritate locală, înlocuindu-l astfel pe cel auto-generat.</p> <p>- sistemul permite setarea periodicității de sincronizare dintre server și componente.</p> <p>- sistemul permite setarea periodicității de transmitere a evenimentelor de pe client pe server.</p> <p>- sistemul poate / permite automatizarea de sarcini de instalare / dezinstalare a componentelor pe stațiile de lucru, de rulare a rapoartelor și de transmiterea de notificări de prin mesagerie electronică.</p> <p>- sistemul (serverul) este capabil să declanșeze acțiuni automate atunci când anumite condiții sunt îndeplinite (ex: generarea unui eveniment pe server, pe o stație de lucru, detectarea unui nou sistem pe rețea).</p> <p>- soluția permite aplicarea de politici diferite pentru sisteme pe: a. sisteme individuale; b. grupuri de sisteme; c. sisteme din Directory Services ce aparțin aceleiași OU.</p> <p>- soluția permite accesarea logurilor componente de sincronizare de pe sisteme în timp real prin intermediul unui serviciu web.</p>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<ul style="list-style-type: none"> <li>• <b><u>Cerințe privind subsistemul de raportare:</u></b></li> <li>- soluția trebuie să asigure generarea de rapoarte despre nodurile administrate (endpoint-uri sau de rețea) și despre evenimentele generate de ele.</li> <li>- soluția trebuie să permită crearea de noi rapoarte în mod granular cu informații extrase din evenimente, sau despre sistemele administrate.</li> <li>- rapoartele pot fi generate sub formă de tabel, pie chart, bubble chart, listă, sumar, sau grafic istoric.</li> <li>- soluția trebuie să poată exporta rapoartele în cel puțin următoarele formate: pdf, csv, html.</li> <li>- soluția trebuie să permită personalizarea rapoartelor (ex. aplicarea logo-ului BNM).</li> <li>- soluția trebuie să permită atât salvarea sub formă de fișiere a rapoartelor cât și expedierea acestora prin e-mail.</li> <li>- soluția trebuie să permită aplicarea de filtre pe evenimente la generarea rapoartelor.</li> <li>- soluția trebuie să poată genera rapoarte privind (dar nelimitându-se la): <ul style="list-style-type: none"> <li>a. log-urile de audit administrative;</li> <li>b. detalii despre sistemele administrate (detalii de configurare, hardware, utilizator);</li> <li>c. evenimente de la sistem;</li> <li>d. informații despre politicile și sarcinile aplicate sistemelor;</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b><u>Cerințe privind subsistemul de raportare:</u></b></li> <li>- soluția asigură generarea de rapoarte despre nodurile administrate (endpoint-uri sau de rețea) și despre evenimentele generate de ele.</li> <li>- soluția permite crearea de noi rapoarte în mod granular cu informații extrase din evenimente, sau despre sistemele administrate.</li> <li>- rapoartele pot fi generate sub formă de tabel, pie chart, bubble chart, listă, sumar, sau grafic istoric.</li> <li>- soluția poate exporta rapoartele în cel puțin următoarele formate: pdf, csv, html.</li> <li>- soluția permite personalizarea rapoartelor (ex. aplicarea logo-ului BNM).</li> <li>- soluția permite atât salvarea sub formă de fișiere a rapoartelor cât și expedierea acestora prin e-mail.</li> <li>- soluția permite aplicarea de filtre pe evenimente la generarea rapoartelor.</li> <li>- soluția poate genera rapoarte privind (dar nelimitându-se la): <ul style="list-style-type: none"> <li>f. log-urile de audit administrative;</li> <li>g. detalii despre sistemele administrate (detalii de configurare, hardware, utilizator);</li> <li>h. evenimente de la sistem;</li> <li>i. informații despre politicile și sarcinile aplicate sistemelor;</li> </ul> </li> </ul>	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p>e. informații furnizate de agenți.</p> <ul style="list-style-type: none"> <li>• <b>Cerințe față de serviciile de suport:</b></li> <li>- Daily product updates (.DATs, engines, etc.);</li> <li>- Product upgrades;</li> <li>- Malware alerts with remediation analysis;</li> <li>- Malware analysis service;</li> <li>- Malware trend podcasts and blogs;</li> <li>- Chat, web, and phone support with remote desktop control;</li> <li>- 24/7 phone support (normally under 5 minutes to expert), unlimited number of calls to McAfee Technical Support;</li> <li>- Automatic diagnostic and remediation tools;</li> <li>- Online product test environments.</li> </ul>	<p>j. informații furnizate de agenți.</p> <ul style="list-style-type: none"> <li>• <b>Cerințe față de serviciile de suport:</b></li> <li>- Daily product updates (.DATs, engines, etc.);</li> <li>- Product upgrades;</li> <li>- Malware alerts with remediation analysis;</li> <li>- Malware analysis service;</li> <li>- Malware trend podcasts and blogs;</li> <li>- Chat, web, and phone support with remote desktop control;</li> <li>- 24/7 phone support (normally under 5 minutes to expert), unlimited number of calls to McAfee (Trellix) Technical Support;</li> <li>- Automatic diagnostic and remediation tools;</li> <li>- Online product test environments.</li> </ul>	

**Lot 3: Extinderea și menținerea licențelor pentru soluția Gemalto SafeNet**

Licență pentru 150 utilizatori pentru soluția de autentificare multifactorială pe bază de certificate PKI Gemalto SafeNet Authentication Client și vSEC:CMS	Gemalto SafeNet Authentication Client și vSEC:CMS	Franta	Thales	<p><b>Tip:</b> Extinderea licenței pentru soluția de autentificare multifactorială pe bază de certificate PKI exploatată în cadrul sistemului informațional al BNM Gemalto SafeNet Authentication Client și vSEC:CMS cu 150 utilizatori sau echivalentul, inclusiv suport standard de la producător.</p> <p><b>Cantitate:</b> Licență de tip vSEC:CMS S-Series Device License pentru 150 utilizatori.</p> <p><b>Cerințe obligatorii:</b> Perioada de suport standard de la producător trebuie să fie egalată cu perioada de suport pentru soluția de autentificare multifactorială pe bază de certificate PKI Gemalto SafeNet Authentication Client și vSEC:CMS exploatată în</p>	<p><b>Tip:</b> Extinderea licenței pentru soluția de autentificare multifactorială pe bază de certificate PKI exploatată în cadrul sistemului informațional al BNM Gemalto SafeNet Authentication Client și vSEC:CMS cu 150 utilizatori, inclusiv suport standard de la producător.</p> <p><b>Cantitate:</b> Licență de tip vSEC:CMS S-Series Device License pentru 150 utilizatori.</p> <p><b>Cerințe obligatorii:</b> Perioada de suport standard de la producător va fi egalată cu perioada de suport pentru soluția de autentificare multifactorială pe bază de certificate PKI Gemalto SafeNet Authentication Client și vSEC:CMS exploatată în</p>	
---	---	--------	--------	---	---	--

Denumirea bunurilor/serviciilor	Denumirea modelului bunului	Țara de origine	Producele	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
				<p><i>cadrul Sistemului Informațional al BNM până la 11.07.2024.</i></p> <p><b>Cerințe față de suport:</b></p> <ul style="list-style-type: none"> <li>- Product updates and releases;</li> <li>- Portal and phone support;</li> <li>- 8 x 5 support, unlimited number of calls to Gemalto Technical Support.</li> </ul>	<p><i>cadrul Sistemului Informațional al BNM până la 11.07.2024.</i></p> <p><b>Cerințe față de suport:</b></p> <ul style="list-style-type: none"> <li>- Product updates and releases;</li> <li>- Portal and phone support;</li> <li>- 8 x 5 support, unlimited number of calls to Gemalto Technical Support.</li> </ul>	
Servicii de asigurare a accesului la suport anual pentru soluția de autentificare multifactorială Gemalto SafeNet Authentication Client și vSEC:CMS	Gemalto SafeNet Authentication Client și vSEC:CMS	Franta	Thales	<p><b>Tip:</b> Servicii de asigurare a suportului anual de la producător de tip Standard, sau echivalent, pentru perioada 12.07.2023 – 11.07.2024, pentru soluția de autentificare multifactorială pe bază de certificate PKI exploatată de către BNM Gemalto SafeNet Authentication Client și vSEC:CMS, cu următoarele componente:</p> <ul style="list-style-type: none"> <li>- SafeNet Authentication Client – User License: 300 un;</li> <li>- vSEC:CMS S-Series Device License: 360 un;</li> <li>- vSEC:CMS S-Series Secure System License: 1 un.</li> </ul> <p><b>Cerințe minime de suport:</b></p> <ul style="list-style-type: none"> <li>- Product updates and releases;</li> <li>- Portal and phone support;</li> <li>- 8 x5 support, unlimited number of calls to Gemalto Technical Support.</li> </ul> <p><b>Forma de prestare:</b> Prelungirea perioadei de acces la suport anual se va confirma prin prezentarea de către Prestator a unui document confirmativ parvenit de la compania producător / partener autorizat de producător pentru perioada solicitată, sau publicarea informației confirmative pe site-ul producătorului.</p>	<p><b>Tip:</b> Servicii de asigurare a suportului anual de la producător de tip Standard, pentru perioada 12.07.2023 – 11.07.2024, pentru soluția de autentificare multifactorială pe bază de certificate PKI exploatată de către BNM Gemalto SafeNet Authentication Client și vSEC:CMS, cu următoarele componente:</p> <ul style="list-style-type: none"> <li>- SafeNet Authentication Client – User License: 300 un;</li> <li>- vSEC:CMS S-Series Device License: 360 un;</li> <li>- vSEC:CMS S-Series Secure System License: 1 un.</li> </ul> <p><b>Cerințe minime de suport:</b></p> <ul style="list-style-type: none"> <li>- Product updates and releases;</li> <li>- Portal and phone support;</li> <li>- 8 x5 support, unlimited number of calls to Gemalto Technical Support.</li> </ul> <p><b>Forma de prestare:</b> Prelungirea perioadei de acces la suport anual se va confirma prin prezentarea de către Prestator a unui document confirmativ parvenit de la compania producător / partener autorizat de producător pentru perioada solicitată, sau publicarea informației confirmative pe site-ul producătorului.</p>	



