Anexa 1 - Exemplu de format pentru proces-verbal de recepție cantitativa

Contract nr.	*[introduceți]*
Contractant	*[introduceți]*
Referința proiectului, dacă este cazul	*[Numele proiectului]*
Dată livrare produs	*[zz/ll/aaaa]*

Nr.	*Denumirea (conform Caiet de Sarcini/Contract*)	*Referință (conform Caiet de Sarcini/Contract*)
1.	*[introduceți]*	*[introduceți clauza din contract sau capitolul din Caietul de Sarcini unde este specificat produsul respectiv]*
2.	*[introduceți]*	*[introduceți]*
3.	*[introduceți]*	*[introduceți]*
4.	*[introduceți]*	*[introduceți]*

Contractant **Autoritatea Contractantă**

Dată:

Nume:

Funcția:

Aprobat:

Anexa 2 - Exemplu de format pentru proces-verbal de recepție calitativa

1. Context

1.1. Contract	
1.2. Contractant	
1.3. Referința proiectului (dacă este cazul)	

2.Lista produselor

2.1. Produs	2.2 Referință (conform Caiet de Sarcini/Contract)	2.3. Termenul de livrare

3. Concluzii cu privire la acceptare

☐	3.1. Acceptare (fără observatii/rezerve)		
☐	3.2. Acceptare cu observatii minore		
☐	3.3. Acceptare cu rezerve (Contractantul se angajează să corecteze - în timpul convenit - defectele constatate și descrise la punctul 5 din prezentul document).		
☐	3.4. Este aplicabilă perioada de garanție?	Data finalizării:	
☐	3.5. Refuzat (Contractantul se angajează să corecteze greșelile constatate și descrise la punctul 5 din prezentul document). Remedierea defectelor trebuie efectuată în conformitate cu cele stabilite în Contract.		

4. Semnaturi

4.1. CONTRACTANT		4.2. AUTORITATE CONTRACTANTĂ/ACHIZITOR			
Data:		Data:		Data:	
Nume:		Nume:		Nume:	
Funcția:		Funcția:		Funcția:	
Aprobat:		Aprobat:		Aprobat:	
Acceptare finală *[dacă este cazul]*:					
Data:		Data:		Data:	
Nume:		Nume:		Nume:	
Funcția:		Funcția:		Funcția:	
Aprobat:		Aprobat:		Aprobat:	

5. Observații

[introduceți]

ANEXA 3- SPECIFICATII MINIME LICENTA ANTIVIRUS

CARACTERISTICI GENERALE ALE PRODUSULUI

Produsul („solutia") reprezinta o platforma integrata pentru managementul securitatii, gandita ca o solutie modulara. Produsul contine urmatoarele module:

A. O consola de management care asigura functionalitati de administrare.
B. Protectie antimalware pentru statii fizice, laptop-uri si servere.

A. CONSOLA DE MANAGEMENT

1. Cerinte generale:

1. Interfata consolei de management va fi in limba romana.
2. Interfata clientului de securitate, care se instaleaza pe statii si servere, va fi in limba romana.
3. Manualul de instalare a produsului va fi in limba romana.
4. Manualul de administrare a produsului va fi in limba romana.
5. Solutia va pemite activarea/dezactivarea actualizarilor de produs/semnaturi.
6. Actualizari automate a consolei de management facute de catre producatorul solutiei, fara a fi necesara interventia utilizatorului.
7. Notificarile – prezente in interfata, notificarile necitite sunt evidentiate, trimise catre una sau mai multe adrese de email, alerteaza administratorul in cazul unor probleme majore: licentiere, detectie virusi, actualizari de produs disponibile).
8. Consola de management este accesibila de oriunde in lume (este bazata pe un serviciu cloud de tip Software-as-a-Service), fara a fi nevoie de setari suplimentare din partea utilizatorului.

2. Panou de monitorizare si raportare (Dashboard):

1. Rapoartele din panoul de monitorizare vor putea fi configurate specificand numele raportului, tipul raportului, tinta raportului, optiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul dupa care o statie este considerata neactualizata).
2. Panoul central contine rapoarte pentru toate modulele suportate.
3. Rapoartele din panoul central de comanda permit: adaugarea altor rapoarte, stergerea lor si rearanjarea.

3. Inventarierea retelei – managementul securitatii:

1. Solutia se va integra cu domeniul Active Directory si va putea importa inventarul.
2. Se permite descoperirea statiilor statii fizice neintegrate in Active Directory (Workgroup) cu ajutorul Network discovery.
3. Solutia va oferi optiuni de cautare, sortare si filtrare dupa numele sistemului, sistem de operare, adresa IP, politica aplicata, ultima data cand s-a conectat (online si/sau offline) si FQDN.
4. Solutia va permite crearea unui pachet unic pentru toate sistemele de operare, de statii sau servere. Astfel, administratorul va putea descarca pachetele pentru protectia statiilor si serverelor pe care ruleaza sistemul de operare Windows, Linux, Mac.

4. Politici:

1. Solutia va permite configurarea setarilor antimalware prin intermediul politicilor din consola de magement.
2. Politica va contine optiuni specifice de activare/dezactivare si configurarea functionalitatilor precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicatiilor, scanarea traficului web,controlul dispozitivelor, power user.
3. Solutia permite aplicarea politicilor pe masini client, grupuri de masini, domeniu, unitati organizationale.

5. Rapoarte:

1. Solutia va contine rapoarte care prezinta statusul masinilor clientil din punct de vedere al actualizarilor, fisierelor malware detectate, aplicatiile blocate, site-urilor web blocate.
2. Rapoartele programate pot fi trimise catre un numar nelimitat de adrese de email (nu este nevoie sa aiba un cont in consola de management).
3. Solutia va permite vizualizarea rapoartelor curente programate de administrator.
4. Solutia va permite exportarea rapoartelor in format .pdf si detaliile ca format .csv.

6. Carantina:

1. Solutia va permite restaurarea fisierelor carantinate in locatia originala sau intr-o cale configurabila cu optiunea de excludere automata a fisierului restaurat.
2. Carantina va fi locala, pe fiecare statia administrata si va fi administrata, fie local, fie din consola de management.

7. Log-uri:

1. Inregistrarea actiunilor utilizatorilor.
2. Se vor oferi informatii detaliate pentru fiecare actiune a unui utilizator.
3. Se va permite filtrarea actiunilor utilizator dupa numele utilizatorului, actiune.

8. Actualizare:

1. Se permite definirea de locatii de actualizare multiple.
2. Se permite activarea/dezactivarea actualizarilor de produs si semnaturi.

B. PROTECTIE STATII SI SERVERE FIZICE

1. Caracteristici generale minimale si eliminatorii:

1. Pentru reducerea la minim a consumului de resurse, solutia antimalware trebuie sa permita instalarea personalizata a modulelor detinute (de exemplu, sa permita instalarea solutiei antimalware fara modulul de control al accesului web, modul de control al dispozitivilelor sau modulul firewall).
2. Pentru o mai buna protectie a statiilor si serverelor, solutia include un vaccin anti-ransomware. Acest vaccin asigura protectia impotriva tuturor amenintarilor cunoscute de tip ransomware, prin imunizarea statiilor si serverelor, chiar daca sunt infectate si prin blocarea procesului de criptare.
3. Vaccinul anti-ransomware primeste actualizari de la producator, odata cu actualizarea semnaturilor produsului Antimalware.
4. entru o mai buna protectie a a statiilor si serverelor, solutia include un modul integrat de tip ERA (Endpoint Risk Analytics – Analiza de risc a endpoint-ului) capabil sa identifice si remedieze in mod automatizat sau manual un numar mare de riscuri existente la nivel de retea sau sistem de operare ce pot afecta functionalitatea si nivelul de securizare al endpoint-ului

2. Cerinte de sistem:

- Sisteme de operare pentru statii de lucru: **Windows 10, Windows 8/8.1, Windows 7**, , **MAC OS X Catalina (10.15.x), Mac OS X Mojave (10.14.x), Mac OS X High Sierra (10.13.x), Mac OS X Sierra (10.12.x), Mac OS X El Capitan (10.11.x), Mac OS X Yosemite (10.10.5), Mac OS X Mavericks (10.9.5)**
- Sisteme de operare embedded: **Windows 10 IoT Enterprise, Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7**
- Sisteme de operare pentru servere: **Windows Server 2019, Windows Server 2016 (inc Core), Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2**
- Sisteme de operare Linux: Red Hat Enterprise Linux / CentOS 6 or higher, Ubuntu 14.04 LTS or higher, SUSE Linux Enterprise Server 11 SP4 or higher, OpenSUSE LEAP 42.x or higher, Fedora 25 or higher, Debian 8.0 or higher, Oracle Linux 6.3 or higher, Amazon Linux AMI 2016.09 or higher.

3. Administrare si instalare remote:

1. Inainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user.
2. Instalarea se va putea face in mai multe moduri:
   a. prin descarcarea directa a pachetului pe statia pe care se va face instalarea;
   b. prin instalarea la distanta, direct din consola de management
   c. trimiterea pe email (oricate adrese) a pachetului de instalare pentru Windows, Linux, Mac.
3. Instalarea clientilor la distanta in alte locatii decat cele in care este instalata consola de management se va face prin intermediul unui client existent in locatiile respective de tip relay pentru a minimiza traficul in WAN.
4. In consola vor fi disponibile informatii despre fiecare statie: numele statiei, IP, sistem de operare, module instalate, politica aplicata, informatii despre actualizari etc.
5. Posibilitatea creari unui singur pachet de instalare, utilizabil atat pentru sistemele de operare pe 32 de biti cat si pentru cele pe 64 de biti.
6. Posibilitatea creari unui singur pachet de instalare, utilizabil pentru statii (fizice si/sau virtuale), servere (fizice si/sau virtuale).
7. Posibilitatea de a crea pachetele de instalare de tip web installer sau kit full.

4. Caracteristici si functionalitati principale ale modulului antimalware:

1. Definirea pana la 16 nivele de profunzime pentru scanarea in arhive.
2. Scanarea automata a emailurilor la nivelul statiei de lucru pentru POP3/SMTP.
3. Clientii antimalware pentru workstation sa permita definirea unor liste de excludere de la scanarea in timp real si la cerere a anumitor directoare, discuri, fisiere, extensii sau procese.
4. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul va trebui sa ofere protectie anti-spyware.
5. Posibilitatea de configura scanarile programate sa se execute cu prioritate redusa
6. Pentru o protectie sporita, solutia antimalware trebuie sa aiba 3 tipuri de detectie: bazata pe semnaturi, bazata de comportamentul fisierelor si bazata pe monitorizarea proceselor.
7. Pentru o protectie sporita, solutia antimalware trebuie sa poata scana paginile HTTP.
8. Pentru siguranta utilizatorului, clientul va include un modul de antiphishing.

5. Anti-Exploit-Avansat:

1. Posibilitatea de a opri atacurile avansate de tip „zero-day” efectuate prin intermediul unor exploit-uri evazive
2. Depistarea in timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare.

6. Firewall:

1. Posibilitatea de a configura reguli de firewall pentru aplicatii sau conectivitate.
2. Posibilitatea de a defini retele de incredere pentru masina destinatie.
3. Abilitatea de a detecta scanarea de porturi.

7. Carantina:

1. Produsul antimalware sa permita trimiterea automata a fisierelor din carantina catre laboratoarele antimalware ale producatorului.
2. Trimiterea continutului carantinei va putea fi expediat in mod automat, la un interval definit de administrator.

8. Controlul continutului:

1. Consola va avea integrat un modul dedicat controlului accesului la Internet cu urmatoarele particularitati:
   a. Permite blocarea accesului la Internet pentru anumite masini client sau grupuri de masini.
   b. Permite blocarea paginilor de internet care contin anumite cuvinte cheie.

c. Permite restrictionarea accesului pe anumite pagini de internet dupa anumite categorii prestabilite (ex: online dating, violenta, pornografie etc).

9. Controlul dispozitivelor:

1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.
2. Modulul va permite controlul urmatoarelor tipuri de dispozitive:

a. Bluetooth Devices
b. CDROM Devices
c. Floppy Disk Drives
d. Modems
e. Tape Drives
f. Windows Portable
g. Printers
h. Network Adapters
i. Wireless Network Adapters
j. Internal and External Storage

10. Actualizare:

1. Posibilitatea efectuarii actualizarii la nivel de statie in mod silentios (fara avertizare).
2. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate).
3. Actualizarea pentru locatiile remote prin intermediul unui client antimalware care are si rol de server de actualizare.