Caiet de sarcini

specificaţii tehnice pentru achiziţie publică de echipamente de tehnică de calcul şi produse software

Scopul achiziţiei:

Dotarea cu tehnica de calcul a sistemului informatic al Secretariatului General al Guvernului.

Prezentul caiet de sarcini conţine specificaţii tehnice pentru echipamente de tehnică de calcul şi produse software ce fac obiectul achiziţiei publice, în procedură de licitaţie deschisă, după cum urmează:

LOT 1	
a)Staţie de lucru (PC desktop SFF)	
(unitate centrală, monitor)	*90 buc.*
b) Staţie de lucru mobilă (pc/laptop)	
(pc/laptop)	*30 buc.*
c) Echipament de tip server	
(server aplicatii si virtualizare)	*1 buc.*
d) Echipament de tip server	
(server aplicatii si virtualizare)	*6 buc.*
e) Echipament de tip firewall	
(echipament de tip firewall)	*3 buc*
f) Licenţe pentru soluţie de virtualizare infrastructura servere	
(licenţe pentru soluţie de virtualizare infrastructura servere (licenţa/CPU)	*12 buc*
g) Licenţa pentru soluţia de management al infrastructurii de servere virtualizate	
(licenţa pentru soluţia de management al infrastructurii de servere virtualizate)	*1 buc*
h) Licenţa pentru soluţia de control al accesului administrativ peste platformele Windows, Unix, Linux	
(licenţa pentru soluţia de control al accesului administrativ peste platformele Windows, Unix, Linux)	*2 buc*
i) ***Licente soluţie pentru automatizarea si securizare accesului la reteaua LAN (Ethernet)***	
(licente soluţie pentru automatizarea si securizare acces-ului la reteaua LAN (Ethernet) (licenta/utilizator)	*500 buc*

Specificaţiile pentru echipamentele hardware (inclusiv accesorii şi repere auxiliare) şi licenţele software sunt detaliate in anexă.

Mențiunile explicite (coduri şi specificații de model, cerințe de interoperabilitate) din fișa tehnică anexată, se referă la componente şi repere efectiv oferite, iar cerințele minime de structură, capacitate şi interoperabilitate expres menționate sunt obligatorii.

Pentru toate componentele şi funcționalitățile menționate explicit, ofertantul va prezenta, în mod obligatoriu, informațiile relevante detaliate - inclusiv (dar fără a se limita la) cod / model, fabricant, specificații etc., care să permită identificarea produselor oferite şi confirmarea respectării cerințelor.

În caz de neconcordanță, specificațiile oficiale publicate de producătorul echipamentului (valabile la data ofertei, pentru produsele oferite) vor fi considerate ca referință, iar conținutul acestora primează asupra detaliilor tehnice ale ofertei

Anexele 1-9 fac parte integrantă din prezentul document, prezentul caiet de sarcini este considerat complet numai împreună cu fișele tehnice din anexe, în total 28 /28 pagini.

UNITATE CENTRALĂ (UC / PC– SMALL FORM FACTOR) - 90 buc. / SPECIFICAȚIE TEHNICĂ Unitate centrală, în configurația minimă (ofertele care prezintă specificații tehnice inferioare vor fi respinse) de mai jos:		
PERFORMAȚE:		
SUBSISTEM DE BAZĂ		
ARHITECTURĂ	**[mainboard / chipset]**	
	Cipsetul sa fie compatibil cu procesorul instalat. Chipsetul trebuie sa înglobeze un set de capabilități de management de la distanta	
	[conectivitate locală]	✓ - 6 x USB 2.0 (din care minim 2 x USB 2.0 in partea frontala) ✓ - 4 x USB 3.0 (din care minim 2 x USB 3.0 in partea frontala) ✓ - 2 x Display Port ✓ - 1 x VGA ✓ - 2 x PS/2 (pentru tastatura si mouse) ✓ - 1 x conector RJ45 ✓ - 1 x serial port Audio: ✓ In fata: 1 x Căști/Microfon ✓ In spate: 1 x Audio intrare/Audio Out
PROCESOR	**[instalat / oferit; nu mai puțin de]**	
		✓ Procesor cu 4 nuclee, 8 fire de execuție cu o frecventa minima 3.60 GHz având posibilitate de overclocking pana la minim 4.00 GHz, memorie cache minim 8MB
MEMORIE ACTIVĂ	**[tip memorie activă]**	✓ DDR3 1600 MHz
	[std. instalat/oferit]	✓ min. 8GB
	[suportat de sistem]	✓ [numai puțin de] 32 GB
SUBSISTEM DE STOCAJ		
HDD	**[std. instalat/oferit]**	✓ (min.) 1 x 1000GB, 7200RPM, SATA 6.0 Gb/s
DVD+/-RW	**[std. instalat/oferit]**	✓ 1 x DVD+/-RW

SURSA	**[std. instalat/oferit]**	✓ max. 240 W
FUNCŢIONALITĂŢI:		
SUBSISTEM DE COMUNICAŢII		
LAN INTEGRAT	**[std. instalat/oferit]**	✓ 1 x Interfața LAN Ethernet Gigabit integrata, conector RJ45, capabilități WOL, PXE
CONSOLĂ		
TASTATURĂ ȘI MOUSE	**[std. instalat/oferit]**	✓ tastatură min. 104 key, layout US, conector USB sau PS/2 ✓ mouse optic, conector USB sau PS/2
ADAPTOR VIDEO	**[std. instalat/oferit]**	✓ 1 x Placa video integrata, cu suport pentru minim 2 display-uri externe
SUPORT SUNET		✓ Integrat de tip High Definition; ✓ Speaker intern integrat minim 1.5 watt
SECURITATE		✓ Modul de securitate (tip TPM) integrat pe placa de baza ✓ Posibilitate dezactivare SATA din BIOS ✓ Posibilitate dezactivare/activare din BIOS pentru porturile USB, Serial. ✓ Posibilitate de setare parola pentru BIOS ✓ BIOS de tip UEFI ✓ Management termic si al puterii prin intermediul BIOS
SOFTWARE PREINSTALAT		
SISTEM DE OPERARE		✓ Microsoft Windows 10 Pro sau echivalent
SOFTWARE FURNIZAT		✓ Echipamentul sa fie livrat cu CD/DVD cu driverele pentru toate componentele sistemului. ✓ Client de management compatibil cu soluțiile DELL Kace K1000&K2000 existente si utilizate in infrastructura, - Clientul de management va suporta instalarea pe sistemele livrate. - Clientul de management va putea fi instalat cel puțin pe următoarele sisteme de operare existente in exploatare: Windows, Vista, 7, 8, 8.1, Mac OS X (platforme Intel), Ubuntu Linux in arhitectura 32bit si 64bit - Clientul de management va putea fi instalat in mod centralizat, atât pentru sisteme Windows parte in Active Directory cat si pentru cele membre in workgroup. - Installer-ul de client va permite customizarea in vederea editării tuturor caracteristicilor privind comportamentul la instalare.

	- Prin clientul de management se va asigura inventarierea completa a hardware-ului si software-ului sistemului gazda. - Clientul de management va permite aplicarea de reguli de inventariere personalizate, pe baza de sintaxa PowerShell. - Prin intermediul clientului de management vor putea fi vizualizate, din interfața web a soluției, într-o maniera centralizata, toate informațiile de inventar. - Din interfața web a soluției, prin intermediul clientului de management, vor fi disponibile capabilități de distribuție de pachete software, managementul patch-urilor, managementul activelor, control la distanta, instalări prin rețea, migrarea stării utilizatorilor etc. - Prin intermediul clientului de management, din interfața web a soluției, vor fi disponibile capabilități de raportare istorica a software-ului instalat, inclusiv sistem de operare, aplicații, intrări de registri, fișiere, starea hotfix-urilor si patch-urilor.
ERGONOMIE:	
DESIGN/CONSTRUCTIE	
FORMAT	✓ De tip SFF (Small Form Factor) ✓ Carcasa sa permită accesul la componente tool-less
EXTENSIBILITATE	
SLOTURI EXPANSIUNE	✓ - 1 x PCI Express x16 ✓ - 3 x PCI Express x1
BAY-URI	✓ - 1 x intern de 3.5 inch ✓ - 1 x intern de 2.5 inch ✓ - 1 x extern de 5.25 inch
CERTIFICĂRI	✓ Echipamentul PC de tip Desktop trebuie sa fie listat de Microsoft in Windows 7 sau Windows 8 Hardware Compatibility List, sectiunea Systems/Desktop PCs.
GARANȚIE	✓ (min.) 3 ani. **HDD-urile defecte nu vor fi returnate.**
NOTĂ:	
✓ Nu sunt acceptate adaptoare sau soluții improvizate pentru porturile si interfețele echipamentului. ✓ Produsele oferite vor fi însoțite de toate accesoriile necesare funcționarii lor (modul hardware sau software) la parametrii ceruți prin prezenta specificație tehnica, chiar daca beneficiarul a omis solicitarea lor explicita. ✓ Se solicita a fi atașate documente cu specificațiile tehnice emise de producător pentru produsele ofertate. ✓ Pentru aplicațiile software se va asigura numărul de licențe necesar	

MONITOR (monitor / PC desktop SFF – 90 buc. / SPECIFICAŢIE TEHNICĂ	
Monitoare, având specificaţiile tehnice minime de mai jos (ofertele care prezintă caracteristici/performanţă inferioare vor fi respinse):	
PERFORMAŢE:	
SPECIFICAŢII TEHNICE	
TEHNOLOGIE	LED
DIAGONALA	min. 23 inch
REZOLUȚIE NATIVA	min. 1920x1080
UNGHI DE VIZUALIZARE	pana la 170° orizontal/160° vertical
LUMINOZITATE (CD/MP)	min. 250 cd/mp

CONTRAST DINAMIC	min.1000:1
TIMP DE RĂSPUNS	maxim 5 ms
INTERFAȚĂ	1 x Display Port 1 x VGA
ERGONOMIE / STANDARDIZARE	
FORMAT	✓ 16:9
VERSATILITATE	✓ Posibilitate inclinare - 5° la +22° ✓ Sistem de prindere tip VESA .
STANDARDE	✓ TCO Certified ✓ - Monitorul trebuie sa fie listat de Microsoft in Windows 7 sau Windows 8 Hardware Compatibility List, sectiunea Monitors&Displays/LCD Monitors.
GARANȚIE	✓ (min.) 3 ani

Notă: Nu sunt acceptate adaptoare sau soluții improvizate pentru porturile si interfețele echipamentului.
- Produsele oferite vor fi însoțite de toate accesoriile necesare funcționarii lor (modul hardware sau software) la parametrii ceruți prin prezenta specificație tehnica, chiar daca beneficiarul a omis solicitarea lor explicita.
- Se solicita a fi atașate documente cu specificațiile tehnice emise de producător pentru produsele ofertate.

STAŢIE DE LUCRU MOBILĂ (PC/LAPTOP) – 30 buc./ SPECIFICAŢIE TEHNICĂ Stație de lucru mobilă (PC/laptop) în configurația minimă (ofertele care prezintă specificații tehnice inferioare vor fi respinse) de mai jos:		
PERFORMAŢE:		
1. SUBSISTEM DE BAZĂ		
ARHITECTURĂ	**[mainboard / chipset]**	
	Compatibil cu procesorul instalat; sa dispună de o tehnologie de tip anti-furt ce permite blocarea PC-ului in caz de furt sau pierdere.	
	conectivitate locală	✓ 1 x DisplayPort 1.2 ✓ 1 x VGA ✓ 3 x USB 3.0 ✓ 1 x USB 3.0 cu functie de incarcare ✓ 1 x Iesire combo casti stereo/microfon ✓ 1 x RJ-45 ✓ 1 x Media Card Reader ✓ 1 x Conector pentru statie de andocare ✓ 1 x AC ✓ 1 x Smart Card Reader
PROCESOR	**[instalat / oferit; nu mai puțin de]**	
	Procesor cu 2 nuclee, 4 fire de executie cu o frecventa minima de 2.20 GHz avand posibilitate de overclocking pana la minim 2.70 GHz, cache minim 3MB, litografie 14nm.TDP maxim 16 W.	
MEMORIE ACTIVĂ	**[tip memorie activă]**	✓ DDR3L 1600 MHz SDRAM
	[std. instalat]	✓ 1 X 4 GB 1600 MHz DDR3L
	[suportat de sistem]	✓ [numai puțin de] 16GB 1600 MHz DDR3L
	[implementare/scalabilitate]	✓ configurația oferită va dispune de (min.) 1 slot liber
2. SUBSISTEM DE STOCARE		
HDD	**[std. instalat/oferit]**	✓ (min.) 1 x 500GB 7200 RPM;
FIABILITATE:		
3. DESIGN / CONSTRUCTIE		
CARCASA	✓ de tip „business” rezistenta la socuri si la uzura ✓ -de preferat caracasa subtire si usoara(aliaj magenziu/aluminiu) , palmrest de dimensiuni mari	
GREUTATE	✓ maxim 1,8 Kg	
ROBUSTEŢE	✓ se vor prezenta elementele de design menite să asigure rezistentă și durabilitatea;	
FUNCŢIONALITĂŢI:		

SECURITATE	✓ Chip/modul de securitate integrat pe placa de baza tip TPM/TCPA	
4. SUBSISTEM DE COMUNICAȚII		
INTEGRAT	**[std. instalat/oferit]**	✓ Placa de retea integrata Gigabit(10/100/1000Mbps) ✓ WLAN DualBand 802.11 a/b/g/n 2X2 ✓ Bluetooth 4.0
5. CONSOLĂ		
TASTATURĂ	**[integrată]**	✓ -Rezistenta la varsarile accidentale de lichide avand canale de scurgere dedicate. Cu iluminare de tip backlit.
POINTING DEVICE/TOUCHPAD	**[integrat]**	✓ Touchpad cu zona scroll si doua butoane, ✓ Suport multi-gesture; ✓ Buton pentru On/Off touchpad. ✓ Sa dispună de un dispozitiv de tip pointstick si doua butoane adiționale
6. SUBSISTEM GRAFIC / MULTIMEDIA		
SUPORT SUNET	✓ DTS studio sound ✓ Difuzoare Stereo integrate ✓ Jack combo stereo casti/microfon ✓ Microfoane cu functie de reducere a zgomotului de fundal ✓ Buton de oprire sunet, crestere volum, descrestere volum	
ADAPTOR VIDEO	✓ Placa video integrata, cu memorie partajata	
MONITOR	✓ min. 14 inch diagonala, anti-glare, retroiluminare LED avand o rezolutie minim FHD (1920 x 1080), cu unghi mare de vizualizare.	
CAMERĂ WEB	✓ camera web cu iluminare si rezolutie 720p HD	
7. ALIMENTARE		
BATERIE STANDARD	✓ min. 3 celule	
ALIMENTATOR A/C	inclus standard	
TIMP DE AUTONOMIE	[min] 10 ore autonomie cu bateria standard (încărcată 100%)	
8. SOFTWARE PREINSTALAT		
SISTEM DE OPERARE	✓ Microsoft Windows 10 Pro sau echivalent cu posibilitate de downgrade Windows 7 PRO 64 biti	
SOFTWARE FURNIZAT	✓ Echipamentul sa fie livrat cu CD/DVD cu driverele pentru toate componentele sistemului. ✓ -Client de management compatibil cu soluțiile DELL Kace K1000&K2000 existente si utilizate in infrastructura: ▪ Clientul de management va suporta instalare pe sistemul de operare solicitat. ▪ Clientul de management va putea fi instalat cel puțin pe următoarele sisteme de operare existente in exploatare: Windows 7, 8, 8.1, Mac OS X (platforme Intel)	

	▪ Clientul de management va putea fi instalat in mod centralizat, atât pentru sisteme Windows parte in Active Directory cat si pentru cele membre in workgroup. ▪ Installer-ul de client va permite customizarea in vederea editării tuturor caracteristicilor privind comportamentul la instalare. ▪ Prin clientul de management se va asigura inventarierea completa a hardware-ului si software-ului sistemului gazda. ▪ Clientul de management va permite aplicarea de reguli de inventariere personalizate, pe baza de sintaxa PowerShell. ▪ Prin intermediul clientului de management vor putea fi vizualizate, din interfața web a soluției, într-o maniera centralizata, toate informațiile de inventar. ▪ Din interfața web a soluției, prin intermediul clientului de management, vor fi disponibile capabilități de distribuție de pachete software, managementul patch-urilor, managementul activelor, control la distanta, instalări prin rețea, migrarea stării utilizatorilor etc. ▪ Prin intermediul clientului de management, din interfața web a soluției, vor fi disponibile capabilități de raportare istorica a software-ului instalat, inclusiv sistem de operare, aplicații, intrări de registri, fișiere, starea hotfix-urilor si patch-urilor.
STANDARDE SI CERTIFICĂRI	✓ Echipamentul PC de tip Notebook trebuie sa fie listat de Microsoft pentru sistemele de operare Windows 7 sau Windows 8 in Hardware Compatibility List, secțiunea Notebooks&Tablets.
GARANȚIE	✓ min. 3 ani pentru notebook ✓ min. 3 ani pentru baterie oferita de producator
NOTĂ:	
Nu sunt acceptate adaptoare externe pentru interfetele si porturile echipamentului. -Produsele oferite vor fi insotite de toate accesoriile necesare functionarii lor(modul hardware sau software) la parametrii ceruti prin prezenta specificatie tehnica, chiar daca beneficiarul a omis solicitarea lor explicita -Se solicita a fi atasate documente cu specificatiile tehnice emise de producator pentru produsele ofertate.	

LOT_1: ANEXA_3

ECHIPAMENT DE TIP SERVER– 1 buc. / SPECIFICAŢIE TEHNICĂ Server aplicatii si virtualizare rack-abile, în configuraţia minimă (ofertele care prezintă specificaţii tehnice inferioare vor fi respinse) de mai jos:		
PROCESOR	[	2 x procesoare instalate Intel Xeon E5-2620v3, frecventa de lucru 2,40 GHz, L3 cache 15 MB, sau echivalent.
MEMORIE	[	64 Gb registered ECC DDR4, 2133 MHz, PC4-2133R, DIMM, memorie instalata, cu suport pentru "Memorie in oglinda" (memory mirroring), Advanced ECC; Rank sparing memory, Memory Scrubbing,
HARD DISK DRIVE	[	2 x 300 GB 15.000 rpm, SAS 12Gb/s, hot plug, instalate 4 x 1000 GB 7.200 rpm, SAS, 6 Gb/s, hot plug, instalate, Cu suport pentru minim 24 HDD x 2.5-inch SAS/SATA In cazul in care serverul nu suporta expandabilitatea necesara, sunt acceptate unităţi de expansiune cu diskuri conectate redundant la server
CONTROLLER RAID	[	2 x Controller SAS/SATA 12Gb/s, 1GB cache, 8 porturi, suport pentru RAID 0,1,10,5,50,6,60,
INTERFAŢĂ GRAFICA	[	Integrata,
INTERFAŢĂ REŢEA	[	4 x Ethernet 10/100/1000Mbps 1 x interfaţa de reţea 10/100/1000Mbps pentru remote management
INTERFAŢA FIBRE CHANNEL	[	1 x interfaţă de fibra optica (Host Bus Adapter) cu doua porturi de minim 8 Gbit/s, conector tip LC
SLOT-URI DE EXPANSIUNE	[	min. 6 slot-uri dintre care minim 3 slot-uri PCI-Express Gen3 x16
CONECTORI INTERFEŢE INTRARE/IEŞIRE	[	1 x VGA, 4 x USB 3.0 4 x USB 2.0 1 x uSSD 4 x RJ 45 1 x port dedicat pentru management
CARCASA	[	montabil in rack cu ocupare a maxim 2U spaţiu.
SURSA DE ALIMENTARE	[	doua surse redundante de maxim 800W fiecare, hot plug.
VENTILATOARE	[	ventilatoare redundante, hot plug
SISTEM DE OPERARE	[	Sistem de operare instalat: Windows Server 2012 R2 Standard sau echivalent
MANAGEMENT	[	- aplicaţie pentru instalarea si configurarea serverului dezvoltata de producătorul serverului capabila de instalare locala si remote in mod neasistat, inclusiv configurare RAID - aplicaţie de management operaţional cu următoarele funcţii: monitorizarea stării sistemului, managementul evenimentelor si alarmelor, inventarul componentelor, inventarul si instalarea up-date-urilor si patch-urilor, analiza performantei, diagnoza on-line, restartarea si reconfigurarea automata a serverului, analiza si previzionarea defectării componentelor (PFA) - chipset pentru remote management integrat compatibil IPMI 2.0 cu acces prin web browser cu securizare prin criptare SSL 128 bit, integrat cu aplicaţia de management, redirectarea interfeţei grafice si funcţionalităţi remote media
SOFTWARE FURNIZAT	[	Client de management compatibil cu soluţiile DELL Kace K1000&K2000 existente si utilizate in infrastructura.

		- Clientul de management va suporta instalare pe sistemul de operare ofertat. - In mod concret, clientul de management va putea fi instalat cel puțin pe următoarele sisteme de operare existente in exploatare:Windows Server 2012 R2, Windows Server 2008 R2 - Clientul de management va putea fi instalat in mod centralizat, atât pentru sisteme Windows parte in Active Directory cat si pentru cele membre in workgroup. - Installer-ul de client va permite customizarea in vederea editării tuturor caracteristicilor privind comportamentul la instalare. - Prin clientul de management se va asigura inventarierea completa a hardware-ului si software-ului sistemului gazda. - Clientul de management va permite aplicarea de reguli de inventariere personalizate, pe baza de sintaxa PowerShell. - Prin intermediul clientului de management vor putea fi vizualizate, din interfața web a soluției, într-o maniera centralizata, toate informațiile de inventar. - Din interfața web a soluției, prin intermediul clientului de management, vor fi disponibile capabilități de distribuție de pachete software, managementul patch-urilor, managementul activelor, control la distanta, instalări prin rețea, migrarea stării utilizatorilor etc. - Prin intermediul clientului de management, din interfața web a soluției, vor fi disponibile capabilități de raportare istorica a software-ului instalat, inclusiv sistem de operare, aplicații, intrări de registri, fișiere, starea hotfix-urilor si patch-urilor.
ACCESORII	[	Kit de montare in rack inclus, împreuna cu toate accesoriile necesare montării în rack, se vor furniza toate cablurile necesare conectării
GARANȚIE	[	3 ani la sediul beneficiarului

ECHIPAMENT DE TIP SERVER– 6 buc. / SPECIFICAŢIE TEHNICĂ Server aplicatii si virtualizare rack-abile, în configuraţia minimă (ofertele care prezintă specificaţii tehnice inferioare vor fi respinse) de mai jos		
PROCESOR	**[std. instalat / oferit]**	2 x procesoare instalate Intel Xeon E5-2620v3, frecventa de lucru 2,40 GHz, L3 cache 15 MB, sau echivalent.
MEMORIE	**[std. instalat / oferit]**	64 Gb registered ECC DDR4, 2133 MHz, PC4-2133R, DIMM, memorie instalata, cu suport pentru "Memorie in oglinda" (memory mirroring), Advanced ECC; Rank sparing memory, Memory Scrubbing,
HARD DISK DRIVE	**[std. instalat / oferit]**	2 x 300 GB 15.000 rpm, 3,5 inch, SAS 12Gb/s, hot plug, instalate, Cu suport pentru minim 12 x 3,5 inch SAS/SATA
CONTROLLER RAID	**[std. instalat / oferit]**	1 x Controller SAS/SATA 12Gb/s, 1GB cache, 8 porturi, suport pentru RAID 0,1,10,5,50,6,60,
INTERFAȚĂ GRAFICA	**[std. instalat / oferit]**	Integrata,
INTERFAȚĂ REȚEA	**[std. instalat / oferit]**	4 x Ethernet 10/100/1000Mbps 1 x interfața de rețea 10/100/1000Mbps pentru remote management
INTERFAȚA FIBRE CHANNEL	**[std. instalat / oferit]**	1 x interfață de fibra optica (Host Bus Adapter) cu doua porturi de minim 8 Gbit/s, conector tip LC
SLOT-URI DE EXPANSIUNE	**[std. instalat / oferit]**	min. 6 slot-uri dintre care minim 3 slot-uri PCI-Express Gen3 x16
CONECTORI INTERFEȚE INTRARE/IEȘIRE	**[std. instalat / oferit]**	1 x VGA, 4 x USB 3.0 4 x USB 2.0 1 x uSSD 4 x RJ 45 1 x port dedicat pentru management
CARCASA	**[std. instalat / oferit]**	Montabil in rack cu ocupare a maxim 2U spațiu.
SURSA DE ALIMENTARE	**[std. instalat / oferit]**	Doua surse redundante de maxim 800W fiecare, hot plug.
VENTILATOARE	**[std. instalat / oferit]**	ventilatoare redundante, hot plug
SISTEM DE OPERARE	**[std. instalat / oferit]**	Sistem de operare instalat: Windows Server 2012 R2 Standard sau echivalent
SOFTWARE FURNIZAT	**[std. instalat / oferit]**	Client de management compatibil cu soluțiile DELL Kace K1000&K2000 existente si utilizate in infrastructura. - Clientul de management va suporta instalare pe sistemul de operare ofertat. - In mod concret, clientul de management va putea fi instalat cel puțin pe următoarele sisteme de operare

		existente in exploatare:Windows Server 2012 R2, Windows Server 2008 R2 - Clientul de management va putea fi instalat in mod centralizat, atât pentru sisteme Windows parte in Active Directory cat si pentru cele membre in workgroup. - Installer-ul de client va permite customizarea in vederea editării tuturor caracteristicilor privind comportamentul la instalare. - Prin clientul de management se va asigura inventarierea completa a hardware-ului si software-ului sistemului gazda. - Clientul de management va permite aplicarea de reguli de inventariere personalizate, pe baza de sintaxa PowerShell. - Prin intermediul clientului de management vor putea fi vizualizate, din interfața web a soluției, într-o maniera centralizata, toate informațiile de inventar. - Din interfața web a soluției, prin intermediul clientului de management, vor fi disponibile capabilități de distribuție de pachete software, managementul patch-urilor, managementul activelor, control la distanta, instalări prin rețea, migrarea stării utilizatorilor etc. Prin intermediul clientului de management, din interfața web a soluției, vor fi disponibile capabilități de raportare istorica a software-ului instalat, inclusiv sistem de operare, aplicații, intrări de registri, fișiere, starea hotfix-urilor si patch-urilor..
MANAGEMENT	**[std. instalat / oferit]**	- aplicație pentru instalarea si configurarea serverului dezvoltata de producătorul serverului capabila de instalare locala si remote in mod neasistat, inclusiv configurare RAID - aplicație de management operațional cu următoarele funcții: monitorizarea stării sistemului, managementul evenimentelor si alarmelor, inventarul componentelor, inventarul si instalarea up-date-urilor si patch-urilor, analiza performantei, diagnoza on-line, restartarea si reconfigurarea automata a serverului, analiza si previzionarea defectării componentelor (PFA) - chipset pentru remote management integrat compatibil IPMI 2.0 cu acces prin web browser cu securizare prin criptare SSL 128 bit, integrat cu aplicația de management, redirectarea interfeței grafice si funcționalități remote media

ACCESORII	**[std. instalat / oferit]**	Kit de montare in rack inclus, împreuna cu toate accesoriile necesare montării în rack, se vor furniza toate cablurile necesare conectării
GARANȚIE	**[std. instalat / oferit]**	3 ani la sediul beneficiarului

ECHIPAMENT DE TIP FIREWALL -3 buc. / SPECIFICAŢIE TEHNICĂ Echipamente de tip firewall, în configuraţia minimă (ofertele care prezintă specificaţii tehnice inferioare vor fi respinse) de mai jos		
SPECIFICATII HARDWARE	**[std. instalat / oferit]**	• Interfete GbE RJ-45 pentru WAN: 2 • Interfete GbE RJ-45: 40 • Interfete GbE RJ-45 pentru management: 1 • Interfete GbE SFP: 2 • Porturi consola RJ-45: 1 • Porturi USB: 1 • Storage intern: 64 GB
CARACTERISTICI	**[std. instalat / oferit]**	• Trafic firewall: 4 Gbps • Latenta Firewall: 6 µs • Trafic Firewall masurat in pachete per secunda: 6.000.000 pps • Trafic IPSec VPN: 1,3 Gbps • Trafic IPS: 2,1 Gbps • Trafic antivirus proxy based /flow based: 600 Mbps / 1,1 Gbps • Numar de tunele IPSec VPN site-to-site: 2.000 • Numar de clienti IPSec VPN: 5.000 • Trafic SSL-VPN: 400 Mbps • Numar de clienti concurenti SSL-VPN: 300 • Numar de sesiuni concurente TCP: 3.200.00 • Numar de sesiuni noi pe secunda TCP: 77.000 • Numar de politici de securitate: 10.000 • Numar de token-uri OTP administrate: 500 • Numar de instante virtuale: 10

FUNCTIONALITATI GENERALE	**[std. instalat / oferit]**	• Echipament integrat de securitate cu functionalitati simultane de:
		  • Firewall de tip stateful
		  • Router cu suport pentru protocoale de rutare dinamice
		  • Posibilitate de instalare in mod bridge Ethernet
		  • Criptare de date: IPSec VPN si SSL VPN
		  • Suport pentru QoS si Traffic Shaping
		  • Detectia si prevenirea intruziunilor – IDS/IPS
		  • Scanare si filtrare WEB – Web Inspection/Filter
		  • Blocarea si controlul traficului din retea generat de aplicatii
		  • Protectie Antispam
		  • Protectie impotriva scurgerii de informatii confidentiale
		  • Update-uri automate si in timp real

		• Suport pentru IPv6 UTM • Functionalitate de proxy SSL – posibilitatea inspectiei traficului criptat • Certificari pentru producator si produs: ICSA Labs pentru Firewall, IPSec, SSL VPN, IPS,
FUNCTIONALITATI SECURITATE		
FUNCTIONALITATI FIREWALL	**[std. instalat / oferit]**	• Functionalitati NAT, PAT si Transparent Bridge • Optiune de a aplica NAT per politica • Suport VLAN Tagging 802.1Q • Autentificarea utilizatorilor pe grupuri • Suport VoIP SIP/H.323/SCCP Traversal NAT • Functionalitate proxy explicit • Suport WINS • Suport securitate VoIP ALG (SIP Firewall/RTP Pinholing) • Suport IPv6 (NAT/mod Transparent) • Politici de securitate bazate pe identitatea utilizatorului/servicii folosite/tipul device-ului sau al sistemului de operare de statie folosit – functionalitate de tip BYOD (bring your own device) • Optiune “Scheduling” pentru politicile de firewall • Mecanism de calcul si afisare al reputatiei utilizatorilor din retea pe baza de scor dedus in mod configurabil din activitatea detectata prin mecanismele de inspectie de blocarea a atacurilor, blocare malware, filtrare web, firewall is inspectie a traficului de aplicati.
FUNCTIONALITATI VPN	**[std. instalat / oferit]**	• Suport PPTP, IPSec, L2TP/IPSec, SSL-VPN • Functionalitate concentrator SSL-VPN • Criptare DES, 3DES, AES 128, AES 192, AES 256 • Autentificare MD5, SHA-1, SHA-256, SHA-384, SHA-512 • Suport pentru PPTP si L2TP VPN Client Pass Through • Functionalitate “Hub and Spoke” IPSec VPN • Autentificare IKE prin certificate X.509 • Suport IPSec Xauth NAT Traversal • Suport configurare IPSec automata • Functionalitate IKE Dead Peer Detection • Suport pentru RSA SecureID • Suport Single-Sign-On pentru pentru book-mark-uri portal SSL-VPN • Functionalitate Two-Factor Authentication pentru SSL-VPN • Suport pentru autentificare de grupuri de utilizatori prin LDAP (SSL-VPN) • Suport tunele SSL in mod tunel si in mod portal • Functionalitati monitorizare tunele VPN • Producatorul are in portofoliu client de VPN IPSec si SSL propriu, care are si functionalitati de: filtrare web si optimizare de banda, filtrare a traficului de aplicatii, scanare de vulnerabilitati
FUNCTIONALITATI FILTRARE TRAFIC WEB	**[std. instalat**	• Filtrare pentru protocoalele HTTP si HTTPS • Filtrare dupa categorii site-uri/URL-uri • Functionalitate de contorizare a timpului de acces sau a volumului de trafic pentru utilizatori – definire de cote de utilizare • Blocare a conexiunilor in functie de URL/cuvant cheie sau expresie in continutul paginilor web • Filtrare pentru Java Applet, Cookies, scripturi Active X

	/ oferit]	
FUNCTIONALITATI SISTEM DE CONTROL AL APLICATIILOR	**[std. instalat / oferit]**	• Identificarea si controlul aplicatiilor • Optiune de Traffic-Shaping per aplicatie • Control specific pentru aplicatiile de tip IM/P2P • Clasificare granulara a aplicatiilor dupa criterii multiple precum: Categorii de aplicatii, Popularitate, Tehnologie si Risc • Monitorizare aplicatiilor cu rata cea mai mare de consum de banda • Monitorizarea aplicatiilor pe baza IP/Utilizator
FUNCTIONALITATI SISTEM DE PREVENIRE A INTRUZIUNILOR/ATACURILOR (IPS)	**[std. instalat / oferit]**	• Protectie si semnaturi de atac • Detectarea anomaliilor de protocol • Suport pentru semnaturi configurabile • Update-uri automate pentru semnaturi • Suport pentru IPv4 si IPv6 DDoS
FUNCTIONALITATI ANTISPAM	**[std. instalat / oferit]**	• Scanare pentru SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI • Suport RBL/ORDBL • Inspectie header MIME • Filtrare dupa cuvinte cheie/expresie • Filtrare dupa Black/White List pentru adrese IP si e-mail • Update-uri automate si in timp real
FUNCTIONALITATE DATA LEAK PREVENTION	**[std. in**	• In caz de scurgere de informatii trebuie sa permita blocarea si arhivarea conversatiei pe protocoale de email, HTTP, FTP si variantele criptate SSL; arhivarea imaginilor si a fisierelor atasate la email, transferate prin aplicatii de tip Instant Messaging , incarcate – descarcate pe un site web

	[std. instalat / oferit]	• Suport pentru document fingerprinting si documente cu watermark • Blocare dupa tip si dimensiune fisier
FUNCTIONALITATI OPTIMIZARE DE BANDA	**[std. instalat / oferit]**	• Optimizare de protocol (CIFS/FTP/MAPI/HTTP/HTTPS/TCP) • Compresie/decompresie in timp real a traficului (byte caching) • Caching prin proxy web transparent si explicit
FUNCTIONALITATI RETEA		
FUNCTIONALITATI RETELISTICA SI RUTARE	**[std. instalat / oferit]**	• Suport pentru legaturi WAN multiple • Suport PPPoE si DHCP Client/Server • Rute statice • Rutare dinamica IPv4: RIP, OSPF, BGP, Multicast (PIM–DM, PIM–SM, IGMP v1 v2 v3), IS-IS • Rutare dinamica IPv6: RIPng, OSPF v3, BGP 4+ • Gruparea interfetelor in zone de securitate • Rutare intre zonele de securitate • Policy-based routing • Suport VRRP si Link Failure Control • Suport sFlow si NetFlow • Suport VLAN Tagging (802.1q) • Rutare intre VLAN-uri • Suport pentru IPv6 (Firewall, DNS, SIP) • Posibilitate mapare (Binding) adrese IP – adrese MAC • Suport One-to-One NAT • Tunelare IP in IP (IETF RFC 2003) • Suport pentru mecanismul GTSM(IETF RFC 3682) • Suport NAT64, DNS64, NAT46, NAT66
FUNCTIONALITATI TRAFFIC SHAPING	**[std.**	• Limitare/garantare/prioritizare a benzii de trafic prin politici • Traffic Shaping per aplicatie si adresa IP • Suport pentru Differentiated Services (DiffServ)

	[instalat / oferit]	• Limitare a cotei de trafic (per adresa IP)
SUPORT INSTANTE VIRTUALE	**[std. instalat / oferit]**	• Firewall/rutare per instanta virtuala • Administrare separata per instanta virtuala • Interfete VLAN separate per instanta virtuala • Politici de securitate per instanta virtuala
SUPORT PENTRU CENTRE DE DATE – DATA CENTER	**[std. instalat / oferit]**	• Balansare de trafic pentru servere pe protocoalele HTTP, HTTPS, SMTPS, IMAPS, POP3S, TCP, UDP, IP • Balansare de trafic prin metode de tip: source IP hash, round-robin, weighted, first alive, least RTT, least session, HTTP host (din header-ul HTTP) • Persistenta sesiunilor prin metode de tip: HTTP cookie, SSL session ID • Health monitoring pentru servere fizice • Multiplexare TCP pentru sesiunile balansate • Offloading pentru SSL (preia operatiunile de criptare/decriptare de la server-ul intern pentru HTTPS si executa aceste operatii direct pe echipament) • Suport WCCP • Suport ICAP
FUNCTIONALITATI HIGH AVAILABILITY - HA	**[std. instalat / oferit]**	• Functionare Active-Active, Active-Passive • Functionalitate Stateful Failover (Firewall si VPN) • Detectare si notificare pentru echipament nefunctional • Monitorizarea conexiunii la retea • Functionalitate Link Failover

FUNCTIONALITATI DE ADMINISTRARE, LOGARE, AUTENTIFICARE A UTILIZATORILOR		
FUNCTIONALITATI DE ADMINISTRARE	**[std. installat / oferit]**	• Administrare prin WEB UI, Secure Command Shell (SSH) si Command Line Interface (CLI) • Utilizatori/Administratori cu drepturi configurabile • Functionalitate de export/import a configuratiei • Politica de control a parolelor
FUNCTIONALITATI DE LOGARE SI MONITORIZARE	**[std. installat / oferit]**	• Monitorizare grafica in timp real si istorica • Optiune de pastrare a log-urilor pe memoria interna • Suport syslog • Suport SNMP • Notificare prin e-mail pentru alerte • Monitorizarea tunelelor VPNs
FUNCTIONALITATI DE AUTENTIFICARE A UTILIZATORILOR	**[std. installat / oferit]**	• Definire locala a utilizatorilor • Integrare cu Windows Active Directory (AD) pentru Single Sign On • Integrare cu RADIUS/LDAP/TACACS+ • Suport Xauth pentru IPSec VPN • Suport pentru autentificarea grupurilor de utilizatori prin LDAP • Suport pentru autentificare prin doi factori folosind OTP generate de token-uri fizice sau software ce pot fi trimise utilizatorilor prin Email sau SMS • Suport pentru autentificare prin certificate digitale PKI X.509
CONDITII DE ALIMENTARE		• Alimentare curent alternativ 100-240V, 50-60 Hz

GARANTIE SI SUPORT	**[std. installat**	• Solutia va beneficia de minim un an de suport ce va include:
		  • Inlocuirea echipamentului in caz de defectiune hardware
		  • Suport tehnic din partea vendorului minim 5 zile pe saptamana, 8 ore pe zi
		  • Update firmware versiuni minore si majore
		  • Update-uri automate de semnaturi de securitate pentru indeplinirea functionalitatilor, Web Filtering, Antispam, IPS si Application Control

	/ofe rit]	

LICENȚE PENTRU SOLUȚIE DE VIRTUALIZARE INFRASTRUCTURA SERVERE *(licența/CPU)*-12 buc. / SPECIFICAŢIE TEHNICĂ *(licențe pentru soluție de virtualizare infrastructura servere (licența/CPU)* în configuraţia minimă (ofertele care prezintă specificaţii tehnice inferioare vor fi respinse) de mai jos:	
CERINȚE	• Să nu depindă de un sistem de operare gazdă a cărui actualizare să afecteze disponibilitatea și funcționalitatea serverelor, respectiv a mașinilor virtuale care rulează pe serverele respective; • Amprenta pe disc a hypervisor-ului să fie cat mai mică (sub 300MB) astfel încât instalarea hypervisor-uIui sa fie făcută foarte rapid (direct pe server) chiar si din rețea, oferind totodată posibilitatea de boot-are de pe stick USB; • Suport pentru USB 3.0 (client attached to Linux VMs) si rularea de aplicații grafice (DirectX 9 sau OpenGL2.1) pe mașinile virtuale; • Suport pentru accelerare video hardware pentru mașinile virtuale cu sisteme de operare Linux sau Windows; • Performanta nativa pentru accelerare grafica 2D/3D prin utilizarea plăcilor grafice NVIDIA GRID; • Sa permită conectarea peste rețea printr-un concentrator de porturi seriale la consola seriala a oricărei mașini virtuale (ex. Linux); • Sa ofere o securitate crescuta prin încărcarea proceselor importante la nivel de hypervisor in zonele de memorie resiliente, prin utilizarea ultimelor funcționalități disponibile in noile versiuni de procesoare; • Sa ofere posibilitatea creării unor profele pentru host-uri (servere fizice) astfel încât instalarea pe mai multe host-uri sa se facă foarte rapid, respectând o configurație prestabilita si eliminând erorile de configurare si oferind totodată posibilitatea modificării parametrilor configurației; • Sa ofere o scalabilitate crescuta prin configurarea in clustere de înaltă disponibilitate cu pana la 64 de host-uri; • Sa dispună de capacitați de failover astfel încât, in cazul defectării unui host, mașinile virtuale care rulau pe acel host sa fie retratate automat pe celelalte host-uri din cluster; • Sa dispună de capacitați de failover astfel încât, in cazul blocării sistemului de operare instalat într-o mașina virtuala, respectiva mașina virtuala sa fie retratată automat pe același host pentru deblocarea sistemului de operare, a serviciilor si aplicațiilor; • Sa dispună de capacitate de failover care sa detecteze problemele de acces la datastore la nivel de host si sa restarteze automat mașinile virtuale afectate pe un alt host din cluster; • Sa ofere posibilitatea de integrare cu soluții 3rd party care sa asigure funcții de failover la nivel de aplicații, astfel încât, in cazul defectării aplicațiilor instalate in interiorul unei mașini virtuale (ex. SQL server, IIS, TC server, aplicații critice SAP HANA) respectivele aplicații sa fie restartate in mod automat pe baza unor politici predefinite, fie local, fie pe un alt host din cluster; • Sa permită identificarea si evitarea situațiilor de split-brain prin monitorizarea stării host-urilor atât la nivelul rețelei de management cat si la nivelul storage-ului comun; • Sa ofere posibilitatea asigurări unei disponibilități continue, fără pierdere de date, pentru mașinile virtuale

	configurare cu 2/4 virtual CPU-uri si maximum 64GB RAM, in cazul defectării fizice a host-urilor pe care rulează; • Sa permită replicarea mașinilor virtuale la nivel de host, independent de tipul stocării folosite la sursa si destinație, asigurând un RPO (recovery point objective) de minimum 15 minute; • Sa permită stabilirea unei politici de retentive a replicărilor cu peste 20 de replici in timp (ex. 4 replici pe zi, timp de 6 zile), care vor permite refacerea sistemului replicat prin procedura de snapshot recovery, soluție utila pentru refacerea in cazul coruperii datelor sau virusării; • Sa ofere posibilitatea mutării simultane a mașinilor virtuale (minim 4, pe legături Gigabit/10 Gigabit) in funcționare de pe un host pe altul/altele fără afectarea funcționarii acestora pentru a se putea executa activități de mentenanța pe host-ul respective; • Sa permită mutarea mașinilor virtuale peste rețele IP cu latente ridicate, de pana la (10ms - ex. rețele metropolitane) (100ms – ex. rețele naționale sau continentale) dând astfel posibilitatea migrării mașinilor intre centre de date distante; • Sa ofere posibilitatea executării operațiunilor de mentenanța sau upgrade la storage fără afectarea funcționarii mașinilor virtuale; • Sa permită identificarea automata a celei mai bune modalități de stocare a unei mașini virtuale, in funcție de nivelul de servicii asociat acesteia si sa ofere informații in timp real privind conformitatea cu nivelul de servicii asociat; • Sa permită gruparea mai multor volume de stocare cu performante similar in clustere pentru simplificarea managementului si plasarea inteligenta, respective balansarea încărcării (spațiu sau timp de acces) mașinilor virtuale in mod automat la nivel de cluster; • Sa ofere balansarea automata a încărcării pe host-uriIe din cluster prin mutarea mașinilor virtuale in vedere asigurării resurselor optime pentru funcționare; • Sa asigure rate mari de consolidare a mașinilor virtuale pe host-uri prin mecanisme de optimizare si supra alocare a memoriei (ex “Memory BalIooning”, ”Transparent Page Sharing”, “Memory Compression”, “Swap to disk”) pentru reducerea costurilor asociate infrastructurii fizice (ex. număr host-uri, număr porturi de rețea/switch-uri); • Sa ofere mecanisme automate de economisire a energiei electrice prin concentrarea masiva a mașinilor virtuale pe câteva host-uri si oprirea host-urilor nefolosite in momentul in care încărcarea mașinilor virtuale scade. In mod similar, atunci când încărcarea mașinilor virtuale creste hosturile nefuncționare vor fi pornite in vederea asigurării resurselor de calcul corespunzătoare prin balansarea automata a încărcării pe fiecare host din cIuster; • Sa poată rula pe host-uri echipate cu pana Ia 480 de CPU-uri logice si 12TB memorie RAM; • Sisteme de operare suportate pe mașinile virtuale: Windows (2012 R2, 2008 R2, 2003 R2, 8.1, 7), RedHat, SuSE, Ubuntu, FreeBSD, CentOS, Solaris, Oracle Linux, Mac OS X Server; • Aplicație de virtualizare sa permită configurarea si rularea unor mașini virtuale cu pana la 128 procesoare virtuale si 4 TB RAM; • Sa suporte diverse tipuri de storage (SAN, NAS, iSCSI) si protocoale de acces (FC, FCOE, ISCSI, NFS) si sa permită

	prioritizarea si garantarea performantelor I/O (SLA) ale maşinilor virtuale, la nivel de cluster; • Sa permită utilizarea disk-urilor SSD sau Flash instalate pe server pentru configurarea ca read cache la nivel de maşina virtuala sau de disk, oferind performate deosebite pentru aplicațiile Tier 1; • Suport larg din partea ISV (Independent Software Vendors) terți pentru aplicațiile Tier 1 si nu numai – ex. Microsoft – SQL, Exchange, SharePoint, Oracle – RAC, SAP – HANA; • Posibilitatea utilizării unui echipament de stocare extern pentru mai multe host-uri; storage-ul trebuie sa poată stoca atât maşina virtuala cat si hard disk-urile virtuale asociate acesteia; • Sa permită o integrare noua si un cadru de management automatizat, bazat pe politici, pentru sistemele externe de stocare (SAN sau NAS) care sa ofere un model operațional optimizat pentru mediul de lucru virtual, centrat pe nevoile aplicațiilor si nu pe infrastructura; • Accesul către sistemul de stocare extern sa poată fi făcut pe mai multe căi (muItipathing), asigurându-se suport pentru failover si load balancing, oferind si posibilitatea de alegere a politicii de stabilire a căii de acces (ex. fixă, MRU, Round Robin); • Sistemul de fișiere va permite accesul concurent a mai multor servere fizice (host) și a mai multor maşini virtuale la aceeași resursă de stocare; • Sistemul de fișiere trebuie să asigure că o maşină virtuală este accesată doar de pe un singur host (sistem de blocarea accesului); în caz de defectare a host-ului maşina virtuală trebuie să poată fi restartata de pe alt server fizic; • Sistemul de fișiere va asigura posibilitatea migrării în timp real (fără întreruperea funcționării) unei maşini virtuale de pe un host pe altul, de pe o capacitate de stocare pe alta; • Sistemul de fișiere trebuie să suporte expansiunea dinamică a volumelor și LUN-urilor la capacitate mai mari de 2TB; • Să ofere switch virtual distribuit care să permită configurarea centralizată a rețelei, eliminând greșelile de configurare, și să ofere interfețe de programare pentru aplicați (API) pentru switch-uri virtuale distribuite 3rd party; • Aplicația si sistemul de fișiere asociat trebuie sa poată permită adăugarea de procesoare virtuale, memorie RAM, interfețe de rețea si disk-uri Ia maşinile virtuale fără a necesita oprirea acestora (dependenta de guest OS); • Aplicația de virtualizare trebuie sa permită crearea de grupuri de maşini virtuale care să împartă aceleași resurse puse Ia dispoziție in comun (memorie și timpi de procesor); • Software-ul instalat pe host trebuie să poată crea echipamente de rețea virtuale (switch-uri) Ia care să se conecteze maşiniIe virtuale și interfețele de rețea fizice de pe host; • Sa permită prezentarea unui adaptor de rețea PCIe (PCI Express) ca mai multe adaptoare logice direct către maşinile virtuale, reducând astfel latenta rețelei respectivelor maşini virtuale (I/O offload) si oferind performante ridicate; • Aplicația trebuie sa ofere suport pentru aplicarea centralizata a actualizărilor (patch-urilor) pentru host-uri, maşini virtuale sau appliance-uri virtuale; • Aplicația de virtualizare trebuie sa permită managementul salvărilor contextuale (snap-shot) ale maşinilor virtuale fără afectarea stării de funcționare, astfel încât o maşină virtuală se va putea restaura din orice salvare anterioară;

	• Interfața unica de management bazata pe interfață web, accesibila de pe browser-e Firefox (Windows, Mac OSX), Google Chrome (Windows, Mac OSX) si IE (Windows) pentru simplificarea managementului; • Soluția de management centralizat sa fie disponibila atât pentru sisteme de operare Windows cat si Linux, eventual ca appliance virtual pentru simplificarea instalării si administrării precum si reducerea costurilor asociate (ex. licența Windows, licența baza de date SQL sau Oracle) ; • Soluție de înaltă eficienta pentru salvarea copiilor de siguranța pe disc si restaurarea acestora, folosind mecanisme avansate de deduplicare cu lungime variabila si deduplicare globala la nivelul tuturor mașinilor virtuale pentru reducerea costurilor asociate mediilor de stocare pe disc, Change Block Tracking atât pentru salvarea cat si pentru restaurarea datelor pentru minimizarea intervalelor de timp alocate operațiilor de salvare si restaurare; • Sa ofere interfețe de programare pentru aplicații (API) care sa permită producătorilor 3rd party de aplicații de securitate sa ofere integrarea si optimizarea aplicațiilor lor cu mediul virtual pentru performante ridicate (exemplu scanare anti-virus sau anti-malware)
Garanție/suport	• Suport pentru minimum 1 an

LICENŢĂ SOLUȚIE DE MANAGEMENT AL INFRASTRUCTURII DE SERVERE VIRTUALIZATE -1 buc. / SPECIFICAŢIE TEHNICĂ licența pentru soluția de management al infrastructurii de servere virtualizate în configuraţia minimă (ofertele care prezintă specificaţii tehnice inferioare vor fi respinse) de mai jos	
CERINȚE	Soluția de management al infrastructurii de servere virtualizate de tip centralizat pentru gestionarea infrastructurii de servere virtualizate, trebuie sa ofere administratorilor IT control simplu și automat peste mediul virtual cu următoarele cerințe: • Utilizarea unui client Web pentru gestionarea funcțiilor esențiale (modificare configurație la nivel de gazda sau mașina virtuala, pornire/oprire mașina virtuala, clonare, snapshot, backup) din orice browser si de oriunde din lume; • Sa ofere posibilitatea de management multi-hypervisor prin care sa permită managementul integrat si simplificat pentru gazdele VMware vSphere si Microsoft Hyper-V; • Sa ofere simplificarea administrării prin autentificare o singura data (single sign on), permițând utilizatorilor să se autentifice o singura data, si apoi sa se poată conecta la toate soluțiile suportate si integrate cu interfață de management; • Sa ofere informații privind întregul inventar al mediului virtual administrat, incluzând mașini virtuale, gazde, medii de stocare și rețele de date, capacitatea fiind de 1.000 de gazde si 10.000 mașini virtuale pornite in modul stand-alone; • Sa suporte entități noi, valori și evenimente, cum ar fi alarme specifice mașinii virtuale sau mediului de stocare. Aceste alarme pot declanșa noi fluxuri de lucru automatizate pentru a remedia și anticipa eventualele problemele; • Trebuie sa permită standardizarea și simplificarea configurării și gestionarii configurațiilor serverelor gazdă, permițând capturarea configurației unei gazde cunoscute, incluzând specificațiile de rețea, de stocare și setările de securitate și utilizarea acestei configurații la mai multe gazde, simplificând configurarea. Politicile de profil pot fi monitorizate cu privire la respectarea lor. • Trebuie sa permită alocarea resurselor de procesor și de memorie pentru mașinile virtuale care rulează pe aceeași servere fizice, putând defini minime, maxime sau resurse proporționale privind configurarea CPU, a memoriei, a discului și a lățimii de bandă de rețea pentru respectivele mașini virtuale. • Trebuia sa permită modificarea alocărilor în timpul execuției respectivelor mașinile virtuale si totodată permite aplicațiilor sa dobândească în mod dinamic mai multe resurse la acomodarea performanțelor de vârf; • Trebuie sa permită alocarea dinamica a resurselor monitorizând continuu utilizarea bazinelor de resurse și alocând inteligent resursele disponibile între mașinile virtuale potrivit regulilor predefinite care reflectă nevoile și schimbarea priorităților. Rezultatul este o auto-gestionare extrem de optimizata a resurselor și un mediu IT eficient cu balansarea încărcării inclusa; • Trebuie sa permită repornirea automata a mașinilor virtuale care au eșuat, fără intervenție manuală; • Trebuie sa sigure păstrarea modificărilor semnificative ale configurației si permite generarea de rapoarte pentru urmărirea evenimentelor; • Trebuie sa asigure simplificarea managementului prin automatizarea sarcinilor folosind fluxuri predefinite (out-of-the-box fluxuri) sau prin asamblarea ori combinarea fluxurilor predefinite folosind o interfață simpla tip drag-and-drop; • Trebuie sa permită evaluarea performanței și sănătății infrastructurii hypervisor-ului oferind vizibilitate operațională si inteligenta extinsa;

	• Soluția de management trebuie sa ofere arhitectură scalabilă și vizibilitatea în mai multe instanțe de management, cu replicarea rolurilor, a permisiunilor și a licențelor peste infrastructura. Astfel administratorul se va putea conecta, va dispune de o imagine extinsa si va putea realiza căutări la nivel de inventar peste toate instanțele de management simultan; • Soluția va trebui sa asigure integrarea cu partenerii din ecosistem prin API-uri pentru extinderea capacităților infrastructurii virtuale.
GARANȚIE/SUPORT	• Suport pentru minim 1 an

LICENȚA PENTRU SOLUȚIA DE CONTROL AL ACCESULUI ADMINISTRATIV PESTE PLATFORMELE WINDOWS, UNIX, LINUX- 2 buc. / SPECIFICAȚIE TEHNICĂ licența pentru soluția de control al accesului administrativ peste platformele Windows, Unix, Linux în configuraţia minimă (ofertele care prezintă specificaţii tehnice inferioare vor fi respinse) de mai jos	
CERINȚE GENERALE	Accesul administrativ peste platformele non-Windows din infrastructura trebuie aliniat la standardul de securitate impus prin serviciul de director asupra serverelor si aplicațiilor Unix si Linux. Se dorește implementarea unei o soluții care sa permită, pe de o parte, extinderea capabilităților de omogenizare a securității si autentificare centralizata către zona non-Windows, iar pe de alta parte, sa granularizeze potențialul de acces la nivel de root, pe aceste sisteme. Soluția trebuie sa aducă următoarele beneficii administrative, operaționale si de securitate ale instituției, respectiv sa: • Sa elimine necesitatea administrării punctuale a accesului pe fiecare server • Sa consolideze la nivelul serviciului de director, gestionarea utilizatorilor cu diverse roluri administrative sau operaționale pe serverele non-Windows, impunând regula de acces a "celui mai mic privilegiu" • Sa ofere flexibilitate in delegarea Unix, prin adăugarea de management si raportare centralizate la sudo, înlocuirea sudo cu capabilități de delegare avansata, sau o combinație a celor doua într-o singura consola • Sa simplifice aderarea la cerințe de audit si conformitate prin asigurarea unui pachet consistent de rapoarte relative la controlul accesului si activitatea utilizatorilor, peste întregul mediu non-Windows • Sa îmbunătățească eficienta prin management centralizat al politicilor peste orice număr de servere non-Windows • Sa implementeze un nivel securizat de autentificare multi-factor la nivel de serviciu de director Soluția trebuie sa ofere următoarele funcționalități minimale si obligatorii: • Sa extindă autentificarea unificata si autorizarea serviciului de director către sistemele Unix, Linux si Mac OS • Sa elimine autentificarea si autorizarea native Unix si sa implementeze o singura identitate si un singur punct de management disponibile la nivelul serviciului de director • Sa centralizeze managementul tuturor serverelor din cadrul instituției, indiferent de sistemul de operare, astfel încât acestea sa fie membri deplini in structura serviciului de director • Sa permită sistemelor non-Windows sa utilizeze tehnologia de autentificare securizata Kerberos • Sa livreze o tehnologie de îmbunătățire sudo, prin adăugarea unui server central de politici, management centralizat si raportare centralizata asupra drepturilor de acces si al activităților • Sa permită ca alternativa, înlocuirea completa a sudo prin delegarea privilegiilor si granularizarea permisiunilor administrative • Sa asigure înregistrarea tastării pentru activitățile derulate prin sudo, sau pentru toate activitățile derulate la nivel de delegare, din momentul autentificării pe sisteme • Sa permită restricționarea shell-urilor si a execuției de comenzi la distanta • Sa blocheze intruziunile care folosesc mecanisme de acces elevat nedetectabil la nivel de comanda
CERINȚE MINIME FUNCȚIONALE PENTRU TEHNOLOGIA DE AUTENTIFICARE SI	Soluția trebuie sa realizeze acces, autentificare si autorizare centralizate la nivelul serviciului de director pentru toate sistemele de operare tip server. Astfel, resursele non-Windows vor fi reprezentate ca membri deplini ai serviciului de director, la fel ca si

AUTORIZARE UNIFICATA	sistemele Windows. Soluția trebuie sa ofere următoarele funcționalități minimale si obligatorii: • Sa includă mecanisme destinate configurării si licențierii aplicației • Sa includă o gama larga de opțiuni pentru migrare si implementare • Sa includă unelte de migrare NIS • Sa includă unelte de management la nivel de Group Policy atât pentru utilizatorii cat si grupurile locale Unix • Sa extindă autentificarea securizata Kerberos la nivelul sistemelor non-Windows • Sa asigure autentificare centralizata si single sign-on pentru sistemele non-Windows, prin intermediul contului utilizator de serviciu de director • Sa extindă metodele de autentificare complexa Windows (smart card, PKI, OTP) către sistemele non-Windows • Sa suporte forest-uri si domenii multiple • Sa suporte orice versiune de Windows Server la orice nivel funcțional de forest • Sa suporte trust-uri two-way, one-way sau no-way • Sa suporte opțiuni de migrare bazate pe schema, la fel ca si opțiuni de migrare care nu sunt bazate pe schema • Mecanisme de securitate multi-factor: soluția trebuie să integreze funcționalități de autentificare multi-factor, care să se mapeze direct pe serviciul de director și să poată fi gestionate direct in cadrul acestuia. Pentru autentificarea multi-factor, soluția trebuie sa ofere următoarele funcționalități minimale si obligatorii: • Identitățile, rolurile si regulile vor fi stocate si obținute direct din soluția de management al accesului sau din Active Directory • Întregul management va fi realizat din consola Active Directory Users and Computers sau din consola de administrare a solutiei • Utilizarea protocolului standard de industrie RADIUS – va include un proxy RADIUS complet • Disponibilitate completa – va livra servicii multiple pentru toleranta la indisponibilitate • Vor fi furnizate mecanisme de auto-înregistrare a utilizatorilor • Suport pentru o mare plaja de vendori de token-uri, hardware si/sau software; suport pentru orice token hardware conform OATH • Suport pentru iPhone, Android, BlackBerry, Windows, SMS si alte tehnologii suport de autentificare multi-factor • Control deplin al mediului de autentificare • Va exista o singura soluție de autentificare multi-factor pentru întregul mediu (Windows, Linux, Unix, aplicații, VPN, webmail etc.) • Fiecare utilizator va putea folosi mai multe token-uri pentru fiecare echipament, iar un token va putea fi alocat mai multor utilizatori Soluția va furniza funcționalități de securitate îmbunătățita prin: • Autentificare multi-factor complexa

	• Acces securizat webmail • Criptarea datelor la nivelul serviciului de autentificare multifactor • Asigurarea suportului de politici de securitate personalizabile • Activarea autentificării desktop prin token • Securizarea accesului VPN Componenta de autentificare multi-factor va livra un portal web-based in care se regăsesc facilitați complete de administrare: • Cadran de bord pentru vizualizarea rapida a principalelor metrici • Configurator de sistem • Înregistrarea si vizualizarea tuturor operațiunilor • Sistem de deployment pentru token-uri • Modul help desk • Management integrat • Rapoarte de stare
CERINȚE DE UZABILITATE SI INTERFAȚARE CU ADMINISTRATORII SI OPERATORII DE APLICAȚIE	• Toate operațiunile efectuate pentru administrarea sau operarea in aplicație vor fi efectuate dintr-o consola administrativa unica • Consola va procesa automat autentificarea in aplicație, in baza credentialelor de utilizator autentificat Windows • Consola va asigura un mediu grafic, vizual de administrare si operare • Consola va permite efectuarea de operațiuni in Active Directory pe baza apartenentei administratorilor la grupul de securitate Domain Admins ori in baza delegărilor de permisiuni efectuate de un administrator de domeniu. Toate funcționalitățile de administrare si operare prevăzute mai sus vor fi asigurate prin operare in consola de management, vor fi afișate in mod grafic, distinct pe categorii de acțiuni; interfața trebuie sa fie una deosebit de intuitiva si cu un nivel mare de uzabilitate
GARANȚIE/SUPORT	Suport pentru minimum 1 an

LOT_1: ANEXA_9

LICENTE SOLUŢIE PENTRU AUTOMATIZAREA SI SECURIZARE ACCESULUI LA RETEAUA LAN (ETHERNET)) (licenta/utilizator) **- 500 buc. / SPECIFICAŢIE TEHNICĂ:** licente soluţie pentru automatizarea si securizare acces-ului la reteaua LAN (Ethernet) (licenta/utilizator) în configuraţia minimă (ofertele care prezintă specificaţii tehnice inferioare vor fi respinse) de mai jos	
CERINȚE GENERALE	Accesul administrativ peste platformele non-Windows din infrastructura, trebuie aliniat la standardul de securitate impus prin serviciul de director asupra serverelor si aplicațiilor Unix si Linux. Astfel, se dorește implementarea unei o soluții care sa permită, pe de o parte, extinderea capabilităților de omogenizare a securității si autentificare centralizata către zona non-Windows, iar pe de alta parte, sa granularizeze potențialul de acces la nivel de root, pe aceste sisteme. Soluția trebuie sa aducă următoarele beneficii administrative, operaționale si de securitate ale instituției, respectiv sa: • Sa elimine necesitatea administrării punctuale a accesului pe fiecare server • Sa consolideze la nivelul serviciului de director, gestionarea utilizatorilor cu diverse roluri administrative sau operaționale pe serverele non-Windows, impunând regula de acces a "celui mai mic privilegiu" • Sa ofere flexibilitate in delegarea Unix, prin adăugarea de management si raportare centralizate la sudo, înlocuirea sudo cu capabilități de delegare avansata, sau o combinație a celor doua într-o singura consola • Sa simplifice aderarea la cerințe de audit si conformitate prin asigurarea unui pachet consistent de rapoarte relative la controlul accesului si activitatea utilizatorilor, peste întregul mediu non-Windows • Sa îmbunătățească eficienta prin management centralizat al politicilor peste orice număr de servere non-Windows • Sa implementeze un nivel securizat de autentificare multi-factor la nivel de serviciu de director Soluția trebuie sa ofere următoarele funcționalități minimale si obligatorii: • Sa extindă autentificarea unificata si autorizarea serviciului de director către sistemele Unix, Linux si Mac OS • Sa elimine autentificarea si autorizarea native Unix si sa implementeze o singura identitate si un singur punct de management disponibile la nivelul serviciului de director • Sa centralizeze managementul tuturor serverelor din cadrul instituției, indiferent de sistemul de operare, astfel încât acestea sa fie membri deplini in structura serviciului de director • Sa permită sistemelor non-Windows sa utilizeze tehnologia de autentificare securizata Kerberos • Sa livreze o tehnologie de îmbunătățire sudo, prin adăugarea unui server central de politici, management centralizat si raportare centralizata asupra drepturilor de acces si al activităților • Sa permită ca alternativa, înlocuirea completa a sudo prin delegarea privilegiilor si granularizarea permisiunilor administrative • Sa asigure înregistrarea tastării pentru activitățile derulate prin sudo, sau pentru toate activitățile derulate la nivel de delegare, din momentul autentificării pe sisteme • Sa permită restricționarea shell-urilor si a execuției de comenzi la distanta • Sa blocheze intruziunile care folosesc mecanisme de acces elevat nedetectabil la nivel de comanda •
CERINȚE FUNCȚIONALE PENTRU TEHNOLOGIA	Soluția trebuie sa realizeze acces, autentificare si autorizare centralizate la nivelul serviciului de director pentru toate sistemele

DE AUTENTIFICARE SI AUTORIZARE UNIFICATA	de operare tip server. Astfel, resursele non-Windows vor fi reprezentate ca membri deplini ai serviciului de director, la fel ca si sistemele Windows. Soluția trebuie sa ofere următoarele funcționalități minimale si obligatorii: • Sa includă mecanisme destinate configurării si licențierii aplicației • Sa includă o gama larga de opțiuni pentru migrare si implementare • Sa includă unelte de migrare NIS • Sa includă unelte de management la nivel de Group Policy atât pentru utilizatorii cat si grupurile locale Unix • Sa extindă autentificarea securizata Kerberos la nivelul sistemelor non-Windows • Sa asigure autentificare centralizata si single sign-on pentru sistemele non-Windows, prin intermediul contului utilizator de serviciu de director • Sa extindă metodele de autentificare complexa Windows (smart card, PKI, OTP) către sistemele non-Windows • Sa suporte forest-uri si domenii multiple • Sa suporte orice versiune de Windows Server la orice nivel funcțional de forest • Sa suporte trust-uri two-way, one-way sau no-way • Sa suporte opțiuni de migrare bazate pe schema, la fel ca si opțiuni de migrare care nu sunt bazate pe schema • Mecanisme de securitate multi-factor: soluția trebuie să integreze funcționalități de autentificare multi-factor, care să se mapeze direct pe serviciul de director și să poată fi gestionate direct in cadrul acestuia. Pentru autentificarea multi-factor, soluția trebuie sa ofere următoarele funcționalități minimale si obligatorii: • Identitățile, rolurile si regulile vor fi stocate si obținute direct din soluția de management al accesului sau din Active Directory • Întregul management va fi realizat din consola Active Directory Users and Computers sau din consola de administrare a solutiei • Utilizarea protocolului standard de industrie RADIUS – va include un proxy RADIUS complet • Disponibilitate completa – va livra servicii multiple pentru toleranta la indisponibilitate • Vor fi furnizate mecanisme de auto-înregistrare a utilizatorilor • Suport pentru o mare plaja de vendori de token-uri, hardware si/sau software; suport pentru orice token hardware conform OATH • Suport pentru iPhone, Android, BlackBerry, Windows, SMS si alte tehnologii suport de autentificare multi-factor • Control deplin al mediului de autentificare • Va exista o singura soluție de autentificare multi-factor pentru întregul mediu (Windows, Linux, Unix, aplicații, VPN, webmail etc.) • Fiecare utilizator va putea folosi mai multe token-uri pentru fiecare echipament, iar un token va putea fi alocat mai multor utilizatori Soluția va furniza funcționalități de securitate îmbunătățita prin:

	• Autentificare multi-factor complexa • Acces securizat webmail • Criptarea datelor la nivelul serviciului de autentificare multifactor • Asigurarea suportului de politici de securitate personalizabile • Activarea autentificării desktop prin token • Securizarea accesului VPN Componenta de autentificare multi-factor va livra un portal web-based in care se regăsesc facilitați complete de administrare: • Cadran de bord pentru vizualizarea rapida a principalelor metrici • Configurator de sistem • Înregistrarea si vizualizarea tuturor operațiunilor • Sistem de deployment pentru token-uri • Modul help desk • Management integrat • Rapoarte de stare
CERINȚE DE UZABILITATE SI INTERFAȚARE CU ADMINISTRATORII SI OPERATORII DE APLICAȚIE	• Toate operațiunile efectuate pentru administrarea sau operarea in aplicație vor fi efectuate dintr-o consola administrativa unica • Consola va procesa automat autentificarea in aplicație, in baza credentialelor de utilizator autentificat Windows • Consola va asigura un mediu grafic, vizual de administrare si operare • Consola va permite efectuarea de operațiuni in Active Directory pe baza apartenentei administratorilor la grupul de securitate Domain Admins ori in baza delegărilor de permisiuni efectuate de un administrator de domeniu. Toate funcționalitățile de administrare si operare prevăzute mai sus vor fi asigurate prin operare in consola de management, vor fi afișate in mod grafic, distinct pe categorii de acțiuni; interfața trebuie sa fie una deosebit de intuitiva si cu un nivel mare de uzabilitate
GARANȚIE/SUPORT	Suport pentru minimum 1 an