Izmjena postupka

OSNOVNI PODACI

Opis predmeta javne nabavke:

Nabavka i implementacija PAM (Privileged Access Management) sistema za pristup IKT serverskoj infrastrukturi Ministartsva pravde

Vrsta predmeta:

Usluge

Vrsta postupka:

Otvoreni postupak

PODACI O NARUČIOCU

Naziv:

MINISTARSTVO PRAVDE

PIB:

11070094

Uslovi prije izmjena

Opis	Tip uslova
U postupku javne nabavke može da učestvuje samo privredni subjekat koji: nije pravosnažno osuđivan i čiji izvršni direktor nije pravosnažno osuđivan za neko od krivičnih djela sa obilježjima: a) kriminalnog udruživanja; b) stvaranja kriminalne organizacije; c) davanje mita; č) primanje mita; ć) davanje mita u privrednom poslovanju; d) primanje mita u privrednom poslovanju; dž) utaja poreza i doprinosa; đ) prevare; e) terorizma; f) finansiranja terorizma; g) terorističkog udruživanja; h) učestovanja u stranim oružanim formacijama; i) pranja novca; j) trgovine ljudima; k) trgovine maloljetnim licima radi usvojenja; l) zasnivanja ropskog odnosa i prevoza lica u ropskom odnosu; dokaz: uvjerenje, potvrda ili drugi akt nadležnog organa izdato na osnovu kaznene evidencije, u skladu sa propisima države u kojoj privredni subjekat ima sjedište, odnosno u kojoj ovlašćeno lice tog privrednog subjekta ima prebivalište, radi utvrđivanja ispunjenosti uslova iz člana 99 stav 1 tačka 1 Zakona o javnim nabavkama	Obavezni uslovi
U postupku javne nabavke može da učestvuje samo privredni subjekat koji je izmirio sve dospjele obaveze po osnovu poreza i doprinosa za penzijsko i zdravstveno osiguranje.Dokaz: uvjerenje, potvrde ili drugi akt koji izdaje organ uprave nadležan za naplatu poreskih prihoda, odnosno nadležni organ države u kojoj privredni subjekat ima sjedište, radi utvrđivanja ispunjenosti uslova iz člana 99 stav 1 tačka 2 Zakona o javnim nabavkama.	Obavezni uslovi
Privredni subjekat treba da je upisan u Centralni registar privrednih subjekata ili drugi odgovarajući registar u državi u kojoj privredni subjekat ima sjedište. Dokaz o registraciji u Centralnom registaru privrednih subjekata ili drugom odgovarajućem registaru sa podacima o ovlašćenom licu privrednog subjekta, radi utvrđivanja ispunjenosti uslova iz člana 102 stav 1 tačka 1 Zakona o javnim nabavkama.	Uslovi za obavljanje djelatnosti
Izjava privrednog subjekta.	ESPD
60 dana od dana otvaranja ponuda.	Rok važenja ponude

Ponuđač je dužan dostaviti bezuslovnu i na prvi poziv naplativu garanciju ponude u iznosu od 2 % procijenjene vrijednosti javne nabavke, kao garanciju ostajanja u obavezi prema ponudi u periodu važenja ponude i 7 dana nakon isteka važenja ponude. Garancija ponude će se aktivirati ako ponuđač: 1) odustane od ponude u roku važenja ponude i/ili 2) odbije da potpiše ugovor o javnoj nabavci Garancija ponude dostavlja se: • neposrednom predajom na arhivi naručioca na adresi Naručioca, Ministarstvo pravde Ul. Vuka Karadžića broj 3, 8100 Podgorica. Preporučenom pošiljkom sa povratnicom na adresi Ministarstvo pravde Ul. Vuka Karadžića broj 3, 8100 Podgorica, radnim danima od 9:00 do 14:00 sati, zaključno sa danom 09.12.2025. godine do 12:00 sati.	Garancija ponude
Rok izvršenja ugovora je 30 dana od dana zaključivanja ugovora.	Rok izvršenja ugovora
Mjesto izvršenja ugovora je Ministarstvo pravde.	Mjesto izvršenja ugovora
30 dana od dana dostavljanja fakture	Rok plaćanja
Način plaćanja: Virmanski. Plaćanje će se obaviti nakon potpisivanja Zapisnika o uspješno izvršenoj instalaciji I implementaciji PAM sistema na infrastrukturi Naručioca, koji je potpisan od strane ovlašćenog lica Direktoraat za IKT pravosuđa.	Način plaćanja
Ponuđač treba da u okviru svoje organizacije posjeduje implementiran i sertifikovan sledeći ISO standard: • Sistem menadžmenta bezbjednošću informacija ISO/IEC 27001:2022 Važeći sertifikat služi kao dokaz da ponuđač ima implementiran ISO standard sistema menadžmenta u svojoj organizaciji.	Stručna i tehnička sposobnost
Privredni subjekat je dužan da posjeduje minimum iskustva na kvalitetnom i uspješnom izvršavanju poslova iz oblasti predmeta nabavke što se dokazuje potvrdama izdatih od strane korisnika o pruženim uslugama, tokom prethodnih godina ali ne duže od pet godina, računajući i godinu u kojoj je započet postupak javne nabavke, koje sadrže opis i predmet nabavke, vrijeme realizacije ugovora i konstataciju da je ugovor blagovremeno i kvalitetno izvršen. Minimum jedna potvrda na implementaciji PAM rješenja u državnim institucijama.	Stručna i tehnička sposobnost

Privredni subjekat je dužan da posjeduje stručne i kadrovske kapacitete koji su potrebni za izvršenje ugovora – minimum jedno stručno lice koja imaju važeći sertifikat CompTIA SecurityX ili ISC2 CISSP ili ISACA CISM sertifikat.Stručna i tehnička sposobnost dokazuje se: • dokazom o angažovanju radne snage (prijava na osiguranje zaposlenog, ugovor o radu, sporazum o preuzimanju zaposlenog, ugovor o korišćenju sposobnosti drugog subjekta ili drugi akt u skladu sa zakonom), dostavljanjem kopije traženog sertifikata i minimum jedna referenca o kvalitetnom i uspješnom izvršavanju usluge na implementaciji PAM rješenja u državnim institucijama. Napomena: Jedno lice može posjedovati više sertifikata.	Stručna i tehnička sposobnost
Privredni subjekat je dužan da posjeduje stručne i kadrovske kapacitete koji su potrebni za izvršenje ugovora – minimum jedno stručno lice koja imaju važeći sertifikat CompTIA Security + ili ISC2 CISSP ili ISACA CISM sertifikat. Stručna i tehnička sposobnost dokazuje se: • dokazom o angažovanju radne snage (prijava na osiguranje zaposlenog, ugovor o radu, sporazum o preuzimanju zaposlenog, ugovor o korišćenju sposobnosti drugog subjekta ili drugi akt u skladu sa zakonom), dostavljanjem kopije traženog sertifikata i minimum jedna referenca o kvalitetnom i uspješnom izvršavanju usluge na implementaciji PAM rješenja u državnim institucijama. Napomena: Jedno lice može posjedovati više sertifikata.	Stručna i tehnička sposobnost
Izabrani ponuđač se obavezuje da pruži tehničku podršku od godinu dana na ponuđeno rješenje .	Garantni rok

Uslovi nakon izmjena

Opis	Tip uslova
U postupku javne nabavke može da učestvuje samo privredni subjekat koji: nije pravosnažno osuđivan i čiji izvršni direktor nije pravosnažno osuđivan za neko od krivičnih djela sa obilježjima: a) kriminalnog udruživanja; b) stvaranja kriminalne organizacije; c) davanje mita; č) primanje mita; ć) davanje mita u privrednom poslovanju; d) primanje mita u privrednom poslovanju; dž) utaja poreza i doprinosa; đ) prevare; e) terorizma; f) finansiranja terorizma; g) terorističkog udruživanja; h) učestovanja u stranim oružanim formacijama; i) pranja novca; j) trgovine ljudima; k) trgovine maloljetnim licima radi usvojenja; l) zasnivanja ropskog odnosa i prevoza lica u ropskom odnosu; dokaz: uvjerenje, potvrda ili drugi akt nadležnog organa izdato na osnovu kaznene evidencije, u skladu sa propisima države u kojoj privredni subjekat ima sjedište, odnosno u kojoj ovlašćeno lice tog privrednog subjekta ima prebivalište, radi utvrđivanja ispunjenosti uslova iz člana 99 stav 1 tačka 1 Zakona o javnim nabavkama	Obavezni uslovi
U postupku javne nabavke može da učestvuje samo privredni subjekat koji je izmirio sve dospjele obaveze po osnovu poreza i doprinosa za penzijsko i zdravstveno osiguranje.Dokaz: uvjerenje, potvrde ili drugi akt koji izdaje organ uprave nadležan za naplatu poreskih prihoda, odnosno nadležni organ države u kojoj privredni subjekat ima sjedište, radi utvrđivanja ispunjenosti uslova iz člana 99 stav 1 tačka 2 Zakona o javnim nabavkama.	Obavezni uslovi
Privredni subjekat treba da je upisan u Centralni registar privrednih subjekata ili drugi odgovarajući registar u državi u kojoj privredni subjekat ima sjedište. Dokaz o registraciji u Centralnom registaru privrednih subjekata ili drugom odgovarajućem registaru sa podacima o ovlašćenom licu privrednog subjekta, radi utvrđivanja ispunjenosti uslova iz člana 102 stav 1 tačka 1 Zakona o javnim nabavkama.	Uslovi za obavljanje djelatnosti
Izjava privrednog subjekta.	ESPD
60 dana od dana otvaranja ponuda.	Rok važenja ponude

Ponuđač je dužan dostaviti bezuslovnu i na prvi poziv naplativu garanciju ponude u iznosu od 2 % procijenjene vrijednosti javne nabavke, kao garanciju ostajanja u obavezi prema ponudi u periodu važenja ponude i 7 dana nakon isteka važenja ponude. Garancija ponude će se aktivirati ako ponuđač: 1) odustane od ponude u roku važenja ponude i/ili 2) odbije da potpiše ugovor o javnoj nabavci Garancija ponude dostavlja se: • neposrednom predajom na arhivi naručioca na adresi Naručioca, Ministarstvo pravde Ul. Vuka Karadžića broj 3, 8100 Podgorica. Preporučenom pošiljkom sa povratnicom na adresi Ministarstvo pravde Ul. Vuka Karadžića broj 3, 8100 Podgorica, radnim danima od 9:00 do 14:00 sati, zaključno sa danom 16.12.2025. godine do 12:00 sati.	Garancija ponude
Rok izvršenja ugovora je 30 dana od dana zaključivanja ugovora.	Rok izvršenja ugovora
Mjesto izvršenja ugovora je Ministarstvo pravde.	Mjesto izvršenja ugovora
30 dana od dana dostavljanja fakture	Rok plaćanja
Način plaćanja: Virmanski. Plaćanje će se obaviti nakon potpisivanja Zapisnika o uspješno izvršenoj instalaciji I implementaciji PAM sistema na infrastrukturi Naručioca, koji je potpisan od strane ovlašćenog lica Direktoraat za IKT pravosuđa.	Način plaćanja
Ponuđač treba da u okviru svoje organizacije posjeduje implementiran i sertifikovan sledeći ISO standard: • Sistem menadžmenta bezbjednošću informacija ISO/IEC 27001:2022 Važeći sertifikat služi kao dokaz da ponuđač ima implementiran ISO standard sistema menadžmenta u svojoj organizaciji.	Stručna i tehnička sposobnost
Privredni subjekat je dužan da posjeduje minimum iskustva na kvalitetnom i uspješnom izvršavanju poslova iz oblasti predmeta nabavke što se dokazuje potvrdama izdatih od strane korisnika o pruženim uslugama, tokom prethodnih godina ali ne duže od pet godina, računajući i godinu u kojoj je započet postupak javne nabavke, koje sadrže opis i predmet nabavke, vrijeme realizacije ugovora i konstataciju da je ugovor blagovremeno i kvalitetno izvršen. Minimum jedna potvrda na implementaciji PAM rješenja u državnim institucijama.	Stručna i tehnička sposobnost

Privredni subjekat je dužan da posjeduje stručne i kadrovske kapacitete koji su potrebni za izvršenje ugovora – minimum jedno stručno lice koja imaju važeći sertifikat CompTIA SecurityX ili ISC2 CISSP ili ISACA CISM sertifikat.Stručna i tehnička sposobnost dokazuje se: • dokazom o angažovanju radne snage (prijava na osiguranje zaposlenog, ugovor o radu, sporazum o preuzimanju zaposlenog, ugovor o korišćenju sposobnosti drugog subjekta ili drugi akt u skladu sa zakonom), dostavljanjem kopije traženog sertifikata i minimum jedna referenca o kvalitetnom i uspješnom izvršavanju usluge na implementaciji PAM rješenja u državnim institucijama. Napomena: Jedno lice može posjedovati više sertifikata.	Stručna i tehnička sposobnost
Privredni subjekat je dužan da posjeduje stručne i kadrovske kapacitete koji su potrebni za izvršenje ugovora – minimum jedno stručno lice koja imaju važeći sertifikat CompTIA Security + ili ISC2 CISSP ili ISACA CISM sertifikat. Stručna i tehnička sposobnost dokazuje se: • dokazom o angažovanju radne snage (prijava na osiguranje zaposlenog, ugovor o radu, sporazum o preuzimanju zaposlenog, ugovor o korišćenju sposobnosti drugog subjekta ili drugi akt u skladu sa zakonom), dostavljanjem kopije traženog sertifikata i minimum jedna referenca o kvalitetnom i uspješnom izvršavanju usluge na implementaciji PAM rješenja u državnim institucijama. Napomena: Jedno lice može posjedovati više sertifikata.	Stručna i tehnička sposobnost
Izabrani ponuđač se obavezuje da pruži tehničku podršku od godinu dana na ponuđeno rješenje .	Garantni rok

Kriterijumi prije izmjena

Opis	Očekivani odgovor ponuđača	Metod bodovanja
Cijena	-	-
Reference sertifikovanog lica (CompTIA SecurityX)= 10 bodova Ponuđač čije sertifikovano lice ima najveći broj referenci dobija 10 bodova. Broj bodova za ponuđeni broj referenci = broj ponuđenih referenci/ najveći broj ponuđenih referenci x 10 Minimum jedna referenca sertifikovanog lica koja potvrdjuje izvršavanje usluge na implementaciji PAM rješenja u državnim institucijama.	Dokaz	Relativno
Reference sertifikovanog lica (CompTIA Security+)= 10 bodova Ponuđač čije sertifikovano lice ima najveći broj referenci dobija 10 bodova. Broj bodova za ponuđeni broj referenci = broj ponuđenih referenci/ najveći broj ponuđenih referenci x 10 Minimum jedna referenca sertifikovanog lica koja potvrdjuje izvršavanju usluge na implementaciji PAM rješenja u državnim institucijama.	Dokaz	Relativno

Kriterijumi nakon izmjena

Opis	Očekivani odgovor ponuđača	Metod bodovanja
Cijena	-	-
Reference sertifikovanog lica (CompTIA SecurityX)= 10 bodova Ponuđač čije sertifikovano lice ima najveći broj referenci dobija 10 bodova. Broj bodova za ponuđeni broj referenci = broj ponuđenih referenci/ najveći broj ponuđenih referenci x 10 Minimum jedna referenca sertifikovanog lica koja potvrdjuje izvršavanje usluge na implementaciji PAM rješenja u državnim institucijama.	Dokaz	Relativno
Reference sertifikovanog lica (CompTIA Security+)= 10 bodova Ponuđač čije sertifikovano lice ima najveći broj referenci dobija 10 bodova. Broj bodova za ponuđeni broj referenci = broj ponuđenih referenci/ najveći broj ponuđenih referenci x 10 Minimum jedna referenca sertifikovanog lica koja potvrdjuje izvršavanju usluge na implementaciji PAM rješenja u državnim institucijama.	Dokaz	Relativno

Tehnička specifikacija prije izmjena

Procijenjena vrijednost bez PDV	Redni broj predmeta nabavke	Opis predmeta nabavke	Bitne karakteristike predmeta nabavke	Količina	Jedinica mjere
40909.10	1	Nabavka i implementacija open-source Privileged Access Management (PAM) sistema koji obezbjeđuje povjerljivost, dostupnost i integritet podataka kroz centralizovano upravljanje privilegovanim nalozima i kontrolu pristupa. Rješenje je predviđeno za do 20 korisnika ali sa mogućnošću proširenja do 1000 korisnika.	PAM sistem omogućava bezbjedan pristup, audit i kontrolu svih aktivnosti privilegovanih korisnika, uz potpuni nadzor, snimanje sesija i zaštitu lozinki. 3. Funkcionalni Zahtjevi Rješenje mora podržavati 4A funkcionalnosti: Autentifikaciju, Autorizaciju, Upravljanje nalozima i Reviziju (Audit). PAM mora biti zasnovan na web-arhitekturi i omogućiti pristup sljedećim platformama i protokolima: Linux, Windows, Kubernetes, Database, RemoteApp (SSH, Telnet, RDP, VNC, K8s, MySQL, MariaDB, ClickHouse, DB2, Dameng, PostgreSQL, Oracle, SQL Server, Redis, MongoDB). Rješenje mora onemogućiti otkrivanje lozinki korisnicima, evidentirati sve aktivnosti, blokirati opasne SQL upite i ograničiti prenos datoteka i clipboard pristup. Upravljanje korisnicima, ulogama, i resursima Sistem mora podržavati vođenje korisničkih naloga (kreiranje, deaktiviranje, brisanje) i prateće grupe korisnika. Sistem mora podržavati definisanje uloga (roles) sa različitim privilegijama (RBAC) kao što su korisnik, administrator, auditor, sl. Sistem mora podržavati upravljanje resursima (“assets”): mrežni uređaji, serveri, storage uređaji, I ostala serverska infrastruktura, baze podataka, klasteri, RemoteApp-servisi, platfore za virtuelizaciju infrastrukture I sl. Sistem mora podržavati “tagging” i organizovanje resursa u zone / organizacione strukture radi lakšeg grupisanja i primjene politika odnosno kontrola. Sistem mora omogućiti određivanje dozvola korisniku ili grupi, resursu pa nakon toga određivanje vrste pristupa (npr. pristup, upravljanje, pregled). Sistem mora omogućiti da dozvole resursa propagiraju (“kaskadno”) sa nadređenih čvorova na podređene. Sistem mora omogućiti audit nad korisničkim ulogama i njihovim promjenama	1.00	komplet

(ko, kada, koja uloga je dodjeljena odnosno uklonjena).
Autentifikacija i pristup
Sistem mora omogućiti integraciju sa autentifikacionim mehanizmima: LDAP/AD, CAS, OIDC, SAML2, OAuth2, RADIUS.
Sistem mora imati mogućnost MFA odnosno 2-faktorsku autentifikacije.
Sistem mora omogućiti kontrolu pristupa na osnovu IP adrese, geografske lokacije, vremenskih pravila, pravila prihvatanja, odbijanja, login-pregleda.
Sistem mora omogućiti pravila koja ograničavaju na koji način i kada korisnik može pristupiti resursu (npr. dozvoljeni protokoli, vrsta klijenta, vrijeme, IP).
Sistem mora omogućiti “command filtering” tokom sesije: blokada/filtriranje naredbi koje korisnik može izvršiti na kranjem sistemu (npr. SSH komande, SQL komande i sl)
Sistem mora omogućiti “data masking / output cleansing”: mogućnost da se izlaz (npr. baze podataka ili terminal) maskira ili ograniči radi povjerljivosti.
Sistem mora podržavati “just-in-time” pristup ili pristup na zahtjev (request/approval workflow) za korisnike kojima pristup mora biti odobren prije nego dobiju pristup resursu.
Povezivanje prema resursima i protokolima
Sistem mora omogućiti pristup target resursima preko web-pregledača (web terminal): SSH, Telnet, RDP, VNC, Kubernetes, baze podataka, RemoteApp.
Sistem treba omogućiti pristup takođe putem desktop klijenata (po mogućnosti), za SSH/SFTP/RDP gdje je korisnički slučaj to zahtijeva.
Sistem mora podržavati broj različitih tipova ciljanih sistema: Linux/Unix, Windows, mrežni uređaji (network devices), baze podataka (MySQL, MariaDB, PostgreSQL, MongoDB, Redis, ClickHouse, Dameng, Oracle, SQL Server) i klasteri Kubernetes.
Sistem mora omogućiti pregled/odabir kredencijala (računa) za pristup krajnjim sistemima bez da se lozinka otkriva korisniku (npr, korisnik bira iz liste, ali nema mogućnost pregleda lozinke).
Sistem mora omogućiti transfer fajlova i clipboard-kontrolu u sesiji (primjer: SFTP web-klijent za prijenos, ograničenje smjera prijenosa, zabrana ako potrebno)

Snimanje sesija, revizija i analiza
Sistem mora snimati sve sesije u skladu sa protokolima:
oSSH/Telnet: snimanje komandi + timestamp + korisnik odnosno korisnički nalog
oRDP/VNC: snimanje video-zapisa (MP4 ili ekvivalent) ekrana sesije.
oBaze podataka: snimanje SQL upita i (gdje primjenjivo) rezultata.
Sistem mora omogućiti centralizovano skladištenje snimaka i logova u okviru lokalnog filesistema uz mogućnost arhiviranja, hash verifikacije i NTP sinhronizacije.
Sistem mora omogućiti playback (reprodukciju) snimljenih sesija sa kontrolama: premotavanje, traženje po vremenu, filtriranje po korisniku odnonso korisničkom nalogu.
Sistem mora bilježiti i čuvati audit zapise: korisnički login/logout, promjene autorizacija, file transferi, clipboard aktivnosti, komande, greške, neuspjeli pokušaji pristupa.
Sistem mora podržavati REST API interfejs za integraciju sa SIEM, ITSM i IAM sistemima. Logovi i audit podaci moraju biti eksportovani u centralni SIEM sistem putem Syslog/HTTP protokola
Sistem mora omogućiti metapodatke i strukturu logova koja omogućava forenzičku analizu i izveštavanje.
Upravljanje privilegovanim nalozima i tajnama
Sistem mora upravljati privilegovanim nalozima (“privileged accounts”) i omogućiti da korisnici pristupaju krajnjim sistemima bez vidljive lozinke.
Sistem mora podržati automatsku rotaciju lozinki, ključeva (gdje je moguće).
Sistem mora omogućiti sigurnu pohranu kredencijala (enkripciju) i kontrolu pristupa tim kredencijalima.
Sistem mora omogućiti reviziju pristupa privilegovanim računima: ko je ostvarion pristup, kada, na koji resurs, za koliko dugo, šta je radio.
Automatizacija i integracije
Sistem mora omogućiti REST API i/ili CLI za automatsko kreiranje/uklanjanje korisnika, resursa, autorizacija, izvještaja.
Sistem mora se integrisati sa IAM sistemima (Identity & Access Management),

			ITSM (ticketing), i/ili LDAP/AD za sinhronizaciju korisnika i grupa. Sistem mora podržati notificiranje (email/SMS) pri određenim događajima (npr. neuspjeli login) Skalabilnost Sistem mora podržati deployment u HA-clustera (Active-Active ili Active-Standby) za visoku dostupnost. Korisničko iskustvo i upravljanje Sistem mora imati web-interfejs za korisnike (pristup resursima) i za administratore (upravljanje, izvještaji). Sistem mora omogućiti “jedan klik” pristup korisnicima za autorizirane resurse, bez potrebe za ručnim unošenjem lozinke.		

Tehnička specifikacija nakon izmjena

Procijenjena vrijednost bez PDV	Redni broj predmeta nabavke	Opis predmeta nabavke	Bitne karakteristike predmeta nabavke	Količina	Jedinica mjere
40909.10	1	Nabavka i implementacija open-source Privileged Access Management (PAM) sistema koji obezbjeđuje povjerljivost, dostupnost i integritet podataka kroz centralizovano upravljanje privilegovanim nalozima i kontrolu pristupa. Rješenje je predviđeno za do 20 korisnika ali sa mogućnošću proširenja do 1000 korisnika.	PAM sistem omogućava bezbjedan pristup, audit i kontrolu svih aktivnosti privilegovanih korisnika, uz potpuni nadzor, snimanje sesija i zaštitu lozinki. 3. Funkcionalni Zahtjevi Rješenje mora podržavati 4A funkcionalnosti: Autentifikaciju, Autorizaciju, Upravljanje nalozima i Reviziju (Audit). PAM mora biti zasnovan na web-arhitekturi i omogućiti pristup sljedećim platformama i protokolima: Linux, Windows, Kubernetes, Database, RemoteApp (SSH, Telnet, RDP, VNC, K8s, MySQL, MariaDB, ClickHouse, DB2, Dameng, PostgreSQL, Oracle, SQL Server, Redis, MongoDB). Rješenje mora onemogućiti otkrivanje lozinki korisnicima, evidentirati sve aktivnosti, blokirati opasne SQL upite i ograničiti prenos datoteka i clipboard pristup. Upravljanje korisnicima, ulogama, i resursima Sistem mora podržavati vođenje korisničkih naloga (kreiranje, deaktiviranje, brisanje) i prateće grupe korisnika. Sistem mora podržavati definisanje uloga	1.00	komplet

(roles) sa različitim privilegijama (RBAC) kao što su korisnik, administrator, auditor, sl.
Sistem mora podržavati upravljanje resursima (“assets”): mrežni uređaji, serveri, storage uređaji, I ostala serverska infrastruktura, baze podataka, klasteri, RemoteApp-servisi, platfore za virtuelizaciju infrastrukture I sl.
Sistem mora podržavati “tagging” i organizovanje resursa u zone / organizacione strukture radi lakšeg grupisanja i primjene politika odnosno kontrola.
Sistem mora omogućiti određivanje dozvola korisniku ili grupi, resursu pa nakon toga određivanje vrste pristupa (npr. pristup, upravljanje, pregled).
Sistem mora omogućiti da dozvole resursa propagiraju (“kaskadno”) sa nadređenih čvorova na podređene.
Sistem mora omogućiti audit nad korisničkim ulogama i njihovim promjenama (ko, kada, koja uloga je dodjeljena odnosno uklonjena).
Autentifikacija i pristup
Sistem mora omogućiti integraciju sa autentifikacionim mehanizmima: LDAP/AD, CAS, OIDC, SAML2, OAuth2, RADIUS.
Sistem mora imati mogućnost MFA odnosno 2-faktorsku autentifikacije.
Sistem mora omogućiti kontrolu pristupa na osnovu IP adrese, geografske lokacije, vremenskih pravila, pravila prihvatanja, odbijanja, login-pregleda.
Sistem mora omogućiti pravila koja ograničavaju na koji način i kada korisnik može pristupiti resursu (npr. dozvoljeni protokoli, vrsta klijenta, vrijeme, IP).
Sistem mora omogućiti “command filtering” tokom sesije: blokada/filtriranje naredbi koje korisnik može izvršiti na kranjem sistemu (npr. SSH komande, SQL komande i sl)
Sistem mora omogućiti “data masking / output cleansing”: mogućnost da se izlaz (npr. baze podataka ili terminal) maskira ili ograniči radi povjerljivosti.
Sistem mora podržavati “just-in-time” pristup ili pristup na zahtjev (request/approval workflow) za korisnike kojima pristup mora biti odobren prije nego dobiju pristup resursu.
Povezivanje prema resursima i protokolima
Sistem mora omogućiti pristup target

resursima preko web-pregledača (web terminal): SSH, Telnet, RDP, VNC, Kubernetes, baze podataka, RemoteApp.
Sistem treba omogućiti pristup takođe putem desktop klijenata (po mogućnosti), za SSH/SFTP/RDP gdje je korisnički slučaj to zahtijeva.
Sistem mora podržavati broj različitih tipova ciljanih sistema: Linux/Unix, Windows, mrežni uređaji (network devices), baze podataka (MySQL, MariaDB, PostgreSQL, MongoDB, Redis, ClickHouse, Dameng, Oracle, SQL Server) i klasteri Kubernetes.
Sistem mora omogućiti pregled/odabir kredencijala (računa) za pristup krajnjim sistemima bez da se lozinka otkriva korisniku (npr, korisnik bira iz liste, ali nema mogućnost pregleda lozinke).
Sistem mora omogućiti transfer fajlova i clipboard-kontrolu u sesiji (primjer: SFTP web-klijent za prijenos, ograničenje smjera prijenosa, zabrana ako potrebno)
Snimanje sesija, revizija i analiza
Sistem mora snimati sve sesije u skladu sa protokolima:
oSSH/Telnet: snimanje komandi + timestamp + korisnik odnosno korisnički nalog
oRDP/VNC: snimanje video-zapisa (MP4 ili ekvivalent) ekrana sesije.
oBaze podataka: snimanje SQL upita i (gdje primjenjivo) rezultata.
Sistem mora omogućiti centralizovano skladištenje snimaka i logova u okviru lokalnog filesistema uz mogućnost arhiviranja, hash verifikacije i NTP sinhronizacije.
Sistem mora omogućiti playback (reprodukciju) snimljenih sesija sa kontrolama: premotavanje, traženje po vremenu, filtriranje po korisniku odnonso korisničkom nalogu.
Sistem mora bilježiti i čuvati audit zapise: korisnički login/logout, promjene autorizacija, file transferi, clipboard aktivnosti, komande, greške, neuspjeli pokušaji pristupa.
Sistem mora podržavati REST API interfejs za integraciju sa SIEM, ITSM i IAM sistemima. Logovi i audit podaci moraju biti eksportovani u centralni SIEM sistem putem Syslog/HTTP protokola
Sistem mora omogućiti metapodatke i strukturu logova koja omogućava forenzičku

			analizu i izveštavanje. Upravljanje privilegovanim nalozima i tajnama Sistem mora upravljati privilegovanim nalozima (“privileged accounts”) i omogućiti da korisnici pristupaju krajnjim sistemima bez vidljive lozinke. Sistem mora podržati automatsku rotaciju lozinki, ključeva (gdje je moguće). Sistem mora omogućiti sigurnu pohranu kredencijala (enkripciju) i kontrolu pristupa tim kredencijalima. Sistem mora omogućiti reviziju pristupa privilegovanim računima: ko je ostvarion pristup, kada, na koji resurs, za koliko dugo, šta je radio. Automatizacija i integracije Sistem mora omogućiti REST API i/ili CLI za automatsko kreiranje/uklanjanje korisnika, resursa, autorizacija, izvještaja. Sistem mora se integrisati sa IAM sistemima (Identity & Access Management), ITSM (ticketing), i/ili LDAP/AD za sinhronizaciju korisnika i grupa. Sistem mora podržati notificiranje (email/SMS) pri određenim događajima (npr. neuspjeli login) Skalabilnost Sistem mora podržati deployment u HA-clustera (Active-Active ili Active-Standby) za visoku dostupnost. Korisničko iskustvo i upravljanje Sistem mora imati web-interfejs za korisnike (pristup resursima) i za administratore (upravljanje, izvještaji). Sistem mora omogućiti “jedan klik” pristup korisnicima za autorizirane resurse, bez potrebe za ručnim unošenjem lozinke.		