

**“O‘zbekiston ipotekani qayta moliyalashtirish kompaniyasi” AJning
axborot resurslarini himoyalash va ma’lumotlarni ruxsatsiz tarqalishining
oldini olish maqsadida DLP tizimini joriy etish uchun**

TEXNIK TOPSHIRIQ

1. Umumiy qoidalar

1. Mazkur texnik topshiriq, "O‘zbekiston ipotekani qayta moliyalashtirish kompaniyasi" aksiyadorlik jamiyatida (bundan keyingi matnda – Kompaniya) axborot xavfsizligi tahdidlarini kamaytirish, axborot resurslarining himoyalashini ta’minlash hamda ma’lumotlarning ruxsatsiz tarqalishining oldini olish maqsadida, DLP (Data Loss Prevention) tizimidan (bundan keyingi matnda – Tizim) foydalanish huquqini (litsenziyalarni) 1 (bir) yil muddatga xarid qilish, **Tizimni amaliyotga to‘liq joriy etish (sozlash, integratsiya qilish va o‘qitish) ishlarini amalga oshirish** hamda Tizim ishlab chiquvchisining 1 (bir) yillik texnik qo‘llab-quvvatlash xizmatini olish uchun ishlab chiqilgan. Xarid predmeti **litsenziyalarni yetkazib berish, Tizimni amaliyotga to‘liq joriy etish ishlarini bajarish hamda Tizim ishlab chiquvchisining va Ijrochining texnik qo‘llab-quvvatlash xizmatini ko‘rsatishni o‘z ichiga oladi.**

2. **Buyurtmachi** - “O‘zbekiston ipotekani qayta moliyalashtirish kompaniyasi” AJ.

3. **Ijrochi** - tomonlar o‘rtasida davlat xaridlari to‘g‘risidagi qonunchilikka muvofiq tuzilgan shartnoma asosida, mazkur texnik topshiriq talablariga muvofiq litsenziyalarni yetkazib berish va Tizim ishlab chiquvchisining (ishlab chiqaruvchisining) texnik qo‘llab-quvvatlash xizmatini ko‘rsatishni ta’minlash majburiyatini olgan yuridik shaxs.

2. Loyihaning maqsadi

4. Kompaniya ma’lumotlarining ichki va tashqi kanallar orqali ruxsat etilmagan (sanksiyanmagan) chiqib ketishini oldini olish.

5. Maxfiy ma’lumotlarning sizib chiqishi bilan bog‘liq insidentlarni aniqlash, tahlil qilish va cheklash.

6. Qonunchilik va ichki me’yoriy hujjatlarning talablariga rioya qilinishini ta’minlash.

7. Kompaniya ishchi stansiyalarida hamda belgilangan axborot resurslarida saqlanadigan maxfiy ma’lumotlarni ularning mazmuni, konteksti, rekvizitlari yoki namunalari asosida aniqlash va tasniflash hamda ularga xavfsizlik siyosatlarini qo‘llash. Tasniflash maxfiylik belgilari (metkalar – label/tag), raqamli izlar (digital fingerprint), lug‘atlar, muntazam iboralar (regular expressions) yoki boshqa ekvivalent mexanizmlardan foydalangan holda amalga oshirilishi mumkin. Ijrochi loyihani amalga oshirish, sozlash va texnik qo‘llab-quvvatlash davrida Buyurtmachining maxfiy ma’lumotlari daxlsizligini to‘liq ta’minlashi shart. Tizimning texnik nosozligi, noto‘g‘ri sozlanishi yoki Ijrochi xodimlarining aybi/loqaydligi sababli maxfiy ma’lumotlarning uchinchi shaxslarga sizib chiqishi (konfidensiallikning buzilishi) hodisasi yuz berganda, **Ijrochi yetkazilgan to‘liq moddiy va ma’naviy zararni (to‘liq moliyaviy javobgarlik) qoplab berishi shart**, shuningdek, Ijrochiga nisbatan **Shartnoma umumiy qiymatining 10% miqdorida bir martalik**

jarima qo'llaniladi va bu holat Shartnomani Buyurtmachi tomonidan bir tomonlama bekor qilishga hamda Ijrochini insofsiz ijrochilar reestriga kiritishga haqli asos bo'ladi.

3. Tizimga qo'yiladigan texnik va funksional talablar

8. Maxfiy ma'lumotlar uzatish jarayonini nazorat qilish – bu nazorat ham ichki lokal tarmoq doirasida, ham tashqi tarmoqlarga bo'lgan uzatmalarni o'z ichiga olishi.

9. Maxfiy ma'lumotlarning har qanday kanal orqali tarqalishini samarali ravishda oldini olish.

10. Tizim ishchi stansiyalar (xizmat kompyuterlari, "Endpoint") darajasida ishlashi, shuningdek, ishlab chiqaruvchi tomonidan qo'llab-quvvatlanadigan standart mexanizmlar, jumladan API, Syslog, elektron pochta orqali bildirishnomalar yuborish yoki boshqa ekvivalent usullar yordamida SIEM, HelpDesk va boshqa markazlashgan monitoring tizimlari bilan integratsiyani ta'minlay olishi kerak.

11. Tizim foydalanuvchilarni boshqarish hamda "**Active Directory**" (AD) bilan integratsiya qilish imkoniyatlarini ta'minlashi. Jumladan:

AD bilan integratsiya orqali foydalanuvchilarning identifikatsion ma'lumotlarini Tizimga import qilish, yangi foydalanuvchilar uchun avtomatik profil yaratish va mavjud profillarni o'zgartirish imkoniyati mavjud bo'lishi;

AD foydalanuvchi ma'lumotlaridagi o'zgarishlar (foydalanuvchining ishchi stansiyasi almashishi, operatsion tizim qayta o'rnatilishi va shu kabi holatlar) Tizim bilan avtomatik ravishda sinxronlashtirilishi;

sinxronizatsiya jarayonlarini belgilangan jadval asosida avtomatik ravishda amalga oshirish parametrlarini sozlash imkoniyati mavjud bo'lishi;

noma'lum (yangi aniqlangan) foydalanuvchilar uchun avtomatik tarzda profil (kartochka) yaratish.

12. Tizim monolit yoki modulli arxitekturaga ega bo'lishi mumkin. Alohida modullar (kichik tizimlar), agentlar, sensorlar yoki konsollardan foydalanish taklifni cheklash uchun asos bo'lmasligi kerak, biroq taklif tarkibiga mazkur texnik topshiriqda belgilangan majburiy funksiyalarni bajarish uchun zarur bo'lgan barcha komponentlar, litsenziyalar va integratsiyalar kiritilishi shart.

13. Tizim Buyurtmachining mahalliy tarmog'ida *on-premise* modeli bo'yicha joylashtirilishi hamda Internet tarmog'iga doimiy ulanishsiz asosiy funksional rejimda ishlashi kerak. Agar litsenziyalarni aktivlashtirish, ularning haqiqiyligini tekshirish, yangilanishlarni olish yoki texnik qo'llab-quvvatlash uchun Internet tarmog'iga vaqtinchalik ulanish zarur bo'lsa, Ijrochi buni taklifda oldindan ko'rsatishi shart.

14. Tizimda ishlab chiqaruvchi tomonidan qo'llab-quvvatlanadigan ma'lumotlar bazasini boshqarish tizimidan (MBBT) foydalanilishi mumkin: MS SQL Server, PostgreSQL, MongoDB, o'rnatilgan MBBT (*embedded DBMS*) yoki boshqa ekvivalent MBBT. Foydalanilayotgan MBBT versiyasi xavfsizlik yangilanishlarini oladigan, hujjatlashtirilgan hamda Tizimning taklif etilayotgan versiyasiga mos bo'lishi kerak.

15. Tizim domenli tarmoq muhitida hamda domenlarsiz (mustaqil) tarmoq muhitida barqaror ishlash imkoniyatini ta'minlashi kerak.

16. Tizim Buyurtmachida mavjud bo'lgan VMware virtual infratuzilmasida yoki Ijrochi tomonidan asoslantirilgan boshqa virtual yoki jismoniy platformada ishlashi kerak. Hyper-V, Citrix, KVM va boshqa platformalarni qo'llab-quvvatlash qo'shimcha afzallik sifatida ko'rsatilishi mumkin..

17. Tizim ishchi stansiyalarda amalga oshirilayotgan faoliyatlarni **chuqur tahlil qilish** imkoniyatini ta'minlashi, xususan **Tizim jarayonlari, foydalanuvchi faoliyati, ma'lumotlar bilan ishlash** jarayonlari hamda **o'rnatilgan dasturlar auditi** yuritilishini nazorat qilishi.

18. Tizim virtual ish stoli infratuzilmasi (VDI – “Virtual Desktop Infrastructure”) muhitida ishlayotgan qurilmalar uchun ham himoya ta'minlashi.

19. Tizim komponentlari o'rtasida ma'lumot almashinuvi TCP/IP” protokollari oilasiga kiruvchi protokollar va “Ethernet / Fast Ethernet / Gigabit Ethernet” interfeyslari orqali, shuningdek, Kompaniyaning mahalliy tarmog'i doirasida yoki korporativ “Wi-Fi” tarmog'i orqali amalga oshirilishi.

20. Masofaviy ishlash holatlarida foydalanuvchi internetga Ethernet, Wi-Fi, mobil modem, uyali aloqa operatorlari yoki boshqa tashqi tarmoqlar orqali ulanishi mumkin. Bunday ulanishlar Kompaniyaning to'liq nazorat doirasidan tashqarida bo'lganligi sababli, masofadan ishlovchi qurilmalarda Kompaniyaning maxfiy ma'lumotlari har qanday ulanish turidan qat'i nazar avtonom ravishda himoyalaniishini ta'minlaydigan tegishli mexanizmlar mavjud bo'lishi.

21. Tizim maxfiy ma'lumotlarni aniqlash maqsadida ishchi stansiyalar, serverlar va belgilangan tarmoq kataloglarida saqlanayotgan ma'lumotlarni mazmunan skanerlashni ta'minlashi yoki ushbu vazifani alohida modul hamda integratsiya orqali bajarishi kerak. Skanerlash sohasi (qamrovi), davriyligi va cheklovlari taklifda ko'rsatilgan bo'lishi lozim.

22. Tizim ishchi stansiyalarga hamda zarurat bo'lganda serverlarga o'rnatiladigan, markazlashgan holda boshqariladigan bir yoki bir nechta agentlar, sensorlar yoki modullar orqali quyidagi funksiyalarni amalga oshirishi kerak:

maxfiy ma'lumotlar sizib chiqishini oldini olish (Data Loss Prevention);

ishchi stansiyalarda maxfiy ma'lumotlarni aniqlash;

ma'lumotlarni avtomatik yoki yarim avtomatik ravishda aniqlash va tasniflash (klassifikatsiya qilish), shu jumladan metkalar, raqamli izlar (*digital fingerprint*), metama'lumotlar yoki boshqa ekvivalent mexanizmlardan foydalangan holda;

ulanayotgan qurilmalarni nazorat qilish;

insidentlarni tahlil qilish va surishtirish (*forensics/investigation*) uchun hodisalarning markazlashgan arxivi hamda tahlil vositalarini taqdim etish;

buyurtmachining asosiy ishchi stansiyalarida foydalaniladigan Windows operatsion tizimlarini qo'llab-quvvatlash; macOS, Linux va VDI muhitlarini qo'llab-quvvatlash imkoniyatlari taklifda alohida ko'rsatilgan bo'lishi lozim;

nazorat vazifasiga qarab oxirgi nuqtaga (*Endpoint*) o'rnatilishi yoki tarmoq sensori, proksi-server, pochta shlyuzi yoki bo'lmasa boshqa ekvivalent mexanizm orqali ishlashi;

Tizim klient-server, veb-arxitektura, dasturiy-apparat majmuasi (*appliance*) yoki ishlab chiqaruvchi tomonidan qo'llab-quvvatlanadigan boshqa arxitektura asosida qurilgan bo'lishi mumkin;

server komponentlari ma'lumotlarni boshqarish, qayta ishlash, saqlash va tahlil qilishni ta'minlashi kerak;

Tizimining agenti ishchi stansiyalar va serverlarda barqaror va yuqori samaradorlik bilan ishlashi lozim. Agent Tizim resurslarini – operativ xotira (RAM), markaziy protsessor (CPU) va disk xotirasini – oqilona darajada iste'mol qilishi, ishchi stansiyalarga ortiqcha yuk tushirmasligi hamda foydalanuvchi ish faoliyatiga salbiy ta'sir ko'rsatmasligi;

ishchi stansiyada ishlaydigan agent yoki modul oddiy foydalanuvchi tomonidan ruxsatsiz o'chirilishi, to'xtatilishi yoki sozlamalari o'zgartirilishidan himoyalangan xizmat rejimida faoliyat ko'rsatishi kerak;

agentning foydalanuvchiga ko'rinishi Kompaniyaning ichki hujjatlari va amaldagi qonunchilikka muvofiq sozlana oladigan bo'lishi lozim;

Agent tarmoq bilan aloqa uzilgan holatlarda ham mustaqil (avtonom) rejimda ishlash, siyosatlarni mahalliy darajada qo'llash va qayta ulanish amalga oshirilgandan so'ng yig'ilgan hodisa ma'lumotlarini markaziy serverga uzatish imkoniyatini ta'minlashi.

23. Tizim agentlari va komponentlarining operatsion tizimlar bilan mosligi quyidagi talablarni inobatga olgan holda ta'minlanishi kerak:

Buyurtmachi tomonidan foydalaniladigan hamda ishlab chiqaruvchi tomonidan qo'llab-quvvatlanadigan Windows 10 va Windows 11 versiyalari;

server operatsion tizimlarini agentlar orqali nazorat qilish ko'zda tutilganda — Windows Server va Linuxning qo'llab-quvvatlanadigan versiyalari (bunda nazorat qilish, skanerlash va ma'lumotlar sizib chiqishining oldini olish bo'yicha mavjud funksiyalar ko'rsatilgan holda).

Linux virtual serverlari uchun qo'llab-quvvatlanadigan aniq distributivlar, yadro (kernel) versiyalari, mavjud nazorat kanallari va funksional cheklovlar ko'rsatilgan bo'lishi lozim;

Agent nazoratni, ma'lumotlarni qidirish moduli (Data Discovery), tarmoq komponenti yoki ishlab chiqaruvchi tomonidan hujjatlashtirilgan boshqa mexanizm orqali amalga oshirishga ruxsat beriladi;

Turli operatsion tizimlar uchun funksional imkoniyatlar bir-biridan farq qilishi mumkin. Ijrochi o'z taklifi tarkibida kamida 75 ta jismoniy yoki virtual foydalanuvchi ish o'rinlari uchun, shuningdek, agar taklifda ularning agentlik nazorati nazarda tutilgan bo'lsa, Windows/Linux server operatsion tizimlari uchun operatsion tizimlar va nazorat kanallari bo'yicha batafsil moslik matritsasini taqdim etishi shart.

24. Texnik platforma, litsenziyalash va resurslarga qo'yiladigan talablar. Jumladan:

Tizim arxitekturasini bir yoki bir nechta ma'lumotlar bazasi, server komponentlari hamda operatsion tizimlar oilasidan foydalanishi mumkin. Barcha komponentlar ishlab chiqaruvchi tomonidan qo'llab-quvvatlanadigan, hujjatlashtirilgan, litsenziyalangan hamda xavfsizlik yangilanishlarini o'rnatish imkoniyatiga ega bo'lishi kerak;

Tizim agent yoki foydalanuvchi komponentlari orqali uzatilayotgan barcha ma'lumotlar shifrlanib himoyalangan bo'lishi;

Tizim agenti orqali kuzatuvdagi barcha operatsiyalar bo'yicha ma'lumotlarni Tizim serveriga uzatish va saqlash;

Litsenziyalash modeli foydalanuvchilar, kompyuterlar, ish o'rinlari, serverlar, pochta manzillari soniga, ma'lumotlar hajmiga, fayl xotiralariga, tarmoq tugunlariga, server komponentlariga, modullarga yoki ularning kombinatsiyasiga asoslanishi mumkin. Ijrochi litsenziyalarni biriktirish va qayta biriktirish tartibini, nafaol obyektlardan litsenziyalarni bo'shatish imkoniyatini, funksional cheklovlarni hamda Tizimni kengaytirish qiymatini belgilash tamoyillarini aniq ko'rsatib berishi shart.

25. Tizim yagona yoki mantiqiy ravishda o'zaro bog'langan konsollar va veb-interfeyslar orqali quyidagilarni ta'minlashi kerak:

sozlamalarni kiritish;

xavfsizlik siyosatlarini boshqarish;

insidentlarni nazorat qilish;

hisobotlarni avtomatik shakllantirish;

konsolga kirish huquqiga ega xodimlarning vazifasiga qarab turli kirish darajalarini aniqlash va rollar modelini keng sozlash imkoniyati;

DLP agentlari yoki komponentlarini oxirgi nuqtalarga markazlashgan holda o'rnatish, shu jumladan Tizim konsoli, Active Directory guruh siyosatlari (GPO), MSI-paketlar, masofadan o'rnatish vositalari yoki boshqa hujjatlashtirilgan usullar orqali;

Tizim ma'lumotlar arxivi, xavfsizlik siyosati sozlamalariga nisbatan huquqni cheklash imkoniyati.

26. Ma'lumotlarga maxfiylik belgilarini (klassifikatsiya) qo'llash. Jumladan:

Fayl fayl yoki elektron xatning joylashuvi, egasi, yaratilgan vaqti, kelib chiqishi, jo'natuvchisi yoki qabul qiluvchisi, hajmi, kengaytmasi hamda boshqa metama'lumotlar yoki kontekstual ma'lumotlar asosida aniqlash;

fayl yoki elektron xatning harakat yo'nalishi, shu jumladan saqlash joyi, uzatish kanali, manbasi va qabul qiluvchisi asosida aniqlash yoki tasniflash;

faylni yaratgan, ochgan yoki tahrirlagan dasturiy ta'minot va jarayonlar kontekstini hisobga olish;

fayl yoki elektron xat egasi, foydalanuvchi, foydalanuvchilar guruhi, qurilma yoki tashkiliy bo'linma asosida siyosatlarni qo'llash;

teglar (belgilar), raqamli izlar (*digital fingerprint*), metama'lumotlar, lug'atlar, iboralar andozalari (*regular expressions*), ma'lumotlarni aniq moslashtirish (*exact data matching*), mashinaviy tahlil yoki boshqa teng qiymatli usullardan foydalangan holda maxfiy ma'lumotlarni aniqlash;

Tizim maxfiylik teglaridan (belgilaridan) foydalansa, teg faylga yoki elektron pochta obyektiga biriktirilishi hamda ishlab chiqaruvchi tomonidan qo'llab-quvvatlanadigan operatsiyalarni bajarishda saqlanib qolishi kerak; agar texnik doimiy biriktirish imkoni bo'lmasa, aniqlashning ekvivalent mexanizmi nazarda tutilgan bo'lishi lozim;

imkoniyatga qarab, arxivlangan fayllarni (ZIP, RAR va boshqalar), kengaytmasi o'zgartirilgan yoki boshqa konteynerga joylashtirilgan fayllarni ochish va tahlil qilish. Agar parol bilan himoyalangan yoki shifrlangan obyektning tarkibini tahlil qilish imkoni bo'lmasa, Tizim metama'lumotlar, fayl turi yoki siyosat asosida bunday uzatishni ro'yxatga olishi, ogohlantirishi yoki bloklashi kerak;

Word, Excel, PowerPoint, PDF hujjatlarini hamda elektron pochta obyektlarini qo'lda yoki avtomatik tarzda tasniflash va aniqlashni ta'minlash yoki shunga o'xshash natijani beruvchi ekvivalent mexanizmni qo'llash.

27. Tizim quyidagi subyektlar, jarayonlar yoki vositalar tomonidan maxfiy yoki siyosatlar bilan cheklangan ma'lumotlarga nisbatan amalga oshiriladigan ruxsatsiz harakatlarni aniqlashni va siyosatda nazarda tutilgan ta'sir choralarini (reaksiyalarni) qo'llashni ta'minlashi kerak:

aniqlangan dasturiy jarayonlar, masalan, ma'lumotlarni avtomatik tarzda nusxalovchi, arxivlovchi yoki tashqi manzillarga uzatuvchi dasturlar;

aniqlangan foydalanuvchi hisoblari (ruxsatsiz kirishga harakat qilgan shaxslar);

aniqlangan ishchi qurilmalar yoki ulanish konteksti, shu jumladan noma'lum tarmoq, ruxsat berilmagan qurilma, yuqori xavf holati va boshqa holatlar.

28. Ushbu texnik topshiriq bilan majburiy deb belgilangan axborot uzatish kanallari doirasida Tizim maxfiy axborotning sizib chiqishini nazorat qilish, ro'yxatga olish, ogohlantirish hamda texnik jihatdan imkon mavjud bo'lgan holatlarda bloklashni ta'minlashi ko'rsatilgan barcha axborot uzatish kanallari doirasida maxfiy axborotlarning sizib chiqishiga qarshi ishonchli himoyani ta'minlash.

29. Tizim tarmoq infratuzilmasi bo'ylab, ma'lumot uzatish tezligi past bo'lgan segmentlarda, tarmoq trafigini optimallashtirish, resurslardan samarali foydalanish va yuklamani muvozanatlash orqali uzatish kanallari bandligidan qat'iy nazar, Tizimning uzluksiz va barqaror ishlashini ta'minlash.

30. Maxfiy ma'lumotlar bilan ishlashda foydalanuvchilar, qurilmalar va dasturiy jarayonlarning nazorat qilinadigan harakatlari jurnalini yuritish.

31. Foydalanuvchi maxfiy ma'lumotlar yoki muhim ilovalar bilan ishlayotganda Tizim taklif etilayotgan modul imkoniyatlari doirasida ilovalarni, fayl operatsiyalarini, oynalarni yoki ekran faolligini nazorat qilishi kerak.

32. Maxfiy ma'lumotlar aks etayotgan hujjatlar yoki ilovalar ochiq bo'lgan holatlarda Tizim PrintScreen va ekran suratlarini yaratishning boshqa usullaridan foydalanishni aniqlashi, ro'yxatga olishi yoki texnik imkoniyat mavjud bo'lganda bloklashi kerak. Agar bloklash qo'llab-quvvatlanmasa, Ijrochii ekvivalent nazorat choralarini ko'rsatishi lozim.

33. Ma'lumotlar formatidan qat'i nazar, shu jumladan matn, tasvir, fayl, elektron pochta va boshqa shakllarda bo'lishidan qat'i nazar, mazmunni aniqlash va unga nisbatan xavfsizlik siyosatlarini qo'llash. Tasvirlar hamda skanerlangan hujjatlarni tahlil qilish uchun OCR alohida modul sifatida taklif etilishi mumkin.

34. Har bir xodim, ishchi stansiya yoki foydalanuvchiga individuallashtirilgan xavfsizlik siyosatlarini qo'llash.

35. Tizim maxfiy yoki cheklangan ma'lumotlarga nisbatan siyosatni buzuvchi harakatlar, masalan, ishlov berish, nusxalash, yuborish, chop etish yoki bulutga yuklash holatlari aniqlanganda, Tizim texnik jihatdan qo'llab-quvvatlanadigan kanallarda alohida yoki birgalikda nazorat qilish, ro'yxatga olish, ogohlantirish yoki bloklash choralarini qo'llashi kerak. Taklif etilayotgan konfiguratsiya imkoniyatlari doirasida quyidagi operatsiyalar nazorat qilinishi lozim:

yaratish - yangi fayl yoki katalog (papka) hosil qilinganida;

o'qish - fayl yoki papkadagi ma'lumot ochilganida yoki ko'rilganida;

yo'zish - faylga yangi ma'lumot kiritilganida yoki mavjud ma'lumot ustidan yozilganida;

o'chirish - fayl yoki katalog tizimdan o'chirilganida;

nomini o'zgartirish - fayl yoki papkaning nomi o'zgartirilganida;

ishga tushirish - bajariladigan fayl (masalan, dastur) ishga tushirilganida;

kengaytmasini o'zgartirish - faylning kengaytmasi o'zgartirilganida (misol uchun: DOCX formatidan PDF, rasm va boshqa shu kabi fayl formati o'zgarishlari);

joyini o'zgartirish - fayl yoki katalog boshqa joyga ko'chirilganida;

nusxa ko'chirish - fayl yoki katalogdan nusxa olinganida;

kirishni taqiqlash - foydalanuvchi tomonidan fayl yoki katalogga kirish urinishiga ruxsat berilmaganida.

36. Ma'lumotlarni saqlash qurilmalari hamda ularni uzatish kanallari, shu jumladan USB va boshqa tashqi qurilmalar, elektron pochta, printerlar, FTP/SFTP, veb-resurslar, bulutli xizmatlar, messenjerlar va boshqa kanallar uchun alohida yoki guruhli xavfsizlik siyosatlarini qo'llash imkoniyati nazarda tutilgan bo'lishi kerak.

37. Tizim axborot xavfsizligi hodisalari (insidentlar) to'g'risidagi ma'lumotlarni real vaqtga yaqin rejimda monitoring qilishni, ularni markazlashtirilgan holda arxivlashni va hisobotlarni shakllantirishni ta'minlashi kerak. Kamida majburiy nazorat kanallari bo'yicha ro'yxatga olish, administratorni xabardor qilish va bloklash ta'minlanishi lozim. Shuningdek, quyidagi qo'shimcha ta'sir choralaridan biri yoki bir nechta qo'llab-quvvatlanishi mumkin:

foydalanuvchini ogohlantirmasdan bloklash;

foydalanuvchini ogohlantirish bilan bloklash;

foydalanuvchini ogohlantirish yoki foydalanuvchining qabul qilgan qarorlarini yozib olish;

asos (izoh) kiritilgandan so'ng yuborishga ruxsat berish;

“Soya nusxasini (shadow copy) yaratish, karantinga joylashtirish yoki boshqa isbotlovchi nusxani yaratish orqali hodisani hujjatlashtirish;

maxfiy ma'lumot uzatilganda mazkur jarayonni va trafik uzatishni avtomatik to'xtatish (matn yoki fayl ko'rinishida).

38. Hisobotlar uchun kamida bitta inson o'qiy oladigan formatda (PDF yoki uning ekvivalenti) va kamida bitta mashina o'qiy oladigan formatda (CSV, XLS/XLSX yoki uning ekvivalenti) eksport qilish imkoniyati nazarda tutilgan bo'lishi kerak.

39. Tizim sozlamalarini boshqarish va uning normal ishlashini avtomatik nazorat qilish, administratorni ogohlantirish.

40. Ma'lumotlar uzatilishini nazorat qilish va bloklash jarayonida Tizim tarmoq sensori, proksi-server yoki shlyuz, pochta serveri bilan integratsiya yoki boshqa ekvivalent mexanizmlar orqali quyidagi funksional imkoniyatlarni ta'minlashi lozim:

Axborot uzatish kanallarini aniqlash, tahlil qilish hamda belgilangan siyosatlariga muvofiq shartli yoki shartsiz bloklash;

HTTP/HTTPS axborot uzatish kanallarini aniqlash va tahlil qilish, belgilangan siyosatlariga muvofiq ro'yxatga olish, ogohlantirish hamda texnik imkoniyat mavjud bo'lganda shartli yoki shartsiz bloklash;

HTTP/HTTPS orqali veb-resurslarga yuborilayotgan ma'lumotlarni agent, proksi-server yoki shlyuz yo bo'lmasa tarmoq sensori darajasida nazorat qilish; shifrlangan trafikni tahlil qilish usuli va cheklovlari tijorat taklifida ko'rsatilishi kerak;

Mahsulot imkoniyatlari doirasida veb-xizmatlarga ma'lumot yuborish operatsiyalarini, shu jumladan POST/GET va boshqa amaliy mexanizmlarni tahlil qilish; Trafikni tahlil qilishda uzatish marshrutlari, tezlik chegaralari hamda oraliq serverlar orqali qayta ishlash mexanizmlarini qo'llash;

FTP va SFTP (SSL orqali) protokollari orqali uzatilayotgan ma'lumotlarni nazorat qilish va maxfiy fayllarni bloklash;

Tarmoq nazoratini amalga oshirishda proksi-server, ICAP, SPAN/TAP, pochta shlyuzi yoki boshqa qo'llab-quvvatlanadigan integratsiya mexanizmlaridan foydalanish;

Agent, MAPI, SMTP/SMTPS protokollari, pochta serveri yoki shlyuzi bilan integratsiya qilish yoxud boshqa teng qiymatli (ekvivalent) usullar orqali elektron xatlar va ularga birlashtirilgan fayllarni to'liq nazorat qilish;

Windows operatsion tizimidagi foydalanuvchilar harakatlarini majburiy nazorat qilish; macOS va Linux operatsion tizimlari uchun mavjud funksional imkoniyatlar va cheklovlar ishlab chiqaruvchining moslik matritsasida (*compatibility matrix*) aks ettirilishi kerak;

Taklif etilayotgan konfiguratsiya imkoniyatlari doirasida desktop va veb-muhitda ishlovchi amaliy dasturlar hamda xizmatlarni nazorat qilish va qamrab olish;

Messenjerlar, ijtimoiy tarmoqlar va korporativ aloqa vositalari orqali uzatilayotgan matn hamda fayllarni nazorat qilish. Telegram, WhatsApp, Viber, Zoom, Microsoft Teams, Discord, Signal va boshqa nomlar funksional toifaga misol sifatida keltirilgan; ijrochi mahsulot versiyasi, operatsion tizim va amaliy dastur turi (lokal/veb) bo'yicha aniq qo'llab-quvvatlash matritsasini (*support matrix*) taqdim etishi shart;

Istisnolarni sozlash hamda maxfiy hisoblanmaydigan yoki xavfsizlik siyosatlarini buzmaydigan ma'lumotlarning qonuniy uzatilishini asossiz ravishda bloklanishiga yo'l qo'ymaslik imkoniyatini ta'minlash;

Tarmoqdagi lokal printerlar orqali maxfiy fayllarni chop etish urinishlarini nazorat qilish hamda mahsulot imkoniyatlaridan kelib chiqqan holda ro'yxatga olish, ogohlantirish yoki bloklash choralari qo'llash;

Bluetooth, AirDrop, Wi-Fi Direct va boshqa simsiz ulanishlar orqali ma'lumotlarni uzatishni nazorat qilish yoki qurilma yo bo'lmasa interfeysdan foydalanishni cheklash imkoniyatlari mavjud bo'lganda, ushbu imkoniyatlar alohida ko'rsatilishi kerak; ushbu kanallarni qo'llab-quvvatlash barcha operatsion tizimlar uchun majburiy hisoblanmaydi;

Agent, veb-nazorat yoki integratsiya mexanizmlari orqali bulutli xotira xizmatlari hamda fayl almashish platformalariga (shu jumladan Google Drive, OneDrive, Dropbox,

Yandex Disk va boshqalarga) maxfiy ma'lumotlar yuborilishini aniqlash va ularni xavfsizlik siyosatiga muvofiq cheklash;

Tizimi tomonidan qo'llab-quvvatlanadigan mexanizm orqali brauzer, lokal (desktop) amaliy dasturlar yoki API vositasida sun'iy intellekt hamda generativ AI (GenAI) servislariga (shu jumladan ChatGPT, Gemini, Copilot, Claude va boshqalarga) yuborilayotgan matn, hujjat va boshqa kontentni tahlil qilish hamda cheklash; nazorat qilinadigan AI servislarining aniq ro'yxati tijorat taklifida ko'rsatib o'tilishi kerak;

Masofaviy boshqaruv va jamoaviy ishlash dasturlarida (shu jumladan TeamViewer, AnyDesk, Microsoft Teams, Zoom va boshqalarda) mahsulot imkoniyatlari doirasida fayllar uzatilishini, bufer almashinuvini (clipboard) hamda boshqa ma'lumot uzatish kanallarini nazorat qilish; agar to'liq bloklash imkoni bo'lmasa, aniqlash va ro'yxatga olishning ekvivalent choralari ko'rsatilishi kerak.

41. Tizimda administratori Tizimda mavjud namunalar (shablonlar) asosida turli foydalanuvchi rollari va ularning vakolatlarini belgilash imkoniyatiga ega bo'lishi lozim. Rollarning nomlanishi ishlab chiquvchiga (ishlab chiqaruvchiga) bog'liq bo'lishi mumkin, biroq kamida quyidagi funksiyalarni o'zaro ajratish imkoniyati nazarda tutilgan bo'lishi shart:

“Tizim administrator” – Tizim faoliyatini, uning komponentlarini, zaxira nusxalash (backup) jarayonlarini va texnik sozlamalarini boshqarish;

“Auditor” yoki “Rahbariyat vakili” – hisobotlarni hamda umumlashtirilgan ma'lumotlarni faqat taqdim etilgan vakolatlar doirasida ko'rib chiqish;

“Axborot xavfsizligi xodimi” – xavfsizlik siyosatlarini, xavfsizlik hodisalarini (insidentlarni) hamda xizmat tekshiruvlarini boshqarish.

42. Tizim administratorni muhim hodisalar, shu jumladan siyosat sozlamalariga o'zgartirish kiritilishi, tizim nosozliklari va boshqa hodisalar haqida elektron pochta, konsol yoki boshqa sozlanadigan kanallar orqali avtomatik ravishda xabardor qilishni ta'minlashi lozim.

43. Tizimda oldindan belgilangan xavfsizlik siyosati sozlamalari (jumladan, DLP qoidalari va ma'lumotlar bilan ishlashga doir cheklovlar) buzilgan holatlarda quyidagi javob choralari ko'rish imkoniyati mavjud bo'lishi:

Xavfsizlik siyosati buzilgan taqdirda, Tizim administratoriga elektron pochta yoki boshqa sozlangan kanal orqali avtomatik ravishda insidentga oid asosiy ma'lumotlarni (siyosat nomi, qoidani buzgan foydalanuvchi, aniqlangan ma'lumot turi, sana va vaqt, shuningdek, imkoniyatga qarab, konsolda insidentni ochish uchun identifikator yoki havolani) o'z ichiga olgan xabarnoma yuborilishi lozim.

Tizimda xabarnomalarni yuborish parametrlarini sozlash (insident aniqlanganda darhol yoki belgilangan vaqt oralig'ida to'plangan holda yuborish), konsol orqali tanlangan xavfsizlik siyosatlari bo'yicha barcha insidentlarni ko'rish hamda ularni saqlash imkoniyati mavjud bo'lishi.

insident tafsilotlarini ko'rish sahifasida qoidani buzgan foydalanuvchi, insident sanasi va vaqti hamda insidentga sabab bo'lgan hujjat yoki ma'lumot turi aks ettirilish.

4. Tizimdagi hisobotlar va monitoringga oid talablar

44. Standart hisobotlar to'plami asosida hisobotlarni shakllantirish, shuningdek filtrlar, maydonlar, davr va guruhlash mezonlarini sozlash orqali yangi hisobotlarni yaratish imkoniyati nazarda tutilgan bo'lishi lozim. Tayyor shablonlar soni mahsulot arxitekturasiga bog'liq bo'lishi mumkin va tijorat taklifida ko'rsatib o'tilishi kerak:

hisobotlarni quyidagi formatlarda taqdim etish:

jadval (table);

"Gistogramma";

"Diagramma" (chiziqli, doira, nuqtaviy) ko'rinishlarda;

foydalanuvchilar faolligi va Tizim siyosati buzilishi bilan bog'liq insidentlar bo'yicha statistikani yig'ish va hisobotlar generatsiyasi.

45. Tizim va agentlarning holati to'g'risidagi hisobotlar, shuningdek, taklif etilayotgan konfiguratsiyada inventarizatsiya funksiyasi mavjud bo'lgan taqdirda, dasturiy ta'minotning quyidagi ko'rsatkichlari bo'yicha ma'lumotlar:

o'rnatilgan va o'chirilgan dasturlar soni (agar inventarizatsiya moduli nazarda tutilgan bo'lsa);

agent o'rnatish/o'chirish statistikasi;

belgilangan dasturlar o'rnatilgan yoki mavjud bo'lmagan ishchi stansiyalar ro'yxati (agar ushbu funksiya qo'llab-quvvatlansa);

Ishchi stansiyalardagi dasturiy ta'minotning o'zgarishlar tarixi (agar ushbu funksiya qo'llab-quvvatlansa);

Foydalanuvchilarning ishchi stansiyalarida o'rnatilgan ichki qurilmalar hamda ulangan tashqi qurilmalar bo'yicha hisobotlarni shakllantirish (agar qurilmalarni nazorat qilish yoki inventarizatsiya moduli taklif etilgan bo'lsa).

46. Quyidagi ma'lumotlar asosida tizim holati haqida hisobotlar:

agentlar/protokollar bilan bog'liq barcha harakatlar (istalgan yoki ko'rsatilgan foydalanuvchi bo'yicha);

agentlar o'chirilgan kompyuterlar ro'yxati;

belgilangan vaqt oralig'ida agent aloqasi bo'lmagan kompyuterlar;

umuman agent mavjud bo'lmagan kompyuterlar ro'yxati;

belgilangan kompyuterlarda ma'lum davrda yuborilgan xabarlar soni;

hisobotlar o'rtasida bog'langan o'tish (navigatsiya) imkoniyati mavjud bo'lishi;

tanlangan foydalanuvchi qaysi manzillardan xabar yuborgan yoki olganligini aniq ko'rish imkoniyati taqdim etilishi;

hisobotlarni "PDF", "XLS" ("Excel"), "CSV", "TXT" va boshqa formatlarda Tizimdan yuklash, (saqlash, eksport qilish) va chop etish (print) imkoniyati bo'lishi.

Insidentlarga tegishli ekran tasvirlari (screenshotlari)ni olish yoki hodisaga oid boshqa dalillarni saqlab qolish;

Ekran tasvirlari (screenshotlar) moduli taklif etilgan taqdirda, tasvirlarning sifati, formati hamda olinish davriyligini (chastotasini) sozlash imkoniyati nazarda tutilgan bo'lishi lozim; ushbu funksiya barcha mahsulotlar uchun majburiy hisoblanmaydi.

47. Server komponentlari faoliyati haqidagi barcha muhim hodisalarni operatsion tizim jurnalida qayd etish.

48. Tizim konsoli orqali hodisalar jurnalini ko'rish, har bir hodisa bo'yicha batafsil ma'lumot va tavsiyalarni shakllantirish imkoniyati mavjud bo'lishi.

49. Jurnal bo'yicha quyidagi mezonlar asosida filtrlash imkoniyati bo'lishi:

ish stansiyasi;

server komponenti;

hodisa darajasi;

sana va vaqt;

muayyan ish stansiyalar bo'yicha monitoring yuritish imkoniyati;

yangi server hodisalari aniqlanganda administratorni avtomatik tarzda xabardor qilish (konsol va e-mail orqali yoki boshqa alternativ yechim);

"E-mail" orqali yuboriladigan xabarnomalarni sozlash;

qabul qiluvchi manzilni tanlash.

5. Tizimning ishonchliligi

50. Buyurtmachining boshqa dasturlarining ishlashiga salbiy ta'sir ko'rsatmasligi.

51. Tizim nosozligi yoki dasturiy ta'minoti xatoligi yuzaga kelganda, uning ishchi holatini tiklash imkoniyati bo'lishi.

52. Tizim Buyurtmachi tomonidan taqdim etilgan hisoblash resurslarida 24/7 rejimida uzluksiz ishlashga mo'ljallangan tegishli arxitekturaga hamda zaxiralash va tiklash mexanizmlariga ega bo'lishi lozim.

53. Ishchi stansiyalardagi Tizim agenti ishlab chiqaruvchi tomonidan qo'llab-quvvatlanadigan xizmat (service), drayver, yadro (kernel) yoki foydalanuvchi rejimi (user mode) mexanizmlaridan foydalanishi mumkin. Tanlangan usul operatsion tizimning barqarorligi va xavfsizligiga salbiy ta'sir ko'rsatmasligi lozim.

54. Agent foydalanuvchi tomonidan o'chirilmasligi yoki to'xtatilmasligi uchun himoyalangan bo'lishi.

55. Tarmoq va apparat resurslariga tushadigan yuklamani optimallashtirish, zarurat tug'ilganda esa komponentlarni ajratish yoki yuklamani taqsimlash imkoniyati nazarda tutilgan bo'lishi lozim.

6. Ijrochiga qo'yiladigan talablar

56. Kiberxavfsizlik to'g'risidagi va MAI obyektlari kiberxavfsizligini ta'minlashga oid amaldagi qonunchilik (PQ-764 va PQ-167) talablariga muvofiq, taklif etilayotgan mahsulot va/yoki uning modifikatsiyalari sertifikatlash shartlariga javob berishi kerak. Agar taklif etilayotgan versiya bo'yicha amaldagi sertifikat mavjud bo'lmasa, Ijrochi tender bosqichida mahsulotning sertifikatlashdan o'tish imkoniyatini tasdiqlovchi hujjatlarni (avvalgi versiyalarining sertifikatlari yoki sertifikatlash organiga berilgan ariza) hamda **ishlab chiqaruvchi va/yoki Ijrochi tomonidan belgilangan muddat ichida muvofiqlik sertifikatini o'z hisobidan olib berish bo'yicha yuridik kuchga ega bo'lgan Rasmiy**

Kafillik/Kafolat xatini taqdim etishi shart. Sertifikatlash jarayonining davomiyligi inobatga olingan holda, amaldagi sertifikat Tizimni joriy etish va ekspluatatsiya qilish davrida Ijrochi tomonidan taqdim etilishi lozim.

57. Ijrochi yoki taklif etilayotgan mahsulotni ishlab chiquvchi axborot xavfsizligi sohasida kamida 5 (besh) yillik umumlashgan amaliy ish tajribasiga ega bo'lishi lozim.

58. Ijrochi, dasturiy ta'minotni ishlab chiquvchi (vendor) yoki ularning rasmiy hamkori kamida 2 (ikkita) analogik shartnoma bo'yicha DLP-tizimlari litsenziyalarini yetkazib berish va texnik qo'llab-quvvatlash bo'yicha amaliy tajribasini tasdiqlashi lozim. Kamida bitta shartnoma bank yoki moliya tashkiloti bilan tuzilgan bo'lishi maqsadga muvofiqdir. O'zbekiston Respublikasidagi amaliy ish tajribasi afzallik sifatida baholanadi, biroq boshqa mamlakatlardagi shunga o'xshash (tenglashtirilgan) tajriba ham inobatga olinadi.

59. Ijrochi O'zbekiston Respublikasida mahalliy ofisiga yoki ishlab chiquvchining rasmiy vakolatli servis hamkoriga, shuningdek zarurat tug'ilganda obyektga bevosita borib xizmat ko'rsatish imkoniyatiga ega bo'lgan texnik mutaxassislariga ega bo'lishi lozim.

60. Ijrochi DLP tizimi muallifi yoki uning rasmiy distribyutori tomonidan sertifikatlangan bo'lishi.

7. Maxfiylik

61. Ijrochi Kompaniyaga tegishli barcha ma'lumotlarning maxfiyligini ta'minlashi shart. Ushbu ma'lumotlar faqat ushbu texnik topshiriq doirasida foydalanilishi mumkin hamda Kompaniyaning yozma rozilgisiz uchinchi shaxslarga berilishi, muhokama qilinishi yoki tarqatilishi taqiqlanadi. Mazkur majburiyat shartnomaning amal qilish muddati davomida hamda u tugagandan keyin ham o'z kuchida qoladi. O'zbekiston Respublikasi qonunchiligida nazarda tutilgan hollar bundan mustasno.

62. Maxfiy hujjatlar va ma'lumotlarni saqlash talablari:

Ijrochi maxfiy hujjatlarni faqat himoyalangan (shifrlangan) vositalarda saqlanishi;

Ijrochi xizmat muddati tugaganidan so'ng 30 kun ichida maxfiy hujjatlarni butunlay yo'q qilishi yoki Buyurtmachiga topshirishi;

ma'lumotlarning noqonuniy oshkor qilinishi aniqlangan taqdirda, Ijrochi Buyurtmachiga bu haqda 24 soat ichida xabar berishi va zarur choralarni ko'rishi.

8. Texnik qo'llab-quvvatlash va litsenziyalashga qo'yiladigan talablar

63. Tizim ishlab chiquvchining va Ijrochining texnik qo'llab-quvvatlovi **Tizim amaliyotga to'liq joriy etilib, foydalanishiga topshirish dalolatnomasi ikki tomonlama imzolangan sanadan e'tiboran to'liq 12 (o'n ikki) oy davomida** taqdim etilishi lozim (*3 oylik joriy etish davri ushbu 12 oylik servis muddatiga kirmaydi*). Oddiy murojaatlar uchun kamida 8x5 rejimida masofaviy texnik qo'llab-quvvatlash, kritik nosozliklar uchun esa ariza berish tizimi (ticket system), elektron pochta, portal yoki telefon orqali 24/7 rejimida murojaatlarni tunu kun qabul qilish va bartaraf etish imkoniyati taqdim etilishi kerak.

64. Zarurat bo'lganda obyektga bevosita borib (on-site) texnik qo'llab-quvvatlash imkoniyati nazarda tutilgan bo'lishi lozim. Agar bunday tashrif bazaviy texnik qo'llab-

quvvatlash paketiga kirmasa, uning shartlari va qiymati tijorat taklifida alohida ko'rsatib o'tilishi shart.

65. Texnik qo'llab-quvvatlash bevosita Tizimni ishlab chiquvchi (vendor) tomonidan taqdim etilishi lozim. Ijrochi Buyurtmachiga 1 (bir) yil davomida ishlab chiquvchining qo'llab-quvvatlash xizmatiga murojaat qilish, maslahatlar olish, xatolarni tuzatish (bug fixes), xavfsizlik yangilanishlari, litsenziyalangan barcha komponentlarning yangi qo'llab-quvvatlanadigan versiyalarini olish uchun amaldagi huquqni ta'minlashi shart. Ijrochi qo'llab-quvvatlashning birinchi liniyasi (1-level support) vazifasini bajarishi mumkin, biroq murojaatlarni bevosita ishlab chiquvchiga eskalatsiya qilishni (yo'naltirishni) ta'minlashga majburdir.

66. Texnik qo'llab-quvvatlash xizmat ko'rsatish darajasi to'g'risidagi kelishuv (SLA) asosida taqdim etilishi lozim: murojaatni qabul qilish va P1 (Critical) kritik insidenti bo'yicha dastlabki javob berish vaqti — 2 soatdan oshmasligi, P2 (High) yuqori ustuvorlikdagi insident bo'yicha — 4 ish soatidan oshmasligi, o'rta va past ustuvorlikdagi murojaatlar bo'yicha esa — 1 ish kunidan kechiktirmay amalga oshirilishi shart. Nosozlikni bartaraf etish muddati insidentning murakkabligi hamda ishlab chiquvchi (vendor) bilan kelishilgan harakatlar rejasi hisobga olingan holda belgilanadi.

67. Tijorat taklifi tarkibiga 1 (bir) yil muddatga quyida keltirilgan talablarning bajarilishini ta'minlaydigan hajmda Tizim litsenziyalari hamda butun litsenziyalangan hajm uchun ishlab chiquvchining (vendoring) 1 (bir) yil muddatga mo'ljallangan texnik qo'llab-quvvatlovi kiritilishi lozim.

68. Tizim kamida 75 ta fizik yoki virtual foydalanuvchi ish o'rinlarida litsenziyalangan tarzda foydalanishni hamda ko'rsatilgan qurilmalarning barcha foydalanuvchilarini to'liq nazorat qilish imkoniyatini ta'minlashi lozim.

69. Tizim kamida 75 ta korporativ hisob yozuvlari (account) va elektron pochta qutilarining nazorat qilinishini ta'minlashi lozim.

70. Litsenziyalash tarkibiga e'lon qilingan funksionalning to'liq ishlashi uchun zarur bo'lgan barcha server komponentlari, ma'lumotlar bazalari, boshqaruv konsollari, indeksatsiyalash, OCR (optik belgilarni tanish), pochta integratsiyasi hamda boshqa barcha modullar kiritilishi shart.

71. Tizim har bir fizik gipervizor yoki ma'lumotlarni saqlash tizimi (MST/CXD) uchun alohida litsenziyalar sotib olish zaruratisiz, virtual infratuzilmada joylashtirilgan fayl serverlari va tarmoq fayl resurslarida saqlanayotgan ma'lumotlarning nazorat qilinishini ta'minlashi lozim.

72. Server operatsion tizimlarini agent orqali nazorat qilish ko'zda tutilgan holatda, Ijrochining taklifi kamida 20 ta tanlangan Windows/Linux virtual serverlariga agentlarni o'rnatish huquqini o'z ichiga olishi yoki Ijrochi ushbu kengaytirish narxini tijorat taklifida alohida ko'rsatishi shart.

73. Litsenziyalash hech qanday qo'shimcha yashirin to'lovlarsiz, Tizimning server komponentlarini kamida ikkita virtual serverda, shu jumladan asosiy va zaxira (rezerv) installatsiyalarida joylashtirish imkoniyatini ko'zda tutishi shart.

74. Ijrochi amalda qo'llaniladigan litsenziyalash metrikasini ko'rsatilgan parametrlar bo'yicha alohida ko'rsatishi shart: foydalanuvchi, kompyuter, ish o'rni, server, pochta manzili, ma'lumotlar hajmi, fayl xotirasi, tarmoq tuguni yoki server komponenti.

75. Litsenziyalarni ulardan foydalanish huquqini tasdiqlovchi hujjatlarni hamda Tizimni ishlab chiquvchining (vendorning) texnik qo'llab-quvvatlovini tasdiqlovchi hujjatlarni yetkazib berish shartnoma tuzilgan sanadan e'tiboran 1 (bir) oy muddatda amalga oshirilishi lozim. Litsenziyalar va texnik qo'llab-quvvatlashning amal qilish muddati **to'liq 12 (o'n ikki) oyni tashkil etishi hamda Tizim amaliyotga to'liq joriy etilib, foydalanishiga topshirish dalolatnomasi imzolangan sanadan boshlanishi shart.**

76. Yetkazib berish tarkibida Ijrochi Tizimdan foydalanish va texnik qo'llab-quvvatlash xizmatiga murojaat qilish uchun zarur bo'lgan Tizimni ishlab chiquvchining (vendorning) rasmiy texnik hujjatlarini taqdim etishi shart: foydalanuvchi qo'llanmasi (User Guide), administrator qo'llanmasi (Administrator Guide), Tizim arxitekturasini tavsifi (Architecture Document), ekspluatatsiya yo'riqnomasi (Operation Manual), SLA hujjati yoki texnik qo'llab-quvvatlash reglamenti (Support/SLA), qo'llab-quvvatlanadigan operatsion tizimlarning moslik matritsasi (Compatibility Matrix) hamda xavfsizlik siyosatlari tavsifi (Security Policy Description).

9. Litsenziyalarning muvofiqligini tasdiqlash va qabul qilish tartibi

77. Ijrochi tender taklifi tarkibida ushbu Texnik topshiriqning har bir punkti bo'yicha "to'liq mos keladi / qisman mos keladi / mos kelmaydi / qo'shimcha modul talab qilinadi" formatidagi Muvofiqlik matritsasini (Compliance Matrix), Tizimni ishlab chiquvchining (vendorning) rasmiy hujjatlariga havolalarni hamda talab qilinadigan litsenziyalarning to'liq ro'yxatini taqdim etishi shart.

78. Shartnoma tuzilgunga qadar yoki litsenziyalar yakuniy qabul qilib olgunga qadar **Ijrochi Buyurtmachi talabiga ko'ra Tizimning majburiy funksiyalarini kamida 5 (besh) ta ish o'rnida namoyish etishi (Demo) yoki pilot sinovdan o'tkazishi (PoC) majburiy hisoblanadi.** Sinov ssenariylari elektron pochta, veb-servislar yoki sun'iy intellekt (AI) servislar, USB-xotiralar, printer, messenjerlar hamda ushbu xarid uchun muhim deb topilgan boshqa kanallarni, shuningdek, agentning tizimga tushiradigan yuklamasini (CPU/RAM load), hodisalar arxivini hamda hisobotlar shakllanishini qamrab olishi lozim. Agar shartnoma amal qilish davrida (12 oy davomida) Buyurtmachining ish o'rinlari (shtat) soni 75 tadan oshib ketsa, Ijrochi qo'shimcha talab qilingan litsenziyalarni ushbu shartnomada **dastlab kelishilgan bir birlik litsenziya narxida** yetkazib berish majburiyatini oladi.

79. Ushbu texnik topshiriqda belgilangan natijani boshqa arxitektura, modul nomi yoki texnologik mexanizm orqali ta'minlaydigan ekvivalent (muqobil) yechimlar qabul qilinadi. Ekvivalentlik Ijrochi tomonidan Tizimni ishlab chiquvchining (vendorning) rasmiy hujjatlari, Muvofiqlik matritsasi hamda, Buyurtmachi tomonidan tekshiruv o'tkazilgan taqdirda, namoyish etish (Demo) yoki pilot sinov (PoC) natijalari bilan tasdiqlanishi shart.

10. Loyihani amaliyotga joriy etish tartibi va muddatlari

80. Tizimni to'liq amaliyotga joriy etish, sinovdan o'tkazish va sanoat foydalanishiga topshirishning umumiy muddati — shartnoma imzolangan vaqtdan boshlab **3 (uch) kalendar oyini** tashkil etadi. Sanoat foydalanishiga topshirish dalolatnomasi imzolanganach, 63 va 75-bandlarda ko'rsatilgan 12 (o'n ikki) oylik kafolatli texnik qo'llab-quvvatlash va litsenziya davri kuchga kiradi.

81. Ijrochi 3 oylik muddat ichida quyidagi bosqichlarni bosqichma-bosqich va jadvalga muvofiq amalga oshirishi shart:

T/r	Bosqich	Bajariladigan ishlar mazmuni	Bajarish muddati
1.	1-bosqich	Tizim arxitekturasini loyihalash, server va agent qismlarini o'rnatish, Active Directory va boshqa infratuzilmalar bilan integratsiya qilish.	1-oy (1–30-kunlar)
2.	2-bosqich	Xavfsizlik siyosatlarini (Policy) sozlash, test rejimida ishlatish, soxta pozitiv (False Positive) hodisalarni filtrlash va xodimlarni o'qitish.	2-oy (31–60-kunlar)
3.	3-bosqich	Tizimni amaliyotga to'liq joriy qilish, muvofiqlik sertifikatini (yoki sinov natijalari bo'yicha yakuniy hujjatlarni) taqdim etish hamda amaliyotga joriy qilish dalolatnomasini imzolash.	3-oy (61–90-kunlar)

Tasdiqladi:

Bosh ijrochi direktor



M.Farmanov

Kelishildi:

IT va raqamlashtirish bo'limi
boshlig'i



D.Alpeyev

Komplayens bo'limi boshlig'i



B.Astanov

Yuridik bo'lim boshlig'i



A.Egamberdiyev

Risklarni boshqarish bo'limi
boshlig'i



D.Toshpulatov

Xaridlar menejeri



K.Jumayeva

Kiritdi:

*Axborot xavfsizligi bosh
mutaxassisi*

U.Teshayev

Tel: (ichki: 134)

