“TASDIQLAYMAN”

“Agrobank” ATB

Boshqaruv raisi o'rinbosari v.b.



F.B.Nasriyev

2026 yil “24” noyabr

«Agrobank» ATB uchun ofis faoliyatini nazorat qilish va ma’lumotlar sizib chiqishining oldini olish (DLP) tizimidan foydalanish huquqlarini xarid qilish, joriy etish va sozlash bo‘yicha

TEXNIK TOPSHIRIQ

Toshkent – 2026

MUNDARIJA

QISQARTMALAR RO‘YXATI **3**

UMUMIY MA’LUMOTLAR VA LOYIHANI TASHKIL ETISH **3**

1. Yetkazib berishning maqsadi **3**

2. Tizimga qo‘yiladigan umumiy talablar **3**

2.1. Tizim arxitekturasi va tarkibiy qismlari 3

2.2. Integratsiya va moslik 4

2.3. Xavfsizlik va kirishni boshqarish 5

2.4. Hisobot va ma’lumotlarni saqlash 6

3. Ma’lumotlarni saqlash va qidirish funksiyalariga talablar **6**

4. Ekspluatatsiya hujjatlariga talablar **7**

5. Texnik qo‘llab-quvvatlash va o‘qitish talablari **7**

5.1. Texnik qo‘llab-quvvatlash 7

5.2. O‘qitish va hujjatlar 7

6. Monitoring tizimi **7**

6.1. Monitoring vazifalari 7

6.2. Monitoring funksiyalariga talablar 7

7. Yakuniy qurilmalar holati **8**

8. Fayllar bilan veb-amallar auditi **8**

9. Microsoft 365 va Google Workspace ma’lumotlarini himoyalash **8**

10. Xulq-atvor tahlili tizimi **9**

10.1. Vazifalar 9

10.2. Funksional talablar 9

11. Ilovalar va veb-saytlarni nazorat qilish siyosatlari **10**

12. Konfidensial ma’lumotlar sizib chiqishidan himoyalash tizimi (DLP) **10**

12.1. DLP vazifalari 10

12.2. DLP funksional talablari 10

13. Konfidensial ma’lumotlarni aniqlash imkoniyatlari **11**

13.1. Kontentga asoslangan tizim 11

13.2. Kontekstga asoslangan tizim 12

13.3. Fayl parametrlariga asoslangan tizim 12

13.4. Foydalanuvchi belgilaydigan ma’lumotlar tasnifi (teglar) 12

14. Ma’lumot uzatish kanallarini nazorat qilish (sizib chiqishdan himoya) **13**

14.1. Ma’lumot uzatish kanallari va manzillari 13

14.2. OCR ishlashiga talablar 16

14.3. AI vositalaridan foydalanishni nazorat qilish 16

15. Xavfsizlik siyosatlarini qo‘llab-quvvatlash **17**

16. Litsenziyalash **17**

17. Qurilmalarni boshqarish va mijozni joylashtirish **17**

18. Apparat va dasturiy ta’minotga talablar 18
18.1. Server 18
18.2. Xizmat konsoli 18
18.3. Veb-boshqaruv konsoli 18
18.4. Windows ish stansiyalari 18
18.5. macOS ish stansiyalari 18
19. Ehtimoliy yetkazib beruvchiga talablar 19

QISQARTMALAR RO‘YXATI

DLP — Data Loss Prevention (ma’lumotlar sizib chiqishining oldini olish);

SOC — Security Operations Center (axborot xavfsizligini monitoring qilish markazi);

SIEM — Security Information and Event Management;

OCR — Optical Character Recognition;

AD — Active Directory;

API — Application Programming Interface;

MBBT — ma’lumotlar bazasini boshqarish tizimi;

TT — texnik topshiriq.

UMUMIY MA’LUMOTLAR VA LOYIHANI TASHKIL ETISH

Buyurtmachi: «Agrobank» ATB. Ijrochi (Yetkazib beruvchi): xarid tartib-taomillari yakuniga ko‘ra aniqlanadigan tashkilot. Ishlarni bajarish muddatlari va bosqichlari shartnomaga ilova qilinadigan, tomonlar kelishgan kalendar reja bilan belgilanadi.

Texnik topshiriq predmeti: 6 000 foydalanuvchiga mo‘ljallangan DLP tizimidan 36 oy foydalanish huquqini taqdim etish, tizimni Buyurtmachi infratuzilmasiga o‘rnatish, integratsiya qilish, sozlash, ishga tushirish, sinash va xodimlarni o‘qitish. Qo‘shimcha ishlar va xarajatlar shartnomada aniq ko‘rsatilishi lozim.

Ijrochi loyiha boshlanishidan avval Buyurtmachi bilan texnik loyiha, tarkibiy qismlarni joylashtirish sxemasi, integratsiyalar ro‘yxati, axborot xavfsizligi choralari, kalendar reja hamda qabul qilish sinovlari dasturini kelishishi kerak.

1. YETKAZIB BERISHNING MAQSADI

1.1 Ofis faoliyatini nazorat qilish va ma’lumotlar sizib chiqishining oldini olish (DLP) tizimini yetkazib berish va joriy etish quyidagi maqsadlarga erishishni ta’minlashi lozim:

- Konfidensial axborotning tashkilot tashqarisiga sizib chiqishi xavfini kamaytirish.

- Ichki firibgarlik alomatlarini va xodimlarning tashkilotga iqtisodiy zarar yetkazuvchi harakatlarini aniqlash.

- Tashkilotdagi axborot xavfsizligi hodisalari yuzasidan tekshiruvlar o‘tkazish.

- Korporativ axborot tarmog‘ida foydalanuvchilar harakatlarini to‘liq nazorat qilish.

- Shaxsga doir ma’lumotlar va axborot xavfsizligini himoya qilish sohasidagi qonunchilikka muvofiqlikni ta’minlash.

- Hodisalarni samarali monitoring va tahlil qilish orqali xavfsizlik hodisalariga javob berishni tezlashtirish.

2. TIZIMGA QO‘YILADIGAN UMUMIY TALABLAR

2.1. Tizim arxitekturasi va tarkibiy qismlari

2.1.1. Mijoz-server arxitekturasi: tizim kengaytiriladigan va nosozliklarga bardoshli mijoz-server arxitekturasiga asoslanishi, barcha server qismlarini Buyurtmachi infratuzilmasida mahalliy (on-premises) joylashtirish imkonini berishi kerak; barcha ma’lumotlar, jurnallar va sozlamalar faqat Buyurtmachi infratuzilmasida saqlanishi shart.

2.1.2. Yagona ishlab chiqaruvchi: tizimning barcha tarkibiy qismlari bitta huquq egasiga tegishli bo‘lishi kerak.

2.1.3. Versiya: Yetkazib beruvchi yetkazib berish sanasida ishlab chiqaruvchi chiqargan dasturiy ta’minotning dolzarb versiyasini taqdim etishi kerak. Shuningdek, yangilanishlar joriy litsenziya amal qilish qilish muddatidagi yangi chiqarilgan dasturiy mahsulot versiyasini o‘z ichiga olishi lozim.

2.1.4. Tizim tarkibi quyidagi qismlarni o‘z ichiga olishi shart:

– Server xizmati: alohida serverda xizmat sifatida ishlashi hamda mijoz dasturlari, ma’lumotlar bazasi va boshqaruv konsoli o‘rtasidagi o‘zaro aloqani ta’minlashi kerak;

– Veb-konsol: qo‘shimcha dastur o‘rnatmasdan brauzer orqali ishlaydigan asosiy boshqaruv interfeysi bo‘lishi; monitoring paneli, insaytlar, ma’lumotlar bilan amallar, ilovalar, saytlar va tashqi qurilmalar auditi, xulq-atvor tahlili, siyosatlar, ma’lumotlar tasnifi va manzillari, foydalanuvchi va qurilmalarni boshqarish, hisobotlar, integratsiyalar hamda sozlamalarni qamrab olishi kerak;

– Xizmat ko‘rsatish konsoli: ogohlantirish qoidalari, SMTP va syslog parametrlari, Active Directory bilan sinxronlash, mijozning o‘zini himoyalash parametrlari hamda diagnostik ma’lumotlarni yig‘ish kabi xizmat funksiyalarini ta’minlashi kerak;

– Mijoz dasturi: Windows va macOS ish stansiyalari hamda serverlariga o‘rnatilishi, asosiy audit va himoya funksiyalarini bajarishi; to‘liq mijozni yuklab olib o‘rnatuvchi yengil agent-o‘rnatuvchi ham bo‘lishi kerak;

– Ma’lumotlar bazasi: tizim MS SQL Server MBBTdan foydalanishi shart.

2.1.5. Yangilash: server qismi va mijoz dasturlarini veb-konsoldan yangilash; server yangilanayotganda mijozlarning qurilmalarni himoyalashda davom etishi; eskirgan mijozlarni konsolda belgilash va ommaviy yangilash imkoniyati ta’minlanishi lozim.

2.1.6. Interfeys tillari: konsol va yakuniy foydalanuvchiga bildirishnomalar rus tilida bo‘lishi qo‘llab-quvvatlanishi shart.

2.2. Integratsiya va moslik

SIEM va boshqa tizimlar (webhook) bilan integratsiya

2.2.1. Tizim barcha muhimlik darajasidagi insaytlar (hodisalar) va administrator harakatlari jurnalini webhook (HTTPS POST) orqali OCSF JSON formatida kiruvchi webhooklarni qabul qiluvchi istalgan tizimga, jumladan SIEM, arizalarni boshqarish tizimlari (masalan Jira), avtomatlashtirish platformalari (Microsoft Power Automate, n8n va boshqalar) va korporativ messenjerlarga (avtomatlashtirish vositalari orqali Microsoft Teams) yuborishi kerak; uzatiladigan hodisada ishga tushgan siyosat hamda bloklashni asosli chetlab o‘tishda foydalanuvchi ko‘rsatgan sabab aks etishi shart.

2.2.2. Tizim avtorizatsiya sarlavhalarini (qiymatlarini shifrlangan holda saqlagan holda) va ulanishni tekshirishni qo‘llashi; integratsiyani boshqarish faqat sozlash huquqiga ega administratorlar uchun ochiq bo‘lishi kerak.

2.2.3. Tizim xizmat ko‘rsatish konsoli ogohlantirishlarini syslog protokoli orqali yuborishi shart.

Microsoft Active Directory bilan integratsiya

2.2.4. Tizim bir vaqtning o‘zida kamida ikkita domen bilan sinxronlashni, sinxronlanadigan obyektlarni — tashkiliy birliklar (OU), bo‘limlar, xavfsizlik guruhlarini — tanlashni, davriy va qo‘lda sinxronlashni qo‘llashi kerak.

2.2.5. ADdan tashqaridagi qurilmalarda aniqlangan foydalanuvchilar avtomatik ravishda o‘z siyosatlari qo‘llanishi mumkin bo‘lgan alohida jamoaga kiritilishi kerak.

Microsoft 365 va Google Workspace bilan integratsiya

2.2.6. Microsoft 365 tenantini ulash, Microsoft Entra IDdan foydalanuvchilar va xavfsizlik guruhlarini sinxronlash, Microsoft Purview Information Protection konfidensiallik belgilarini import qilish ta’minlanishi shart.

2.2.7. Google Workspace tashkilotini foydalanuvchilar sinxronlanishi bilan ulash ta’minlanishi shart.

2.2.8. Bulutli xizmatlardagi ma’lumotlar 9-bo‘limga muvofiq himoyalanishi kerak.

Tizim quyidagi platforma va ilovalarni qo‘llashi lozim:

2.2.9. Windows: barcha xavfsizlik yangilanishlariga ega Windows 10 (64-bit, 22H2 va 21H2), Windows 11 (64-bit), Windows Server 2019 va yangiroq versiyalar.

2.2.10. macOS: macOS 12 va yangiroq versiyalar.

2.2.11. Brauzerlar (veb-faoliyat auditi va nazorati): kamida Microsoft Edge, Google Chrome, Mozilla Firefox, Safari, Opera, Yandex Browser.

2.2.12. Pochta mijozlari: kamida klassik Outlook 2016–2021, Windows uchun yangi Outlook, Outlook on the web, SMTP/POP3/IMAP mijozlari (Thunderbird va boshqalar), Apple Mail (macOS).

2.2.13. Messenjerlar: kamida Microsoft Teams, Slack, WhatsApp, Telegram, Viber, Facebook Messenger, Cisco Jabber.

2.2.14. Bulutli saqlash sinxronlash mijozlari: kamida OneDrive (shaxsiy va korporativ), SharePoint, Google Drive, Dropbox, Box.

2.2.15. Virtual va terminal muhitlari bilan moslik: tizim Citrix, Azure Virtual Desktop, Microsoft RDS terminal va VDI muhitlarida ishlashi hamda har bir foydalanuvchi sessiyasini alohida nazorat qilishi shart.

2.3. Xavfsizlik va kirishni boshqarish

Administrator hisob yozuvlari

2.3.1. Rollar: «Administrator» (to‘liq kirish), «Auditor» (faqat o‘qish), «Moslashtirilgan» (huquqlarni qo‘lda tanlash), shuningdek tanlangan jamoa/bo‘limlar doirasida huquqlarni cheklash.

2.3.2. Autentifikatsiya: mahalliy hisob yozuvi, Active Directory xavfsizlik guruhlari orqali kirish va provayderning ko‘p faktorli autentifikatsiyasidan foydalangan holda OpenID Connect orqali yagona kirish (SSO).

2.3.3. Parolni taxmin qilishdan himoya: kamida 12 belgili va murakkablik talablariga ega parol siyosati hamda ketma-ket muvaffaqiyatsiz kirish urinishlari haqida ogohlantirish.

2.3.4. Administrator harakatlari jurnali: konsoldagi barcha o‘zgarishlarni (siyosatlar, huquqlar, o‘chirish va boshqalar), o‘zgargan obyektning oldingi va keyingi holatini, faqat o‘zgargan parametrlarni alohida ko‘rsatish, obyekt va amal bo‘yicha filtrlash, XLSX eksporti va webhook orqali uzatishni ta’minlash.

Tizimning o‘zini himoyalashi

2.3.5. Yashirin rejim: mijoz jarayonlari va papkalari, shu jumladan mahalliy va domen administratoridan yashirilishi; yashirish va foydalanuvchiga bildirish rejimi markazlashgan boshqarilishi kerak.

2.3.6. To‘xtatish va o‘chirishdan himoya: mijozni to‘xtatish, o‘chirish, yangilash va qurilmadagi ulanishini o‘zgartirish faqat konsolda berilgan mahalliy administrator paroli bilan; mijozni o‘chirish va faolsizlantirish konsoldan bajarilishi; yakuniy foydalanuvchi mijozni to‘xtata yoki o‘chira olmasligi shart.

2.3.7. Sozlamalarni o‘zgartirishdan himoya: yakuniy qurilmadan sozlamalarni o‘zgartirishga yo‘l qo‘yilmasligi kerak.

2.3.8. Xavfsiz rejimda himoya: qurilma safe mode rejimida yuklanganda ham mijoz himoyasi ishlashi shart.

2.3.9. Avtonom rejim: qurilma korxona tarmog‘idan tashqari boshqa mahalliy tarmoq yoki internetga ulanganda funksiyalar saqlanishi; qaydlar qurilmada yig‘ilib, aloqa tiklanganda serverga yuborilishi kerak.

TLS tekshiruvi va himoya istisnolari

2.3.10. Tizim mijozning o‘z sertifikati bilan yakuniy qurilmada shifrlangan TLS 1.2/1.3 trafikni tekshirishi shart.

2.3.11. Sertifikatni tekshirishning kamida ikki rejimi: «mo‘tadil» (soxta, muddati o‘tgan, bekor qilingan sertifikatlarni bloklash) va «qat’iy» (qo‘shimcha ravishda o‘zi imzolagan va ishonchsiz sertifikatlarni bloklash).

2.3.12. Himoya istisnolari: ishonchli veb-saytlarni (domen, niqob, IP manzil, kichik tarmoq), tashqi qurilmalarni apparat identifikatori bilan hamda ilovalarni TLS tekshiruvidan istisno qilish.

2.3.13. Server sertifikati: server ↔ konsol ↔ mijoz ulanishlarini himoyalash uchun Buyurtmachining ishonchli sertifikatini import qilish.

2.4. Hisobot va ma’lumotlarni saqlash

Hisobotlar

2.4.1. Formatlar: umumlashtirilgan hisobotlarni PDF va DOCX, ma’lumotlar eksportini XLSX formatida tayyorlash.

2.4.2. Maketlar: konsol bo‘limlarining saqlangan ko‘rinishlari (filtrlar, ustunlar, guruhlash) bo‘yicha oldindan sozlangan va administrator yaratgan hisobotlar.

2.4.3. Avtomatik tarqatish: kamida har kuni, haftada, oyda va chorakda yuborish; foydalanuvchi/jamoa va tilni tanlash; istalgan e-mail manziliga havola yoki ilova ko‘rinishida yetkazish.

2.4.4. So‘rov bo‘yicha: istalgan davr uchun hisobot yaratish.

2.4.5. «Xavfsizlik auditi» hujjati: risklarni kamaytirish bo‘yicha xulosa va tavsiyalar bilan hujjat yaratish.

2.4.6. Jadvallar eksporti: istalgan bo‘lim jadvalini filtr va guruhlashni hisobga olgan holda XLSXga chiqarish.

Ma’lumotlarni saqlash

2.4.7. Hodisalar tarixini markazlashgan saqlash.

2.4.8. Boshqaruv serveri bilan aloqa bo‘lmaganda mijoz stansiyasida ma’lumotlarni saqlash.

2.4.9. Ma’lumotlar bazasini jadval bo‘yicha (oylik/choraklik/yarim yillik/yillik) va qo‘lda arxivlash, arxivlarni konsoldan ulash va ko‘rish.

2.4.10. Ma’lumotlar bazasi to‘lishi va diskda joy yetishmasligi haqida xizmat ogohlantirishlari.

2.4.11. Qaydlar va konfiguratsiyalarni o‘z ichiga olgan komponentlarning zaxira nusxasini olish.

Interaktiv monitoring paneli

2.4.12. Tizim axborot xavfsizligi va ma’lumotlar himoyasi holatini yagona oynada ko‘rsatishi, kamida so‘nggi 30 kunning quyidagi asosiy ko‘rsatkichlarini aks ettirishi shart:

– sabablari va dinamikasi bo‘yicha o‘rta va yuqori muhimlikdagi ochiq insaytlar;

– manzillar (xavfsiz, xavfli, belgilanmagan) va tasniflar bo‘yicha ma’lumotlar oqimi;

– eng ko‘p hodisa qayd etilgan foydalanuvchilar, shubhali va xizmatga aloqasiz faollik;

– ruxsat etilmagan generativ AI xizmatlariga fayl yuklashni aniqlagan holda AI vositalaridan foydalanish;

– joriy sozlamalarga asoslangan himoya darajasini oshirish tavsiyalari;

– har bir vidjetdan batafsil yozuvlarga o‘tish; administrator faqat o‘z vakolati doirasidagi ma’lumot va bo‘limlarni ko‘rishi.

3. MA’LUMOTLARNI SAQLASH VA QIDIRISH FUNKSIYALARIGA TALABLAR

3.1. Hodisalar tarixini markazlashgan saqlash.

3.2. Boshqaruv serveri bilan aloqa bo‘lmaganda mijoz stansiyalarida ma’lumotlarni saqlash.

3.3. MS SQL Server 2016 SP1 CU2 va yangiroq (jumladan Express) bazasini qo‘llash; tavsiya etilgan versiya — MS SQL Server 2025; Azure SQL ham qo‘llanishi kerak.

3.4. Qaydlarni davr, foydalanuvchilar/jamoalar/qurilmalar, manzil, fayl hajmi, siyosat amali, ilova, tasnif bo‘yicha filtrlash; filtrlarni bo‘limlar o‘rtasida saqlash.

3.5. Ustunlar (foydalanuvchi, ilova, manzil turi, tasnif, siyosat, amal) bo‘yicha jamlanmalar bilan guruhlash, saralash, ustunlar tarkibi va tartibini sozlash.

3.6. Batafsillashtirish va tekshiruv: fayl amallari tarixi hamda nusxa/o‘zgarishlarini kuzatish uchun yagona identifikatorga ega karta; ishga tushgan tasnif va qoidalar, mosliklar soni (shaxsga doir ma’lumot qiymatini oshkor etmasdan); qayd, foydalanuvchi, siyosat va tasnif o‘rtasida o‘tishlar.

3.7. Har bir qayd tarkibi: foydalanuvchi, ilova, manba va manzil, tasnif, ishga tushgan siyosat va amal (ruxsat/jurnal/bildirish/bloklash/asosli chetlab o‘tish), kontent tahlili holati, soyali nusxa mavjudligi.

4. EKSPLUATATSIYA HUJJATLARIGA TALABLAR

4.1. Dasturiy ta’minotning ekspluatatsiya hujjatlari kamida foydalanuvchi (administrator) qo‘llanmasi va masofaviy boshqarish vositalari administratori qo‘llanmasidan iborat bo‘lishi lozim. Ular dasturiy ta’minotni o‘rnatish, sozlash va ishlatish tartibini batafsil yoritishi shart.

5. TEXNIK QO‘LLAB-QUVVATLASH VA O‘QITISH TALABLARI

5.1. Texnik qo‘llab-quvvatlash

5.1.1. O‘zbekiston Respublikasining butun hududida yoki tashqarisida ishlab chiqaruvchining sertifikatlangan mutaxassislari rus yoki davlat tilida e-mail, internet va telefon orqali tunu kun yordam ko‘rsatish imkoniga ega bo‘lishi kerak.

5.1.2. O‘zbekiston Respublikasidagi ishlab chiqaruvchining rasmiy vakili ish kunlari va ish soatlarida davlat hamda rus tillarida texnik yordam ko‘rsatishi shart.

5.1.3. Texnik qo‘llab-quvvatlash muddati joriy litsenziyaning amal qilish muddati bilan mutanosib bo‘lishi shart.

5.2. O‘qitish va hujjatlar

5.2.1. Ijrochi Buyurtmachining kamida 2 nafar administrator/mutaxassisiga amaliy yo‘riqnoma o‘tkazishi, arxitektura, siyosatlar, hodisalarni tekshirish, zaxiralash va tiklash, nosozliklarni diagnostika qilishni qamrab olishi hamda ishtirokchilar va natijalar bo‘yicha tasdiqlovchi hujjat taqdim etishi lozim.

5.2.2. O‘quv materiallari: qo‘llanmalar, videodarslar va ma’lumotnomalar.

5.2.3. Vebinar va treninglar: administratorlar va foydalanuvchilar uchun onlayn o‘quv mashg‘ulotlari.

5.2.4. Maslahatlar: tizimni sozlash va optimallashtirish bo‘yicha ekspert yordami.

6. MONITORING TIZIMI

6.1. Monitoring vazifalari

6.1.1. Saqlanayotgan konfidensial ma’lumotlarni (data at rest) aniqlash.

6.1.2. Hujjatlarni chop etish kanallaridan foydalanishni monitoring qilish.

6.1.3. Xodimlar harakatlarini monitoring qilish.

6.1.4. Axborot xavfsizligi voqealari va hodisalarini boshqarishni avtomatlashtirish.

6.2. Monitoring funksiyalariga talablar

6.2.1. Audit siyosatlari: administrator belgilangan foydalanuvchi va jamoalar uchun qayd qilinadigan faollik turlarini — ilovalar, tashqi qurilmalar, e-mail, fayl amallari, chop etish, veb-saytlarni — tanlashi kerak.

6.2.2. Ish stansiyalaridagi xodimlar harakatlari: ilovalarni ishga tushirish va foydalanishni kuzatish, faollik/harakatsizlik vaqtini hisoblash; korporativ fayl resurslarini nazorat qilish; xodimlar haqidagi ma’lumotlarni yig‘ish; ichki tahlil vositalari asosida faollik profilini shakllantirish.

6.2.3. Fayl amallari auditi: yaratish, ochish, nusxalash, saqlash joylari o‘rtasida ko‘chirish, brauzerdan yuklab olish/yuklash, e-mail va messenjerlarda yuborish, tashqi qurilma/tarmoq/bulutga nusxalash, chop etish, o‘chirish, AI yordamchilari va Git repozitoriyalariga yuborishni qayd etish; manba va manzil turi (mahalliy disk, tashqi qurilma, veb-manzil, bulut, veb-pochta, tarmoq yo‘li, printer va boshqalar), yo‘li/URL va qurilma identifikatorini aniqlash.

6.2.4. Aloqa auditi: qo‘llaniladigan messenjerlarning ilova va veb-versiyalari orqali fayl jo‘natish; har qanday pochta xizmatining veb-interfeysi orqali yuborilgan ilovalarni qayd qilish.

6.2.5. Chop etishni nazorat qilish: virtual, mahalliy va tarmoq printerlari hamda chop etishga yuborilgan ma’lumotlarni nazorat qilish.

6.2.6. Tashqi qurilmalar auditi: USB xotira, ko‘chma qurilmalar (WPD), Bluetooth qurilmalarining ulanishi/uzilishi va Bluetooth orqali fayl uzatilishini qayd etish; tushunarli nom berish; birinchi aniqlanganda xavfsiz yoki ishonchsiz toifaga ajratish.

6.2.7. Saqlanayotgan ma’lumotlarni aniqlash: yoqilgan barcha tasniflar bo‘yicha qurilma mahalliy disklarida konfidensial fayllarni doimiy fon rejimida skanerlash (foydalanuvchi papkalari yoki barcha disklar, qurilmalarni tanlash); natijalarni tasniflar va mosliklar soni bilan ro‘yxat, filtr va eksport ko‘rinishida taqdim qilish.

7. YAKUNIY QURILMALAR HOLATI

7.1. Har bir qurilma uchun konsolda onlayn/oflayn holati, so‘nggi javob vaqti, oxirgi kirgan foydalanuvchi, mijoz versiyasi, operatsion tizim va jamoalarga mansublik ko‘rsatilishi kerak.

7.2. Himoya holati «himoyalangan» / «pasaygan» (e’tibor talab etiladi) / «himoyalanmagan» sifatida, sababi bilan (aloqa yo‘q, mijoz eskirgan, komponent o‘rnatilmagan, faolsizlantirilgan va boshqalar) aks etishi; bosh panelda holatlar bo‘yicha qurilmalar soni vidjeti bo‘lishi kerak.

7.3. Qurilma kartasida mijozning alohida xizmatlari holati tegishli sozlamalarga havolalar bilan ko‘rsatilishi shart.

7.4. Barcha tashkilot uchun standart mijoz parametrlari va alohida qurilma/guruhlar uchun istisno sozlamalari bo‘lgan alohida konsol bo‘limi bo‘lishi kerak.

7.5. Bitta obrazdan mijoz o‘rnatilgan holda yaratilgan klon qurilmalar qo‘lda nizolarni bartaraf etmasdan avtomatik tanilishi kerak.

8. FAYLLAR BILAN VEB-AMALLAR AUDITI

8.1. Tizim brauzer orqali fayllarni yuklash/yuklab olishni URL, domen, sayt toifasi, fayl hajmi va tasnifi, qo‘llangan siyosat va amal bilan qayd etishi shart.

9. MICROSOFT 365 VA GOOGLE WORKSPACE MA’LUMOTLARINI HIMOYALASH

9.1. Exchange Online: tenant foydalanuvchilarining istalgan qurilmadan (jumladan mobil va mijoz o‘rnatilmagan qurilmalardan) yuborgan barcha chiqish xatlarini (mavzu, matn, ilovalar) audit qilish.

9.2. Outlook: Outlook on the web va Windows/Mac uchun yangi Outlook qo‘shimchasi xat yuborishdan oldin «jurnalga qayd etish», «xabardor qilish», «bloklash», «asosli chetlab o‘tish bilan bloklash» amallarini, qabul qiluvchi domenlarini xavfsiz/ishonchsizga tekshirishni ta’minlashi; Microsoft 365 admin markazidan markaziy o‘rnatilishi; klassik Outlook va SMTP/POP3/IMAP mijozlari qurilmadagi mijoz orqali himoyalanishi kerak.

9.3. SharePoint Online, OneDrive for Business, Microsoft Teams: faylni yuklash/yuklab olish va unga kirish berish (ichki, tashqi, «havolasi bor barchaga») audit qilinishi; jurnal, ogohlantirish, bloklash (noto‘g‘ri ruxsatni avtomatik bekor qilish va xabar berish), asosli chetlab o‘tish bilan bloklash siyosatlari; administrator ruxsatni qo‘lda bekor qilishi; qurilmada mijozsiz ishlash; tenant, sayt yoki SharePoint papkasi darajasida nozik nazorat.

9.4. Google Drive: ichki/tashqi oluvchilarga kirish berish va faylni yuklab olishni audit qilish; yuklab olishni bloklash mijoz o‘rnatilgan qurilmalarda ta’minlanishi.

9.5. Bulutli tasnif: qurilmada mijoz qo‘ygan tasnif va tashqi tizimlar (Microsoft Purview Information Protection va boshqalar) belgilarini bulut fayllariga qo‘llash.

10. XULQ-ATVOR TAHLILI TIZIMI

10.1. Vazifalar

10.1.1. Xavf guruhlari va ayrim xodimlarning aloqalarini nazorat qilish.

10.1.2. Xodimlar harakatlarini monitoring qilish.

10.1.3. Axborot xavfsizligi voqea va hodisalarini boshqarishni avtomatlashtirish.

10.1.4. Tahlil va ustuvorlashtirishni tezlashtirish uchun hodisalar/foydalanuvchi faolligini xulq-atvor kategoriyalariga (ish faoliyati, ishga aloqasiz, shubhali, kategoriyasiz) ajratish.

10.2. Funksional talablar

Ilovalar auditi

10.2.1. Ilovalardan foydalanish, xodimlarning faol va nofaol vaqtini hisobga olish.

10.2.2. Ilovalarning ishga tushish va faol foydalanish vaqtini batafsil ko‘rsatish.

10.2.3. Tez baholash uchun ilova kategoriyalaridan foydalanish, noma’lum ilovalarni qaydlardan to‘g‘ridan-to‘g‘ri kategoriyalash.

Veb-saytlar auditi

10.2.4. Tashrif buyurilgan saytlarni (HTTPS ham) faol vaqtini hisobga olgan holda jurnalga yozish.

10.2.5. Brauzerdan qat’i nazar URL, protokol va sahifa sarlavhalarini batafsil ko‘rsatish.

10.2.6. Tez baholash uchun veb-sayt kategoriyalaridan foydalanish.

E-mail auditi

10.2.7. Yuborilgan va olingan xatlar, jumladan ilovalar, mavzu, jo‘natuvchi/qabul qiluvchi manzili, vaqt va hajmni qayd etish.

10.2.8. Eng faol qabul qiluvchilar va jo‘natuvchilarni manzil yoki domen bo‘yicha guruhlab tahlil qilish.

10.2.9. 2.2.12-banddagi pochta mijozlari, jumladan SSL/TLS ulanishlarini qo‘llash.

Ogohlantirishlar

10.2.10. Qoidalar: tur, foydalanuvchi/jamoa/qurilma va oluvchilarni tanlab, darhol yoki kunlik jamlanma ko‘rinishida ogohlantirish yaratish.

10.2.11. Usullar: kamida e-mail, konsol, SIEMga syslog.

10.2.12. Xavfsizlik ogohlantirishlari: DLP siyosati buzilishi (qayd/bildirish/bloklash/chetlab o‘tish); bir foydalanuvchining bir kunda ko‘p marta buzishi; himoyasiz konfidensial ma’lumotning qurilmadan chiqishi (e-mail, sayt, USB, bulut, messenjer, printer); sayt yoki ilovaga kirish rad etilishi.

10.2.13. Xizmat ogohlantirishlari: konsolga ko‘p marta muvaffaqiyatsiz kirish, baza to‘lishi/diskda joy yetishmasligi, litsenziya holati.

10.2.14. Axborot ogohlantirishlari: kun/hafta chegaralari bo‘yicha fayl amallari (fayllar soni va zarur bo‘lsa tasnifi), veb-toifalarda vaqt/xatlar soni, ilova toifalarida vaqt, bosma hujjat yoki sahifalar soni.

Hisobotlar

10.2.15. Kamida quyidagi tayyor hisobot maketlari: veb-saytlar bilan ishlash; e-mail; ilovalar; chop etish; faol vaqt; umumiy sharh; xulq-atvor tahlili (umumiy ko‘rinish, shubhali faoliyat, AI vositalari, ish qidirish).

Samaradorlikni baholash

10.2.16. Ilova va saytlarni sozlanuvchi kategoriyalash: ichki va maxsus kategoriyalar, xulq-atvor sinfi (ish faoliyati/ishga aloqasiz/shubhali).

10.2.17. Vaqt faqat foydalanuvchi oyna/sahifada amalda faol bo‘lganda (bosish, kiritish, sichqoncha harakati) hisoblanishi; fon oynalari hisobga olinmasligi; harakatsizlikning 5 daqiqasidan so‘ng hisob to‘xtashi, chegara sozlanishi.

10.2.18. Foydalanuvchi, jamoa, qurilma, davr, ish soati va xulq-atvor toifasi bo‘yicha tanlashli panellar/jadvallar, tekshiruv uchun batafsil ma’lumotga tez o‘tish.

11. ILOVALAR VA VEB-SAYTLARNI NAZORAT QILISH SIYOSATLARI

11.1. Ilova siyosatlari: toifa yoki individual ilovalar bo‘yicha ishga tushirishni bloklash yoki ruxsat etish, bloklanganda foydalanuvchini xabardor qilish.

11.2. Sayt siyosatlari: toifa yoki sayt bo‘yicha kirishni bloklash/ruxsat etish, bloklangan foydalanuvchini Buyurtmachining sahifasiga yo‘naltirish.

11.3. Qo‘llanish: butun tashkilotga yoki ayrim jamoa/qurilma/foydalanuvchilarga.

11.4. Siyosat amallari, ustuvorligi va qo‘llanish mantiqi 15-bo‘limga muvofiq bo‘lishi kerak.

11.5. Bloklangan ilova ishga tushirishlari va saytga kirish urinishlari audit bo‘limida ko‘rsatilishi hamda insaytlar (12.2-band) yaratilishi shart.

12. KONFIDENSIAL MA'LUMOTLAR SIZIB CHIQISHIDAN HIMOYALASH TIZIMI (DLP)

12.1. DLP vazifalari

12.1.1. Aloqa kanallarida siyosat va ma'lumotlar tasnifiga muvofiq konfidensial ma'lumot uzatishni nazorat qilish/bloklash.

12.1.2. Qoidalarga ko‘ra konfidensial ma'lumotli elektron hujjatlarni topish.

12.1.3. Axborot xavfsizligi (DLP) siyosatlarini yaratish.

12.1.4. Axborot xavfsizligi administratorini buzilishlar haqida ogohlantirish.

12.1.5. Biznes uchun muhim axborot uzatilishini nazorat qilish/bloklash.

12.1.6. Axborot xavfsizligi voqea va hodisalarini boshqarishni avtomatlashtirish.

12.2. DLP funksional talablari

Umumiy talablar

12.2.1. Ma'lumotlar himoyasi: dastur va protokoldan qat'i nazar, shifrlangan ulanishlarni ham qamrab olishi.

12.2.2. Tasnifni saqlash: fayl mazmuni har o‘zgarganda tasnifni avtomatik qayta baholash; foydalanuvchi tasnifi teglarini .docx, .xlsx, .pptx, .pdf, .xlsm metama'lumotlariga yozish va arxivlashda saqlash; tasniflangan hujjatdan parcha boshqa hujjatga ko‘chirilganda tasnif va cheklovlarni yangi hujjatga o‘tkazish.

12.2.3. Soyali nusxa: tasnifga ega siyosat bilan bog‘liq hodisa vaqtida fayl nusxasini yaratish (siyosat bo‘yicha yoqish/o‘chirish); foydalanuvchi kirishini cheklash, qurilmadagi alohida omborda eski nusxalarni yangilari bilan almashtirish, maksimal fayl hajmini cheklash; konsoldan hodisa qaydi bo‘yicha nusxa so‘rash, unga alohida huquq belgilash.

12.2.4. Imtiyozli vaqtinchalik kirish: favqulodda holatda ayrim foydalanuvchi uchun siyosatni vaqtincha to‘xtatish (masalan katta hajmdagi konfidensial axborotni tez uzatish); 1 soat, 6 soat yoki joriy kun oxirigacha faolsizlantirish, yarim tunda avtomatik tugatish va administratorning muddatidan oldin bekor qilishi; barcha harakatlarni qayd etishda davom etish va yuqori muhimlikdagi insayt yaratish.

12.2.5. Kontent tahlili: «barchasi», «tavsiya etilgan» (ofis hujjatlari, PDF, matn, pochta fayllari, arxivlar) yoki «maxsus» fayl to‘plamini tanlash; kengaytmasidan qat'i nazar haqiqiy fayl turini mazmunidan aniqlash; zip, rar, 7z, gz arxivlari ichidagi fayllarni tekshirish; shifrlangan va noma'lum formatlarni alohida tasniflash/siyosat qo‘llash; tahlil holatini «to‘liq/qisman/shifrlangan/o‘qib bo‘lmaydi/tahlil qilinmagan» ko‘rsatish.

Qurilmalarni nazorat qilish

12.2.6. Kamida USB, WPD, Windows/macOSga USB orqali ulangan iOS (iPhone), Bluetooth qurilmalar va fayl uzatish, kartani o‘qish qurilmalari, CD/DVD, FireWire nazorat qilinishi kerak.

12.2.7. Ruxsat rejimlari: bloklash, faqat o‘qish, qayd bilan bildirish, faqat qayd, to‘liq ruxsat.

12.2.8. Korporativ qurilmalar istisnosi: xavfsiz manzil belgilash va har bir tur uchun «xavfsizlardan tashqari barcha» qoidasini qo‘llash.

12.2.9. Audit jurnali barcha tashqi qurilmalarni, jumladan monitor, klaviatura va sichqonchani qayd etishi kerak.

12.2.10. Windows Portable Devices (smartfon, multimedia qurilmalari)da fayl amallarini nazorat qilish.

Tarmoq resurslaridagi konfidensial ma’lumotni nazorat qilish

12.2.11. Yakuniy qurilmadan SMB (jumladan DFS) tarmoq resurslari bilan ishlaganda fayl amallarini nazorat qilish, tarmoq yo‘li bo‘yicha tasniflash hamda yo‘llarni xavfsiz yoki ishonchsiz manzil sifatida ishlatish.

Boshqa tasniflash tizimlari bilan integratsiya

12.2.12. Hujjat metama’lumotlarida, shifrlangan hujjatlarni ham qo‘shib, Microsoft Purview Information Protection, Boldon James, Tukan GREENmod belgilarini tanish; Microsoft 365 tenantidan konfidensiallik belgilarini import qilish.

Tahdid, hodisa va voqealarni intellektual boshqarish (insaytlar)

12.2.13. Veb-konsolning yagona joyida ma’lumotlar, ilovalar, saytlar, tashqi qurilmalardagi ustuvor tahdid/hodisalarni avtomatik ustuvorlashtirish; dastlab faqat yangi, ko‘rib chiqilmagan voqealar («vazifalar ro‘yxati») ko‘rinishi.

12.2.14. Har bir insaytda sabab va daraja (past/o‘rta/yuqori) bo‘lishi; kamida quyidagilar uchun insayt: bloklash bilan ma’lumot siyosati buzilishi; asosli chetlab o‘tib bloklash; ilova ishga tushishini bloklash; saytni bloklash; tashqi qurilma siyosati buzilishi; foydalanuvchi uchun dinamik siyosat qat’iyligi oshishi; imtiyozli kirish berilishi.

12.2.15. Qaydlarni foydalanuvchi, manzil turi, siyosat, sayt, ilova, qurilma va tasnif bo‘yicha yagona insaytga birlashtirish; yopilgan insaytga yangi qayd qo‘shilmasligi, takrorlansa yangisi yaratilishi; umumiy muhimlik tarkibdagi maksimal darajaga teng bo‘lishi.

12.2.16. «Yangi»/«yopilgan» holatlari, yopish sabablari («choralar ko‘rildi», «shaxsiy foydalanish», «kelishilgan faoliyat», «noto‘g‘ri ishga tushish», «boshqa»), yopish uchun alohida huquq, bog‘liq qayd/foydalanuvchi/siyosat/tasnifga o‘tish.

12.2.17. Siyosat darajasida insaytni «standart/har doim/hech qachon» yaratish sozlamasi va webhook orqali yuborish.

13. KONFIDENSIAL MA’LUMOTLARNI ANIQLASH IMKONIYATLARI

13.1. Kontentga asoslangan tizim

13.1.1. Aniqlash usullari: tekshiruv algoritmli tayyor lug‘atlar (IBAN, to‘lov kartalari raqami, milliy identifikatorlar va boshqalar); foydalanuvchi kalit so‘zlari va muntazam ifodalari, bir necha qatordagi moslikni aniqlash uchun standart/kengaytirilgan ishlov; shaxsga doir ma’lumotlarni himoyalashning xalqaro/milliy talablari (kamida GDPR, CCPA, PIPEDA, LGPD, HIPAA, PCI DSS) bo‘yicha ishlab chiqaruvchi yangilaydigan tayyor shablonlar/qoidalar.

13.1.2. Tizim ishlab chiqaruvchi yaratgan axborotni avtomatik aniqlash/ishlov berish uchun oldindan sozlangan tasnif qoidalarini o‘z ichiga olishi shart.

13.1.3. Tasnif qoidalari elektron hujjatlardagi belgilangan ma’lumot turlarini to‘g‘ri aniqlashi va himoya/nazorat mexanizmlarida ishlatilishi kerak.

13.1.4. Kamida tayyor tasniflar: shaxsga doir, moliyaviy, tibbiy, katta hajmdagi sezgir ma’lumotlar, dastlabki kod, bajariladigan fayllar va skriptlar, boshqa tizimlardagi mavjud tasnif.

13.1.5. Foydalanuvchi kalit so‘zlar lug‘atini import qilish.

13.1.6. Moslik minimal soni, qoida ichidagi elementlar yaqinligi, elementlar orasida «VA», qoidalar/tasniflar orasida «YOKI» mantiqlarini sozlash.

13.1.7. Fayl bilan ishlashda yakuniy qurilma, tarmoq/bulutdan olingan fayl va mahalliy diskda saqlangan fayllardagi ma’lumotni aniqlash.

13.1.8. Hujjat metama’lumotlaridagi boshqa tizim belgilaridan foydalanish.

13.2. Kontekstga asoslangan tizim

13.2.1. Har qanday fayl turini va hujjat tili/kodlashidan mustaqillikni qo‘llash.

13.2.2. Ilova va sayt kategoriyasi (fayl manbasi) bo‘yicha aniqlash qoidalari.

13.2.3. Mahalliy va tarmoq papkalari bo‘yicha yangi fayllarga meros qoladigan qoidalar.

13.2.4. Fayl formatini o‘zgartirganda qoidalar yaratish.

13.3. Fayl parametrlariga asoslangan tizim

13.3.1. Metama’lumotlarida tasniflashni yoki kontent tizimida aniqlashni qo‘llamaydigan fayllarni tasniflash.

13.3.2. Fayl turi (kengaytma yoki CAD, arxiv, rasm, bajariladigan fayl kabi kategoriyalar) va nomi (muntazam ifoda) bo‘yicha tasniflash.

13.3.3. AI yordamchisi yaratgan faylni avtomatik belgilash, fayl kartasida kelib chiqishini ko‘rsatish va alohida himoya siyosati qo‘llash.

13.3.4. Qo‘shimcha server talab qilmaydigan ichki OCR moduli (14.2-band).

13.4. Foydalanuvchi belgilaydigan ma’lumotlar tasnifi (teglar)

13.4.1. Tizim yakuniy foydalanuvchiga administrator boshqaruv konsolida yaratgan teglar orqali faylni qo‘lda tasniflash imkonini berishi kerak. Tegni qo‘yish, almashtirish yoki olib tashlash faylga qo‘llaniladigan siyosatga bevosita ta’sir qilishi shart.

13.4.2. Administrator tomonidan teg boshqaruvi: «Ochiq», «Ichki», «Maxfiy», «O‘ta maxfiy» kabi teglarni yaratish; nom/tavsifni tahrirlash; o‘chirishdan oldin bog‘liq tasnif/siyosatlar va oqibatni ko‘rsatish; o‘chirilgan teg eski faylda saqlanishi, yangi faylga qo‘yilmasligi.

13.4.3. Teg siyosatida huquqlar: foydalanuvchi/jamoaga ruxsat etilgan teglar ro‘yxati va qat’iylikni belgilovchi tartibi; qo‘yish, qat’iyroq tegga ko‘tarish, yumshatish yoki olib tashlash huquqlarini ajratish; foydalanuvchiga faqat ruxsat etilgan teg va amallar ko‘rinishi.

13.4.4. Foydalanuvchi qo‘llashi: Windows/macOS kontekst menyusi (o‘ng tugma → «Faylni tasniflash») orqali teg qo‘yish/o‘zgartirish/pasaytirish/o‘chirish; tegga bog‘liq siyosatni avtomatik qo‘llash.

13.4.5. Teglardan foydalanish: ularni tasnif qoidalariga va himoya siyosatlariga bog‘lash (masalan «Ichki» yoki «Maxfiy» tegli fayllar uchun skrinshotni bloklash).

13.4.6. Monitoring: ma’lumotlar bo‘limida teg va amalni (qo‘yildi/oshirildi/pasaytirildi/olib tashlandi) aks ettirish, filtrlash.

13.4.7. Texnika: .docx, .xlsx, .pptx, .pdf, .xlsm fayl metama’lumotlariga teg yozish, boshqa formatlarda qurilmada keshlash; bir faylda bir vaqtning o‘zida faqat bitta foydalanuvchi tegi bo‘lishi, boshqa tizim teglari bilan birga mavjud bo‘lishiga ruxsat.

14. MA’LUMOT UZATISH KANALLARINI NAZORAT QILISH (SIZIB CHIQISHDAN HIMOYA)

14.1. Ma’lumot uzatish kanallari va manzillari

14.1.1. Tizim 1-jadvaldagi kamida barcha kanallarda konfidensial axborot uzatilishini nazorat va bloklashi kerak.

1-jadval. Ma’lumot uzatish kanallari va talablar

Kanal	Talablar	Qo‘shimcha shartlar
Bulutli xotiralar	• Tizim sinxronizatsiya klientlari, sinxronizatsiya papkalari va veb-interfeys orqali bulutli disklarga fayl uzatishni nazorat qilishi va bloklashi kerak. • Qo‘llab-quvvatlanadigan xizmatlar kamida: Box, Dropbox, Google Drive, OneDrive (shaxsiy va korporativ), SharePoint Online. • Muayyan tenantlar, SharePoint saytlari va papkalari uchun siyosatlar qo‘llab-quvvatlanishi kerak. • DLP siyosatlarining barcha turlarida qo‘llab-quvvatlanishi ta’minlanishi kerak.	• Fayllarning soyali nusxasi olinishi ta’minlanishi kerak. • Amallar qayd etilishi ta’minlanishi kerak.
Veb orqali yuklash	• Tizim veb-brauzer orqali barcha saytlarga, jumladan veb-pochta ilovalari, messenjerlarning veb-versiyalari va brauzer orqali bulutli disklarga fayl yuklashni nazorat qilishi va bloklashi kerak. • Umumiy va maxsus DLP siyosatlarida qo‘llab-quvvatlanishi ta’minlanishi kerak.	• Fayllarning soyali nusxasi olinishi ta’minlanishi kerak. • Amallar qayd etilishi ta’minlanishi kerak.
Elektron pochta orqali uzatish	• Tizim pochta klientlari (kamida klassik va yangi Outlook, SMTP/POP3/IMAP klientlari) orqali xat yuborishni nazorat qilishi va bloklashi kerak. • Tizim xat mavzusi, matni va ilovalarini tahlil qilishi, shuningdek qabul qiluvchilarni xavfsiz va ishonchsiz domen va manzillar bo‘yicha tekshirishi kerak. • Umumiy va maxsus DLP siyosatlarida qo‘llab-quvvatlanishi ta’minlanishi kerak.	• Outlook on the web uchun himoya Outlook qo‘shimchasi orqali ta’minlanishi kerak (9-bo‘lim). • Fayllarning soyali nusxasi olinishi ta’minlanishi kerak. • Amallar qayd etilishi ta’minlanishi kerak.
Messenjerlar	• Tizim messenjerlarning ilovalari va veb-versiyalari (kamida Microsoft Teams, Slack, WhatsApp, Telegram, Viber, Facebook Messenger, Cisco Jabber) orqali fayl uzatishni nazorat qilishi va bloklashi kerak. • Tizim korporativ va shaxsiy messenjerlar uchun alohida amallarni qo‘llab-quvvatlashi kerak. • Umumiy va maxsus DLP siyosatlarida qo‘llab-quvvatlanishi ta’minlanishi kerak.	• Siyosatlar xabar almashishni cheklamasdan, fayllarga qo‘llanilishi kerak. • Fayllarning soyali nusxasi olinishi ta’minlanishi kerak. • Amallar qayd etilishi ta’minlanishi kerak.

Kanal	Talablar	Qo‘shimcha shartlar
Tashqi qurilmalar	• Tizim USB-to‘plagichlar, portativ qurilmalar (WPD) va Bluetooth orqali fayl uzatishni nazorat qilishi va bloklashi kerak. • «Faqat o‘qish» rejimi qo‘llab-quvvatlanishi kerak. • Korporativ qurilmalar uchun «xavfsizlaridan tashqari barchasi» qoidasi qo‘llab-quvvatlanishi kerak. • DLP siyosatlarining barcha turlarida qo‘llab-quvvatlanishi ta’minlanishi kerak.	• Fayllarning soyali nusxasi olinishi ta’minlanishi kerak. • Amallar qayd etilishi ta’minlanishi kerak.
Tarmoq fayl resurslari	• Tizim SMB tarmoq resurslariga, jumladan DFS’ga fayl yuklashni nazorat qilishi va bloklashi kerak. • Umumiy va maxsus DLP siyosatlarida qo‘llab-quvvatlanishi ta’minlanishi kerak.	• Fayllarning soyali nusxasi olinishi ta’minlanishi kerak. • Amallar qayd etilishi ta’minlanishi kerak.
Masofaviy uzatish	• Tizim Microsoft Remote Desktop (RDP) seanslarida fayl uzatish va almashinuv buferi bilan amallarni nazorat qilishi va bloklashi kerak. • Umumiy va maxsus DLP siyosatlarida qo‘llab-quvvatlanishi ta’minlanishi kerak.	• Siyosatlar ulanishlarni cheklamasdan, fayllarga qo‘llanilishi kerak. • Amallar qayd etilishi ta’minlanishi kerak.
Chop etish	• Tizim chop etishni, jumladan virtual chop etishni nazorat qilishi va bloklashi kerak. • Tizim faqat virtual chop etish uchun qoidalar yaratish imkonini berishi kerak. • DLP siyosatlarining barcha turlarida qo‘llab-quvvatlanishi ta’minlanishi kerak.	• Amallar qayd etilishi ta’minlanishi kerak.
Almashinuv buferi	• Tizim matn va tasvirlarni nusxalashni nazorat qilishi va bloklashi kerak. • Ma’lumot toifalari va ilovalar uchun maxsus siyosatlarda qo‘llab-quvvatlanishi ta’minlanishi kerak.	• Siyosatlar boshqa ilovalarga nusxalash amallariga qo‘llanilishi, lekin manba ilovaning ichida qo‘llanilmasligi kerak.
Ekranni suratga olish	• Tizim skrinshot olish, ekran tasvirini uzatish va ekranni yozib olishni nazorat qilishi va bloklashi kerak. • Ma’lumot toifalari va ilovalar uchun maxsus siyosatlarda qo‘llab-quvvatlanishi ta’minlanishi kerak.	

Kanal	Talablar	Qo‘shimcha shartlar
Git-repozitoriylar	• Tizim SSH va HTTPS protokollari orqali kod yuborishni (git push) nazorat qilishi kerak. • Tizim repozitoriylar va repozitoriylar guruhlarini (tashkilot prefiksi bo‘yicha bitta qoida bilan) xavfsiz yoki ishonchsiz manzil sifatida belgilashni hamda yangi repozitoriylarni avtomatik aniqlashni qo‘llab-quvvatlashi kerak.	• Amallar qayd etilishi ta’minlanishi kerak.
AI-yordamchilar	• Tizim AI-yordamchilarning ilovalari va veb-versiyalariga (kamida Claude, ChatGPT, Microsoft Copilot, jumladan alohida Copilot ilovasi) fayl yuklash, matnni joylashtirish va sudrab tashlash, elektron pochta ilovalarini sudrab tashlash hamda so‘rovlarni (promptlarni), jumladan qo‘lda yozilganlarini, nazorat qilishi kerak. Har bir yordamchi uchun alohida amallar belgilanishi kerak. • Boshqa AI-xizmatlar uchun nazorat «Veb orqali yuklash» kanali va AI-vositalar manzillari guruhi orqali ta’minlanishi kerak. • Batafsil talablar – 14.3-band.	• Amallar qayd etilishi ta’minlanishi kerak. • Fayllar va so‘rovlarning soyali nusxasi olinishi ta’minlanishi kerak.
Microsoft 365 da birgalikda foydalanish	• Tizim SharePoint / OneDrive / Teams fayllariga berilgan kirish huquqlarini audit qilishi va bekor qilishi kerak (9-bo‘limga qarang).	• Qurilmada klient o‘rnatmasdan ishlashi ta’minlanishi kerak.

Ma’lumot manzillari

14.1.2. Manzillar katalogi: «belgilanmagan» (avtomatik topilgan), «ishonchsiz» (himoyalangan perimetr tashqarisi), «xavfsiz» (perimetr ichida, siyosat istisnolari) kamida uch toifa; ichki guruhlash.

14.1.3. Manzillarni qo‘lda qo‘shish: pochta domen/manzillari, saytlar (niqoblar), tarmoq yo‘llari, veb-toifalar, bulut disklari (SharePoint tenant/sayt/papka, OneDrive tenant), Git repozitoriylari.

14.1.4. Tayyor manzil guruhlari: AI vositalari, fayl almashish xizmatlari, bepul pochta, ijtimoiy tarmoqlar, veb-messenjerlar, ommaviy bulut platformalari, Microsoft 365.

14.1.5. Siyosat filtrlari: barchasi / xavfsizlardan tashqari barchasi / faqat xavfsiz / faqat belgilanmagan / tanlangan guruhlar.

14.1.6. Xavfsiz/ishonchsiz hududlar: USB (xotira va boshqa), printerlar (tarmoq, mahalliy, virtual), tarmoq (yo‘l, IP, veb-manzil, kategoriya, bulut, Git), e-mail (manzil va domen).

14.1.7. Siyosat amallari, ustuvorligi va mantiqi 15-bo‘limga mos bo‘lishi shart.

14.2. OCR ishlashiga talablar

14.2.1. Tizim OCR (Optical Character Recognition — belgilarni optik tanish) orqali rasm, foto va skaner hujjatlardagi konfidensial mazmunni aniqlashi kerak. OCR rasm matnini mashina o‘qiydigan matnga

aylantirib, so‘ng sezgir kontentni standart tahlil qiladi. Modul bitta ishlab chiqaruvchiga tegishli tizim ichida bo‘lishi, alohida OCR serveri talab qilmasligi shart.

14.2.2. Kamida .png, .tiff, .jpg, .jpeg, .jpe, .bmp formatlarini qo‘llash; PDF, taqdimot, elektron kitob va boshqa fayldan rasmlarni ajratish; to‘liq ro‘yxat hujjatlarda berilishi.

14.2.3. Kamida qozoq, rus, ingliz, arab, arman, ivrit, xitoy (soddalashtirilgan va an’anaviy), litva, mo‘g‘ul, nemis, polyak, portugal (Braziliya), slovak, ispan, turk, ukrain, fransuz, chex tillari.

14.2.4. Kerakli til ro‘yxatda bo‘lmasa, belgilari yaqin tilni tanlash; bir vaqtda kamida ikki OCR tilidan foydalanish.

14.2.5. Kamida ikki rejim: standart (ish stansiyasiga past yuklama) va yuqori aniqlik; administrator rejimni tanlashi va yuklamani taqsimlash uchun alohida qurilmalarda OCRni yoqib/o‘chira olishi.

14.3. AI vositalaridan foydalanishni nazorat qilish

14.3.1. Tizim xodimlar generativ AI xizmatlaridan foydalanishi va ularga konfidensial axborot uzatishini aniqlashi, tahlil qilishi hamda nazorat qilishi shart.

AI xizmatlaridan foydalanish sharhi:

14.3.2. Kamida oxirgi 30 kunni ko‘rsatadigan alohida konsol bo‘limi.

14.3.3. Xodimlar ishlatgan AI xizmatlarni, jumladan IT bilan kelishilmaganlarini avtomatik aniqlash; foydalanuvchi o‘z ilova/saytini qo‘sha oladigan ichki AI toifasi.

14.3.4. Desktop ilovalari, saytlar va bitta xizmatning ilova/veb-versiyasini yagona qaydga birlashtirish.

14.3.5. Har AI xizmat bo‘yicha faol vaqt, foydalanuvchi va ma’lumot amallari soni (bloklanganlari ham), uzatilgan ma’lumot tasnifi, natija («bloklandi», «jurnalga yozildi yoki xabar qilindi», «ruxsat etildi», «siyosatsiz konfidensial ma’lumot», «konfidensial ma’lumot topilmadi»).

14.3.6. Siyosatsiz konfidensial ma’lumot uzatish holati, ustuvor ko‘rib chiqiladigan AI xizmatlar reytingi, kamida 30 kunlik kunma-kun dinamika.

14.3.7. AI xizmat kartasi: faollik grafigi, amallarning tasnif/natija bo‘yicha taqsimoti, eng faol va eng ko‘p konfidensial ma’lumot yuborgan foydalanuvchilar, bog‘liq sayt/ilova, asl qaydlarga o‘tish.

14.3.8. AI xizmatlar jadvalini filtr, saralash va ustun tarkibi bilan XLSXga chiqarish.

AI yordamchilariga ma’lumot uzatishni nazorat qilish:

14.3.9. Himoya siyosatida kamida Claude (Claude Cowork bilan), ChatGPT, Microsoft Copilot (Microsoft 365 Copilot va alohida Copilot ilovasi) uchun alohida manzil turi; veb/ilova shakllari hamda har biri uchun alohida amal.

14.3.10. Windows/macOSda fayl yuklashni; Windowsda matnni qo‘yish/tortish va e-mail ilovasini tortishni; Windows/macOSdagi Chrome/Edgeda AI saytiga qo‘lda yozilgan promptlarni yuborishdan oldin ishlab chiqaruvchining avtomatik o‘rnatiladigan brauzer kengaytmasi orqali nazorat qilish.

14.3.11. Windowsda shaxsiy va korporativ Claude hisobini farqlash, korporativga ruxsat va shaxsiyga uzatishni cheklash.

14.3.12. Siyosatni buzgan fayl/promptning soyali nusxasini yaratish.

14.3.13. Boshqa AI xizmatlariga tayyor AI vositalari manzil guruhi orqali fayl yuklash siyosatini qo‘llash; ruxsatsiz AI saytlari va ilovalarini kategoriyasi bo‘yicha bloklash.

15. XAVFSIZLIK SIYOSATLARINI QO‘LLAB-QUVVATLASH

15.1. Siyosatlar: ma’lumot uzatish kanallari uchun umumiy; ma’lumot kategoriyasi/tasnifi uchun kombinatsiyalanadigan maxsus; audit, ilova/veb-sayt, tashqi qurilma, ma’lumot va foydalanuvchi teglari siyosatlarini yaratish.

15.2. Tatbiq: butun tashkilotga yoki jamoa/alohida qurilma/foydalanuvchilarga.

15.3. Siyosat amallari: «ruxsat etish» (umumiy siyosatdan istisno), «jurnalga yozish» (sezdirmasdan qayd), «xabardor qilish» (foydalanuvchiga bildirish bilan qayd), «bloklash» (bildirish bilan), «asosli chetlab o‘tish bilan bloklash» (foydalanuvchi ro‘yxatdan sabab tanlab asos yozadi, ular qayd va ogohlantirishga kiritiladi).

15.4. Qo‘llash mantiqi: siyosatlar ro‘yxatda yuqoridan pastga tekshirilib, mos kelgan birinchisi qo‘llanadi; barcha shartlar (tasnif, manzil turi, foydalanuvchi/jamoa/qurilma) bir vaqtda bajarilishi; ustuvorlik ro‘yxat tartibida; siyosatni o‘chirish imkoniyati; yagona elementi o‘chirilgan siyosat ishlamaydi deb belgilanishi.

15.5. Kengaytirilgan boshqaruv: bir siyosatda turli manzil turlari/guruhlari, ilovalar, saytlar yoki qurilma turlariga alohida amallar.

15.6. Dinamik amal: konfidensial axborot bilan foydalanuvchining odatiy xatti-harakatidan chetlanishi va hajmiga qarab individual siyosat qat’iyligi «belgilanmagan → jurnal → xabar → bloklash» bo‘yicha bosqichma-bosqich oshirilishi (statik ruxsat/bloklash o‘rniga); daraja oshsa insayt yaratilishi.

15.7. Tayyor siyosatlar: kamida barcha chiqishdagi sezgir axborotni hodisa sifatida jurnalga olish, xavfli ilova/saytni bloklash, barcha faollik toifalarini audit qilish bo‘yicha misol va tavsiyalar.

16. LITSENZIYALASH

16.1. Qurilmaga emas, kamida 6000 foydalanuvchiga litsenziya; mijoz dasturini litsenziya sonidan ko‘proq qurilmaga o‘rnatish; bir necha kun faol bo‘lmagan yoki katalogdan o‘chirilgan hisoblar hisoblanmasligi; administrator litsenziyani qo‘lda ajratishi va qayta tayinlashi.

16.2. Qurilmadan topilgan yoki katalogdan sinxronlangan yangi hisoblar avtomatik litsenziyalanishi va siyosatlar bilan himoyalanishi.

16.3. Litsenziya tugashidan oldin administratorga e-mail va konsolda holat haqida xabar berilishi.

16.4. Litsenziya muddati 36 oyni tashkil etishi lozim.

16.5. Muddat tugaganda: konsol, qaydlar tarixi va hisobotlar ochiq qolishi; uzaytirilganda qayta o‘rnatmasdan ishlash tiklanishi.

17. QURILMALARNI BOSHQARISH VA MIJOZNI JOYLASHTIRISH

17.1. Konsoldan individual/ommaviy boshqarish: mijozni yangilash, qayta yuklash, jurnallar va kengaytirilgan diagnostikani yig‘ish, faolsizlantirish/faollashtirish, o‘chirish, savatchaga ko‘chirish/tiklash, holat bo‘yicha filtr/guruh, XLSX eksport.

17.2. Windows/macOS o‘rnatuvchilarini konsoldan yuklash; qo‘lda, GPO, Microsoft Intune, Microsoft Configuration Manager (jim o‘rnatish) va macOS MDM orqali o‘rnatish.

17.3. Antivirus va EDR mosligi: ishlab chiqaruvchi mijoz/server jarayon va kataloglari uchun istisnolar ro‘yxatini e’lon qilishi kerak.

18. APPARAT VA DASTURIY TA’MINOTGA TALABLAR

18.1. Server

6000 foydalanuvchi hisobidan serverga minimal talablar:

18.1.1. Protsessor: kamida 8 ta fizik yadro.

18.1.2. Operativ xotira: kamida 32 GB (foydalanuvchilar ortsa oshirish tavsiya etiladi).

18.1.3. Disk: ma’lumotlar bazasi va zaxira nusxalar bilan kamida 1 TB bo‘sh SSD yoki RAIDdagi 15 000 ayl/min HDD.

18.1.4. Operatsion tizim: Windows Server 2019 yoki yangiroq (64-bit), IIS 10 va .NET Framework 4.7.2 yoki yangiroq.

18.1.5. MBBT: Microsoft SQL Server 2025 Standard Edition (16 Core License Pack) — muddatsiz litsenziya; to‘liq tijorat nashri, Express/Developer/Evaluation yoki qisqartirilgan/sinov versiyalari mumkin emas. «Kalit topshirish» asosidagi to‘liq yetkazish: 16 yadrolik litsenziya (8 ta SQL Server 2025 Standard core — 2 core License Pack); belgilangan muddat davomida o‘rnatish, faollashtirish va foydalanish huquqlari; ishlaydigan aktivatsiya kalitlari va distributivlar (elektron litsenziya/ESD).

18.1.6. Ma’lumotlar bazasi serveri: alohida, kamida 16 fizik yadro, 64 GB operativ xotira, 1 TB bo‘sh SSD yoki RAIDdagi 15 000 ayl/min HDD.

18.1.7. Kengaytirish: server xizmati va MBBTni alohida serverlarga o‘rnatish.

18.1.8. Tarmoq: konsol, xizmat va mijoz ulanishlari uchun kiruvchi portlar hujjatlarda ko‘rsatilishi; serverning internetga chiqishisiz ishlash.

18.2. Xizmat konsoli

18.2.1. Protsessor: kamida 2 yadro; RAM: 2 GB; disk: 2 GB.

18.2.2. OT: barcha xavfsizlik yangilanishlariga ega Windows 10 (64-bit), Windows 11 (64-bit), Windows Server 2019 va yangiroq.

18.3. Veb-boshqaruv konsoli

18.3.1. Har qanday zamonaviy brauzer, kamida Chrome, Edge, Firefox, Safari, Opera, Yandex Browser.

18.4. Windows ish stansiyalari

18.4.1. Minimum: 4 yadroli 2,4 GHz protsessor; 4 GB RAM (8 GB tavsiya); 8 GB bo‘sh disk (20 GB tavsiya); .NET Framework 4.8, .NET 10 Desktop Runtime va ASP.NET Core 10 Runtime (x64), dolzarb VCRedist.

18.4.2. OT: Windows 10 (64-bit, 22H2 va 21H2), Windows 11 (64-bit), Windows Server 2019 va yangiroq.

18.4.3. Terminal (Citrix, Azure Virtual Desktop, Microsoft RDS) va virtual muhitda ishlash.

18.5. macOS ish stansiyalari

18.5.1. macOS 12 va yangiroq, Intel va Apple Silicon platformalari.

18.5.2. MDM orqali konfiguratsiya profilida kerakli tizim ruxsatlarini markaziy berish.

18.5.3. macOS mijozi: ilova/sayt (Safari, Chrome, Opera, Edge), fayl, e-mail (Apple Mail; Outlook qo‘shimcha orqali), USB, messenjer auditini; kontent (OCR), tur/nom va foydalanuvchi teglari bilan tasniflashni; veb yuklash, bulut, pochta, messenjer, USB, tarmoq, chop etish, AirDrop, AI yordamchilar

(Claude, ChatGPT, Microsoft Copilot), iOS qurilmalarda «ruxsat/jurnal/xabar/bloklash» siyosatlarini qo‘llashi.

18.5.4. Xizmat: avtomatik yangilash, konsoldan o‘chirish/faolsizlantirish, debug ma’lumotini yig‘ish, yangi server manziliga yo‘naltirish.

18.5.5. Ruxsatsiz kirishdan mijoz jarayoni va papkalarini himoyalash.

19. EHTIMOLIY YETKAZIB BERUVCHIGA TALABLAR

19.1. Yetkazib beruvchi ishlab chiqaruvchining Buyurtmachiga yo‘llangan, xarid nomi va raqamini ko‘rsatgan vakolat xat (MAF)ini taqdim etishi shart.

19.2. Buyurtmachi infratuzilmasida server qismlari, baza, konsol va agentlarni joylashtirish; Microsoft Active Directory integratsiyasi va mavjud bo‘lsa Microsoft 365/Google Workspace ulash; antivirus istisnolari; ogohlantirishlar va Buyurtmachi SIEMi bilan integratsiya; Buyurtmachi talablariga ko‘ra audit siyosatlari, ma’lumot manzillari, tasnif va himoya siyosatlari; ma’lumotlar bazasi arxivi va administrator hisoblarini sozlash; barcha qismlar ishlashini tekshirish.

19.3. Tizimni ishga tushirish, Buyurtmachi bilan qabul sinovlarini o‘tkazish hamda ushbu texnik topshiriqqa funksional mosligini tasdiqlovchi texnik taklifni taqdim etish.

19.4. Buyurtmachi kamida ikki nafar xodimlarini tizim administratsiyasi va ishlatishga o‘qitish.

Kelishildi:

Z.X.Mamajonov

S.R.Mamasiddikov

A.R.Ibodov

F.S.Abdukadirov

A.F.Iskandarov