REPUBLIKA E KOSOVËS-REPUBLIKA KOSOVA-REPUBLIC OF KOSOVO
ZYRA KOMBËTARE E AUDITIMIT
NACIONALNA KANCELARIJA REVIZIJE / NATIONAL AUDIT OFFICE
DATE:PRANUAR/DORËZUAR: DATUM:PRIMLJEN/DOSTAVLJEN: DATE:RECEIVED/SUBMITTED: 9. 10. 2020

| Njësia Org. Org. Jedin. Org. Unit | Shifra klasif. Klasif. Kod Class. Code | Nr. Prot. Br. Prot. Prot. No. | Nr.i faqeve Br. Stranica No. Pages |
|---|---|---|---|
| 06 | 47 | 1786 | 18 |

ask

KOSOVO AGENCY OF STATISTICS
04-052-2463
1117
07.07.2020
PRISHTINË/PRIŠTINA/PRISTINA

Për Zyrën Kombëtare të Auditimit
Nga z. Isa Krasniqi, Kryeshef i Agjencisë së Statistikave të Kosovës

# PLANI I VEPRIMIT PËR ZBATIMIN E REKOMANDIMEVE

**të dhëna në Raportin e Auditimit nga Zyra Kombëtare e Auditimit**

## RAPORTI I AUDITIMIT TË TEKNOLOGJISË SË INFORMACIONIT NË AGJENCINË E STATISTIKAVE TË KOSOVËS QEVERISJA, MENAXHIMI I OPERACIONEVE DHE SIGURIA E SISTEMEVE

| Nr. | Gjetja/titulli | Rekomandimi | Njësia përgjegjëse për zbatimin e rekomandimit/Zyrtari/ët përgjegjës | Veprimet e planifikuara për tu ndërmarrë | Koha/Data e planifikuar e zbatimit të rekomandimit | |
|---|---|---|---|---|---|---|
| 1 | ASK-ja nuk kishte bërë një vlerësim adekuat të gjendjes ekzistuese të pajisjeve të TI-së dhe nevojave në fushën e TI-së | Vendosë politika dhe plane të menaxhimit të riskut, si dhe duhet të ketë të përcaktuar burimet e mjaftueshme dhe të drejtuara drejt zonave me përparësi për të minimizuar rreziqet në mënyrë që të mos rrezikohet objektivi i paraparë i organizatës; | Departamenti i Metodologjisë dhe TI-së | DMTI do të bëjë një vlerësim më të detajuar të gjendjes ekzistuese të pajisjeve të TI-së dhe nevojave në fushën e TI-së | Nëntor 2020 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | ASK-ja nuk ka arritur që të krijojë një ndarje adekuate të detyrave dhe përgjegjësive të stafit sa i përket fushës së teknologjisë së informacionit | Sigurohet që departamenti i TI-së të jetë i pozicionuar në atë mënyrë që ndarjet e detyrave të përfshijnë të gjitha funksionet për të arritur objektivat e ASK-së, duke iu përmbajtur parimeve/funksioneve të aprovimit, zhvillimit dhe kontrollimit për të shmangur konfliktin e interesit si dhe stafi me përgjegjësi të TI-së të menaxhohet në mënyrë të centralizuar; | Qeveria e Kosovës<br><br>Agjencia e Statistikave të Kosovës | ASK-ë do të bëjë përpjekje për mbulueshmëri me staf përkatës për të gjitha pozitat e nevojshme për funksionim normal të TI-së, si për pozitën administrator i bazës së të dhënave ashtu siç është e paraparë në përshkrimin e pozitave të punës, si dhe do bëjë përpjekje për shtimin e pozitave të reja për pozitat zhvillues softueri, zyrtar për siguri si dhe zyrtar për tavolinën ndihmëse (Help Desk).<br><br>Stafi i ri me përgjegjësi të TI-së në departamente të tjera do të menaxhohet në mënyrë të centralizuar nga divizioni i TI-së. | 2021-2022 | Kjo varet edhe nga institucionet e tjera jashtë ASK, se sa pozita të reja do ti aprovojnë. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 3 | ASK-ja nuk kishte të hartuara politika, procedura dhe procese të operimit të cilat do të orientonin funksionet e TI-së | Hartojë, të aprovojë dhe të komunikojë politikat, procedurat dhe proceset e operimit në mënyrë që të udhëzojnë funksionet e TI-së dhe njëkohësisht të mundësojnë mekanizma që sigurojnë që këto politika dhe procedura janë duke u ndjekur me qëllim të arritjes së objektivave të agjencisë; | Departamenti i Metodologjisë dhe TI-së dhe Departamentet e Statistikave Prodhuese | ASK-ja përveç GSBPM-it dhe udhëzimeve të ASHI-së, do të hartojë procedura dhe politika shtesë për të lehtësuar menaxhimin e proceseve të punës në ASK. | Prill, 2021 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 | ASK-ja nuk ka hartuar procedura dhe nuk ka zhvilluar procese dhe mekanizma lidhur me identifikimin, raportimin, trajtimin dhe menaxhimin e incidenteve dhe problemeve në sistemet e informacionit | Hartojë një procedurë lidhur me identifikimin, menaxhimin dhe trajtimin e incidenteve dhe problemeve të teknologjisë së informacionit, po ashtu të krijojë një proces apo sistem lidhur me mbledhjen, trajtimin, menaxhimin dhe ruajtjen e tyre, me qëllim të minimizimit të ndodhive të tilla në të ardhmen; | Divizioni i TI-së në ASK | DMTI do të zhvilloj dhe dokumentoj një sistemi për raportimin e problemeve. | Mars, 2020 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 5 | ASK-ja nuk ka të krijuar një proces lidhur me menaxhimin e ndryshimeve në sistemet e informacionit, përfshirë edhe menaxhimin e ndryshimeve emergjente që mund të ndodhin | Hartojë dhe ndjekë një procedurë të përcaktuar të menaxhimit të ndryshimeve, e cila kërkon aprovim përpara implementimit në mjedisin operacional, përfshirë edhe menaxhimin e ndryshimeve emergjente që mund të ndodhin. Procesi i menaxhimit të ndryshimit duhet të sigurojë që ndryshimet janë regjistruar, vlerësuar, autorizuar, renditur në bazë të rëndësisë, planifikuar, testuar, zbatuar, dokumentuar dhe rishikuar në përputhje me procedurat e dokumentuara dhe të aprovuara të menaxhimit të ndryshimit; | Departamenti i Metodologjisë dhe TI-së | ASK do të dokumentojë një procedurë për aprovim të kalimit të aplikacioneve nga sistemi testues në sistemin produktivë. | Qershor, 2020 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 6 | Testimet në aplikacionin për regjistrimin e anketave të bujqësisë janë bërë në ambientin produktiv, si dhe stafi përgjegjës për zhvillimin e sistemeve të informacionit ka qasje të vazhdueshme në sistemet e prodhimit | Të sigurohet që të gjitha testimet e aplikacioneve të bëhen në një ambient testues dhe vetëm pas testimit nga palët përgjegjëse, të njëjtat të kalojnë në ambient produktiv. Qasja në ndryshime të sistemeve në ambient produktiv të jetë e kufizuar; | Departamenti i Metodologjisë dhe TI-së | | Realizuar | *Gjatë periudhës së auditimit është bërë kjo gjetje vetëm për një aplikacion i cili ishte zhvilluar nga stafi i ri. DMTI do të sigurohet që edhe stafi ri të ndjek proceduar e njëjta.* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 7 | Në dy aplikacione të ASK-së, ka mungesë të vendosjes së rregullave të vlefshmërisë së të dhënave hyrëse në sisteme | Sigurohet që në aplikacionet e procedimit, rregullat e vlefshmërisë të jenë të hartuara, mirë, të dokumentuara dhe të zbatuara në ndërveprimin e të dhënave hyrëse; | Departamenti i Metodologjisë dhe TI-së | DMTI do të sigurohet që aplikacionet e zhvilluara nga stafi i ri të jenë të hartuara mirë me rregullat e vlefshmërisë, të dokumentuara dhe të zbatuara në ndërveprimin e të dhënave hyrëse. | Qershor, 2020 | *Pas identifikimit të mangësive nga ekipi i auditimit DMTI ka ndërmarr veprime për përmirësimet në pjesët e identifikuara.* |

| | | | | | | |
|---|---|---|---|---|---|---|
| **8** | ASK-ja nuk ka plan të vazhdimësisë së proceseve të punës në rast të ndonjë katastrofe natyrore, gabimi njerëzor apo dështimit të sistemeve të informacionit | Hartojë një plan të vazhdimësisë së biznesit sipas standardeve ndërkombëtare për të minimizuar ndikimin nga ndërprerja e operacioneve të punës (të mundshme) në një nivel të pranueshëm përmes një kombinimi të kontrolleve të parandalimit dhe rikuperimit; Përfshirja e menaxherëve të lartë të Agjencisë kërkohet në zhvillimin e procesit të administrimit të vazhdimësisë së biznesit duke e konsideruar atë si një projekt jo vetëm për TI-në; | Qeveria apo ASHI<br><br>Departamenti i Metodologjisë dhe TI-së | Në mbështetje të ASHI-së, ASK-ja do ta krijojë një plan të vazhdimësisë së proceseve të punës në rast të ndonjë katastrofe natyrore, gabimi njerëzor apo dështimit të sistemeve të informacionit.<br>ASK do të krijoj ekipet për reagim emergjent duke përcaktuar rolet dhe përgjegjësitë që duhet t'i ketë ekipi për reagim emergjent. | Korrik, 2021 | Kjo varet edhe nga realizimi në nivel të Qeverisë, respektivish ttë ASHI-së |

| | | | | | | |
|---|---|---|---|---|---|---|
| 9 | ASK-ja nuk kishte politikë të aprovuar dhe të komunikuar në lidhje me sigurinë e informacionit dhe nuk kishte të vendosura kontrolle shtesë mbi sigurinë e informacionit | Vendosë dhe të dokumentojë një politikë të qartë mbi sigurinë e informacionit në përputhje me objektivat e veprimtarisë dhe të demonstrojë mbështetjen dhe angazhimin për të. Politika të cilat mbulojnë të gjithë rreziqet e operacioneve dhe që sigurojnë mekanizma që ofrojnë mbrojtje në mënyrë të arsyeshme për të gjithë pasurinë e informacioneve kritike kundrejt humbjeve, dëmtimit dhe abuzimit; | Qeveria e Kosovës | ASK ka draftuar "Udhëzimin Administrativ për mbrojtjen e të dhënave statistikore dhe qasjen në të dhëna mikro", dhe pas aprovimit nga Qeveria e Kosovës pritet të zbatohet ky UA. | Dhjetor, 2020 | Proces i varur nga inztitucione t jashtë ASK-së |

| | | | | | | |
|---|---|---|---|---|---|---|
| **10** | ASK-ja shfrytëzon serverët CLOUD33 për regjistrimin e të dhënave pa ndonjë marrëveshje paraprake mbi sigurinë e të dhënave | Caktojë zyrtarin për mbrojtjen e të dhënave si dhe ASK-ja në bashkëpunim me Agjencinë e Shoqërisë së Informacionit dhe Agjencinë Shtetërore për Mbrojtjen e të Dhënave duhet të sigurohet që të dhënat e ndjeshme që procedohen në sistemin aktual nuk janë të ekspozuara ndaj palëve të paautorizuara dhe shfrytëzimi i sistemit është në përputhje me aktet ligjore në fuqi të Republikës së Kosovës: | Departamenti i Metodologjisë dhe TI-së | | I realizuar | *Pas procesit të ekzekutimit të auditimit, ASK-ja ka instaluar platformën në serverët lokalë. Të gjitha anketat administrohen nga serverët lokal. .* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 11 | ASK-ja nuk kishte të përcaktuar zyrtar për mbrojtjen e të dhënave | Caktojë zyrtarin për mbrojtjen e të dhënave si dhe ASK-ja në bashkëpunim me Agjencinë e Shoqërisë së Informacionit dhe Agjencinë Shtetërore për Mbrojtjen e të Dhënave duhet të sigurohet që të dhënat e ndjeshme që procedohen në sistemin aktual nuk janë të ekspozuara ndaj palëve të paautorizuara dhe shfrytëzimi i sistemit është në përputhje me aktet ligjore në fuqi të Republikës së Kosovës: | • Qeveria dhe Kuvendi i Kosovës | Pas aprovimit nga Qeveria dhe Kuvendi i Kosovës të kësaj pozite, ASK-ja sipas ligjit dhe dispozitave ligjore të shërbyesve civil, do ta konsideroj rekrutimin e një zyrtari për kontrollues dhe përpunues të të dhënave dhe do të plotësohen rekomandimet e kësaj pike, por gjithnjë duke pasur parasysh mundësitë dhe përkrahjet buxhetore, përkrahje kjo e cila ka pamundësuar realizimin edhe të disa pozitave tjera si të domosdoshme në divizionin e TI-së në ASK. | 2022 | Proces që varet nga institucionet e tjera dhe jo nga ASK-ja |

| | | | | | | |
|---|---|---|---|---|---|---|
| **12** | ASK-ja nuk ka të krijuar një program të vetëdijesimit dhe trajnimit lidhur me ndërgjegjësimin mbi sigurinë nga sulmet e mundshme kibernetike | Ketë një proces të shkruar, i cili ka për qëllim informimin/trajnimin, njohjen e detyrave dhe përgjegjësive të personelit mbi sigurinë e informacionit. Gjithashtu, ASK-ja duhet të sigurohet se personeli ka njohuritë e nevojshme mbi sigurinë e informacionit që prej rekrutimit të tij e deri në shkëputjen e marrëdhënies së punës, si dhe duhet të ruajnë sigurinë e informacionit; | Departamenti i Metodologjisë dhe TI-së | ASK-ja përkatësisht DMTI-ja, në bashkëpunim me projektin e EU-SIDA, si dhe në bashkëpunim me ASHI-në, do të përgatisë një plan i cili përfshin ngritjen e vetëdijes së zyrtarëve të ASK-së rreth mënyrës së shfrytëzimit të resurseve të Teknologjisë Informative, rrezikut që mund të vijë nga sulmet kibernetike dhe shfrytëzimi i pakontrolluar i e-mailit apo pajisjeve të tjera.<br><br>Divizioni i TI-së do inskenoj një sulm kibernetikë dhe paraqet rezultatet e përmbledhura në raport para KE të ASK-së. | **Tetor, 2021** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 13 | ASK-ja nuk kishte krijuar mekanizma për monitorimin e shfrytëzuesve të llogarive elektronike zyrtare | Krijojë mekanizma të nevojshëm për monitorimin e të gjithë shfrytëzuesve të llogarive elektronike zyrtare në artikulacion me njësinë e burimeve njerëzore dhe në harmoni me udhëzimet në fuqi. Gjithashtu, të sigurohet që hapja, ndryshimi dhe mbyllja e llogarive të bëhet sipas funksioneve të zyrtarëve, të sigurohet që llogaritë të jenë unike dhe të personalizuara, fjalëkalimet të ndërrohen në periudha të caktuara kohore, si dhe gjurmët për çfarëdo transaksioni të jenë të identifikueshme; | DMTI-ja | I realizuar | Prill, 2020 | *Pas procesit të ekzekutimit të auditimit, çdo zyrtarit i që i përfundon/ndërpritet/pezullohet marrëdhënia e punës, ndërron vendin e punës apo ndërron të dhënat, njësia e personelit është duke informuar obliguar administratorin e llogarive zyrtare të institucionit përkatës, i cili bënë veprimet e nevojshme për mbylljen e* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 14 | ASK-ja nuk i kishte të gjitha llogaritë zyrtare elektronike unike dhe të personalizuara | Krijojë mekanizma të nevojshëm për monitorimin e të gjithë shfrytëzuesve të llogarive elektronike zyrtare në artikulacion me njësinë e burimeve njerëzore dhe në harmoni me udhëzimet në fuqi. Gjithashtu, të sigurohet që hapja, ndryshimi dhe mbyllja e llogarive të bëhet sipas funksioneve të zyrtarëve, të sigurohet që llogaritë të jenë unike dhe të personalizuara, fjalëkalimet të ndërrohen në periudha të caktuara kohore, si dhe gjurmët për çfarëdo transaksioni të jenë të identifikueshme; | DMTI-ja në ASK | Në kuadër të projektit EU-SIDA është drafluar "Politika e fjalëkalimit", një dokument i detajuar i cili i adreson të gjitha çështjet që kanë të bëjnë me fjalëkalimet, sigurinë e tyre, kompleksitetin dhe kohëzgjatjen. | realizuar | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | *llogarive elektronike siç është e parapaë me UA 02/2015 neni 7.* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 15 | Një të tretës së llogarive zyrtare elektronike në ASK nuk u kërkohej të ndryshonin fjalëkalimin | Krijojë mekanizma të nevojshëm për monitorimin e të gjithë shfrytëzuesve të llogarive elektronike zyrtare në artikulacion me njësinë e burimeve njerëzore dhe në harmoni me udhëzimet në fuqi. Gjithashtu, të sigurohet që hapja, ndryshimi dhe mbyllja e llogarive të bëhet sipas funksioneve të zyrtarëve, të sigurohet që llogaritë të jenë unike dhe të personalizuara, fjalëkalimet të ndërrohen në periudha të caktuara kohore, si dhe gjurmët për çfarëdo transaksioni të jenë të identifikueshme; | DMTI-ja | Në kuadër të projektit EU-SIDA është draftuar "Politika e fjalëkalimit", një dokument i detajuar i cili i adreson të gjitha çështjet që kanë të bëjnë me fjalëkalimet, sigurinë e tyre, kompleksitetin dhe kohëzgjatjen. | Realizuar | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **16** | ASK-ja nuk ka një proces të definuar lidhur me aprovimin e qasjeve në sisteme, të dhëna, informacione, pajisje periferike | Sigurohet se masat organizative dhe fizike sigurojnë parandalimin e qasjeve të paautorizuara. Gjithashtu, duhet të sigurohet që USB, CD ROM dhe mënyra të tjera të futjes së informacionit në infrastrukturën e TI-së janë të bllokuara dhe ose lejohen vetëm pasi informacioni vlerësohet i pastër; | DMTI-ja | Në kuadër të projektit EU-SIDA është draftuar "Politika për mediumet e lëvizshme USB/CD etj" një dokument i detajuar i cili e adreson këtë çështje. Fillimisht është filluar si "pilot" duke mos lejuar qasjen në USB të zyrtarit i cili ka qasje në të dhëna sensitive që kanë të bëjnë me ATK-në. | Realizuar | |