



TERMAT E REFERENCËS

PËR

**ZGJERIMIN E INFRASTRUKTURËS IT, RITJEN E NIVELIT TË SIGURISË
DHE ADMINISTRIMIN E QENDËRZUAR TË AKSESIT NË RRJETET E
KOMUNIKIMIT NË KESH SHA**

FAQJA E KONTROLLIT TË DOKUMENTIT

HISTORIKU I VERSIONEVE DHE NDRYSHIMEVE TË DOKUMENTIT

Data	Autori	Versioni	Shënime mbi Rishikimet
		1.0	Përpilimi origjinal i TORs
		1.0	Përpilimi origjinal i TORs

NËNSHKRIMET MIRATUESE

Përgatiti:

<Nënshkrimi>

Përgatiti:

<Nënshkrimi>

Kontrolloi:

Mbikqyrësi i Projektit

<Nënshkrimi>

Përmbajtja	
FAQJA E KONTROLLIT TË DOKUMENTIT	2
HISTORIKU I VERSIONEVE DHE NDRYSHIMEVE TË DOKUMENTIT	2
NËNSHKRIMET MIRATUESE	2
1. Hyrje	5
1.1. Përfituesi /Autoriteti Kontraktues	5
1.2. Historiku	5
1.3. Situata Aktuale	5
2. Objektivat, risqet, qëllimi dhe rezultatet e pritura	6
2.1 Objektivi i Përgjithshëm	6
2.2 Qëllimi	7
2.3 Rezultatet që duhet të arrihen nga kontraktori	8
2.4 Supozimet e Projektit	9
2.5 Rrisqet	9
2.6 Hapsira gjeografike dhe vendodhja	9
3. Detyrat specifike	9
3.1. Përcaktimi i planit të punës për ekzekutimin e projektit	10
3.2. Ngritja e grupeve të punës nga të dyja palët e interesuara	10
3.3. Mbledhja, specifikimi dhe dokumentimi i analizës së kërkesave	10
3.4. Realizim punime civile jo të specializuara	10
3.5. Spostim të pajisjeve ekzistuese dhe riorganizim të dhomës së serverave	11
3.6. Furnizim dhe vendosje i pajisjeve të reja në dhomën e servereve dhe dhomën teknike	11
3.7. Dizenjimi dhe përcaktimi i infrastrukturës së rrjetit	12
3.8. Implementimi i zgjidhjes wireless	12
3.9. Implementimi i zgjidhjes së sigurisë	12
3.10. Integrimi me infrastrukturën ekzistuese	12
3.11. Përgatitja e manualeve udhëzuese dhe trajnimi i përdorueseve për politikat e sigurisë	12
3.12. Raportimi i çdo faze të projektit	12
3.13. Dokumentimi përfundimtar dhe marrja në dorëzim	12
4. Logjistika dhe koha	13
4.1. Vendndodhja	13
4.2. Data e Fillimit dhe Periudha e Implementimit të Detyrave	13
5. Raportimi	13
5.1. Kërkesat e Raportimit	13
5.2. Dorëzimi dhe Miratimi i Raporteve	13
6. Planifikimi i buxhetit për levrimin e projektit	14
7. Kërkesat Funktionale	14
7.1. Funkcionalitete dhe bllokskema të infrastrukturës	16
7.2. Kërkesat funksionale për zgjidhjen teknike mbi kontrollin e aksesit në rrjet	16
7.3. Kërkesat funksionale për përmirësim të rrjetit LAN të HQ	18
7.4. Kërkesat funksionale për zgjidhjen teknike mbi Sistemin e menaxhimit dhe supervizimit për pikat e aksesit radio	18
7.5. Kërkesat funksionale për zgjidhjen teknike mbi rrjetin e aksesit	19
7.6. Shërbimet e kërkuara	20
8. Specifikimet Teknike	20
8.1. Pikë aksesi radio	21

8.2.	Platformë për kontrollin e pikave të aksesit radio (Virtual)	22
8.3.	Switch aksesi	24
8.4.	Platformë Sigurie për kontrollin e aksesit në rrjet (Virtual)	25
8.5.	Derë zjarrduruese.....	27
8.6.	Dysheme teknologjike	27
8.6.1.	Pllakat	27
8.6.2.	Aksesorët e ajrimit	27
8.6.3.	Rampë ose Shkallë	28
8.7.	Sistemi i shuarjes së zjarrit	28
8.7.1.	Paneli i kontrollit.....	28
8.7.2.	Detektorët e tymit dhe të temperaturës	28
8.7.3.	Butonat e aktivizimit dhe ndalimit manual	29
8.7.4.	Pajisjet e sinjalizimit	29
8.7.5.	Sprucatorët	29
8.7.6.	Cilindri dhe agjenti i shuarjes	29
8.8.	Sistemi i monitorimit	30
8.9.	Sistemi i kontrollit të aksesit.....	31
8.10.	Sistemi CCTV	31
8.11.	Sistemues kabllorsh horizontale.....	31
8.12.	Sistemues kabllorsh vertikale.....	31
8.13.	Patch Cord OM5	31
8.14.	Patch Cord ethernet Cat.6A	32
9.	Dorëzimi i dokumentacionit	32

1. Hyrje

1.1. Përfituesi /Autoriteti Kontraktues

Korporata Elektroenergjetike Shqiptare (KESH sh.a), është një shoqëri tregtare aksionere shtetërore e integruar vertikalisht dhe është prodhuesi kryesor dhe më i rëndësishëm i energjisë elektrike në Shqipëri, që administron dhe operon hidrocentralet e kaskadës së lumit Drin (HEC-Fierzë, HEC-Koman, HEC-Vau i Dejës) të cilët janë të rëndësishëm së veçantë për ekonominë e vendit.

1.2. Historiku

Korporata Elektroenergjetike Shqiptare synon në mënyrë të vazhdueshme të përmirësojë infrastrukturën e aksesit të rrjetit internet si dhe të rrisë nivelin e sigurisë e administrimit e aksesit në rrjetat e komunikimit në funksion të miradministrimit dhe rritjes së efikasitetit të korporatës. Për këtë qëllim gjatë viteve janë kryer investime të rëndësishme në këtë sektor.

1.3. Situata Aktuale

Në ditët e sotme është rritur shumë përdorimi i pajisjeve mobile siç janë Laptop, tableta, telefona smart, etj, nga përdorues të organizatës apo edhe vizitorë. Për rrjedhojë është rritur nevoja për lidhjen e këtyre pajisjeve në rrjet me qëllim shkëmbimin e informacionit. Një pjesë e këtyre pajisjeve janë legjitime për të shfrytëzuar informacioni i cili ruhet në infrastrukturën e brendshme të sistemeve ku kërkohet një nivel i lartë i sigurisë, ndërsa për disa të tjera është e nevojshme vetëm akses i sistemeve në perimetrat DMZ apo vetëm thjesht akses në Internet. Lidhja e këtyre pajisjeve në rrjet shton edhe rrezikun që këto pajisje mund të induktojnë në rrjetin e brendshëm. Përdoruesit mund të lidhin pajisje të ndryshme në rrjet siç mund të jenë pikat e aksesit radio apo pajisje mobile personale pa dijeninë e administratorëve të rrjetit duke krijuar në këtë mënyrë pika aksesit vulnerabël të cilat mund të shfrytëzohen mjaft lehtë nga keqdashës. Aktualisht në infrastrukturën e rrjetit nuk ka vizibilitet dhe kontroll mbi pajisjet të cilat lidhen në rrjetin kabllor dhe radio. Për rrjedhojë nuk është e dukshme në atë çka po ndodh në rrjet, si p.sh. kush është i lidhur, cilat aplikacione janë instaluar dhe ekzekutuar. Nuk ka informacion mbi identitetet e përdoruesve dhe pajisjeve, kërcënimet dhe dobësitë të cilat ekzistojnë në rrjet në mënyrë që të mund të identifikohen, kontrollohen dhe të korrigjohen kërcënimet sa më shpejt të jetë e mundur.

Shpesh here nevojitet të mundësohet akses në rrjet për pajisjet e vizitoreve. Mënyra e qasjes në rrjet për vizitorët kryhet në po të njëjtattribute si përdoruesit e brendshëm duke mos patur mundësi për ti diferencuar dhe për ti dhënë aksese të veçanta në rrjet. Nëse pajisjet e vizitoreve janë të infektuar dhe qasen në të njëjtin rrjet me përdoruesit e brendshëm, kjo mund të shkaktojë probleme serioze në rast se nuk ka një mekanizëm i cili arrin të parandalojë këtë efekt negativ. Në infrastrukturën aktuale nuk ka një sistem automatik i cili të mund të garantojë aksesin e vizitoreve në rrjet. Meqenëse sasia e informacionit që shkëmbehet në ditët e sotme është e lartë, nevojitet një infrastrukturë aksesit radio e cila ofron kapacitetet e duhura për të suportuar ngarkesën e trafikut. Infrastruktura ekzistuese bazohet mbi protokolle të vjetërsuar radio dhe nuk garanton kapacitetet fizike për të transferuar throughput të lartë. Për të zgjidhur problemet e evidentuara është e nevojshme implementimi i një zgjidhje teknike e cila mund të bllokojë aksesin në rrjet për ato

pajisje të cilat nuk janë në përputhje me politikat e sigurisë ose t'iu japë pajisjeve akses të limituar me qëllim sigurimin e rrjetit nga risqet që mund të injektohen. Gjithashtu kjo zgjidhje duhet të garantojë kapacitete teknike për të mundësuar transferimin e shpejte të informacionit.

Gjithashtu Korporata Elektroenergjitike Shqiptare ka një dhomë serveresh ekzistuese në të cilën janë të instaluar:

- 4 kabinate rack me permasa 42U 600 mm x 1000 mm
- 3 x sisteme ftohje precision cooling
- 1 x sistem shuarje zjarri
- 1 x UPS tower
- 1 x sistem CCTV dhe kontroll aksesi

Dhoma është e pajisur me dysheme teknologjike. Dimensionet e dhomës së serverave janë 274 cm x 570 cm. Rack në dhomën e serverave janë të pozicionuar në mesin e dhomës, dhe janë të pozicionuar në trajte jo të rregullt. Nderlidhja e paisjeve me njera tjetren është realizuar me patch corda bakri (ethernet) dhe fibër optike, të pa organizuara, të pa-etiketuara dhe pa përdorur organizues kabllorsh. Pllakat e dyshemese teknologjike, janë amortizuar duke përbërë rrezik për aktivitetet në vijim (instalime dhe mirembajtje).

2. Objektivat, risqet, qëllimi dhe rezultatet e pritura

2.1 Objektivi i Përgjithshëm

Objektivi i përgjithshëm i projektit është implementimi i një zgjidhje të re të infrastrukturës wireless e cila do të bëjë upgrade të ekzistueses duke ofruar funksionalitete dhe veçori të reja. Një tjetër objektivi është implementimi i një zgjidhje të re për të zhvilluar me tej politikat e sigurisë të infrastrukturës wired si dhe wireless e cila do duhet të integrohet me infrastrukturën ekzistuese. Gjithashtu, duhet të realizohet integrimi me rrjetin ekzistues për pajisjet Layer 2 si dhe Layer 3. Për efekt të zgjerimit të infrastrukturës IT fizike, duhet të realizohet riorganizimi i dhomës ekzistuese të serverave nëpërmjet zgjerimit me një ambient tjetër shtesë, ngjitur me dhomën ekzistuese. Ambienti i ri, do të përdoret si dhomë teknike ndërsa server room aktual do të përdoret vetëm për “hostimin” e pajisjeve IT.

Në dhomën teknike duhet të vendosen pajisjet si mëposhtë:

- 3 x sisteme ftohje precision cooling (transferim i sistemit ekzistues)
- 1 x UPS tower (transferim i UPS ekzistues)
- 1 x sistem shuarje zjarri (furnizim dhe vendosje i një sistemi të ri)
- 1 x sistem CCTV dhe kontroll aksesi (furnizim dhe vendosje i sistemeve të reja)

Sistemet e ftohjes, dhe UPS janë momentalisht të instaluar dhe funksional brenda dhomës së serverave, dhe duhet të transferohen në ambientin e ri, dhomë teknike. Njesite e jashtme të kondicionereve nuk do të spostohen. Ato do të qëndrojnë në vendet aktuale. Duhet të kryhet lidhja e njesive të jashtme me njesite e brendshme respektive në pozicionet e reja në dhomën teknike (duhet të bëhet zgjatim i tubave të bakrit nga pozicioni aktual i njesive të ftohjes deri tek pozicioni i ri). Paneli elektrik i dhomës së serverave nuk do të ndryshojë, por linjat elektrike të furnizimit me energji të sistemeve ftohese do të instalohen nga paneli ekzistues deri tek pozicioni i ri i njesive ftohese). Instalimet e brendshme elektrike në dhomën aktuale të serverave nuk do të ndryshojnë. Duhet të instalohen vetëm linjat hyrje/dalje të UPS nga pozicioni i ri në dhomën teknike, deri në panelin elektrik ekzistues. Ambienti i ri, i cili do të përdoret si dhomë teknike për UPS dhe sistemin

e ftohjes, ndodhet në dhomën ngjitur me dhomën ekzistuese të serverave. Dimensionet e këtij ambienti janë 427 cm x 337 cm, dhe lartësi 2.8 m (nga dyshemeja deri në tavan). Ky ambient nuk është i pajisur me dysheme teknologjike.

2.2 Qëllimi

Qëllimi i kësaj kontrate është gjetja e një kontraktori me përvojë, i cili do të ofrojë një zgjidhje profesionale dhe të qëndrueshme, në funksion të kërkesave të mëposhtme të KESH SH.A. Qëllimi kryesor i këtij projekti është zëvendësimi i infrastrukturës aktuale me një infrastrukturë wireless të re bazuar mbi teknologjinë WIFI-6, e cila duhet të mundësojë performancë me të mire, kapacitet të lartë dhe funksione të reja duke ofruar një eksperiencë me të mire për përdoruesit e rrjetit wireless.

Disa nga veçoritë kryesore që duhet të ofrojë zgjidhja teknike për infrastrukturën wireless janë:

- Rritje të sigurisë në ndërfaqen wireless, për përdoruesit dhe pajisjet.
- Integrimi i Infrastrukturës së re Wireless me sistemin e sigurisë për kontrollin e aksesit për autentifikim të sigurt për të gjitha Wireless SSID.
- Implementim i kësaj infrastrukture me wireless controller të cilët mund të instalohen në infrastrukturën ekzistuese.
- Akses Point-e të cilët ofrojnë shume veçori të reja dhe mundësi për tu bere upgrade në të ardhmen.
- Mundësi për tu automatizuar duke përdorur një set të gjere të ndërfaqeve standarte API.

Gjithashtu, ky projekt duhet të përmirësojë sigurinë e Infrastrukturës në tërësi, nëpërmjet dhe implementimit të një sistemi të sigurisë për kontrollin e aksesit në rrjet.

Vec të tjerash duhet të mundësohet:

- implementimi i politikave BYOD – Bring Your Own Device,
- Integrimi i Infrastrukturës aktuale AD me zgjidhjen e propozuar mbi sistemin e sigurisë për kontrollin e aksesit,
- prezantimi i politikave të sigurisë për VPN users
- prezantim dhe konfigurim i politikave të sigurisë për përdoruesit e rrjetit kabllor (Wired users) sipas departamenteve përkatëse,
- autentifikim i sigurt i sensoreve (apo IoT Devices),
- implementimi i portaleve të autentifikimit të sigurt Guest dhe Sponsor përmes “HTTPS redirect” etj.

Projekti duhet të mundësojë:

- performancë me të mire,
- nivel sigurie të lartë,
- koleksionim i device Information përmes funksionalitetit të sistemit të sigurisë për kontrollin e aksesit për menaxhimin e aseteve të KESH,
- autentifikim i përdoruesave Guest dhe atyre të lidhur me AD përmes “HTTPS-SSL enabled portals”, BYOD portals për përdoruesit që sjellin pajisjet e tyre në zyrat e korporatës
- autentifikim i sigurt për përdoruesit Guest përmes Guest portal

Disa nga veçoritë kryesore që duhet të mundësojë sistemi i sigurisë për kontrollin e aksesit janë si me poshtë:

- Vizibilitet i aseteve të kompanisë
- Aksese të ndryshme sipas kontentit
- Aplikim apo zbatim i politikave të sigurisë mbi aksesin

-
- Metoda aksesi për përdoruesit Guest me anë të “Guest Portals & Sponsor Portals”
 - Funkcionalitet BYOD
 - Verifikim i automatizuar mbi pajtueshmërinë e pajisjeve
 - Politika sigurie aksesi
 - TrustSec Group Based Policy – Markim i paketave sipas sistemit të sigurisë për kontrollin e aksesit
 - Auditim i pajisjeve
 - Koleksionim informacioni rreth pajisjeve të përdorura në korporatë – “Profiling”
 - Vendosja e politikave të detajuara të sigurisë në nivel aplikacioni apo rregjistrash – “Posture Services”

Tjetër qëllim i projektit është si me poshtë:

- Lirim i hapësirave në dhomën ekzistuese të serverave, në mënyrë që të lejojë shtimin e rack dhe paisjeve të reja. Momentalisht është e pamundur që në dhomën e serverave të shtohet një rack i ri për vendosjen e paisjeve të reja.
- Riorganizim i rack-eve ekzistues në server room, në mënyrë që të rritet eficensa e sistemit të ftohjes, e cila automatikisht përkthehet në me pak konsum energjie elektrike.
- Sistemimi i paisjeve nëpër racke dhe etiketimin e tyre, për të lehtësuar operimin, mirembajtjen dhe ndryshimet që mund të nevojiten.
- Sistemimi i kabllimeve ndërmjet rackeve, lidhja e paisjeve me patch corda baker (ethernet) dhe fibër optike me patch panelet përkatëse, si edhe etiketimet e të gjitha patch cordave, për të lehtësuar operimin, mirembajtjen dhe ndryshimet që mund të nevojiten.
- Ndarje në dy ambiente të dedikuara të pajisjeve IT dhe pajisjeve teknike. në server room duhet të jenë të instaluar vetëm pajisjet IT (servera, storage, pajisje telekomunikacioni), ndërsa në dhomën teknike duhet të jenë të instaluar sistemet teknike që garantojnë kushtet operacionale të pajisjeve IT.

2.3 Rezultatet që duhet të arrihen nga kontraktori

Rezultatet që priten të arrihen gjatë zbatimi të kësaj kontrate janë si me poshtë:

- Përbushja e të gjitha kërkesave funksionale dhe teknike të paraqitura nga KESH në këtë dokument brenda afatit kohor.
- Dokumentim i plotë i çdo faze të projektit dhe raportim të autoriteti kontraktues
- Implementimin e AP-ve wireless dhe një kontrolleri wifi për menaxhimin e tyre.
- Implementimin e sistemit të sigurisë për kontrollin e aksesit me 2 node për të arritur disponueshmeri të lartë duke ndare shërbimet midis nodeve në Active dhe Standby.
- Implementimin e funksionalitetit të RADIUS për pikat e mëposhtë:
 - Wired 802.1X Authentication/Authorization/Auditing.
 - Wireless 802.1x Authentication/Authorization/Auditing.
 - Implementim i BYOD për pajisjet Wireless.
 - Aktivizim i politikave BYOD për përdoruesit që sjellin pajisje të reja On-premise.
 - Implementim i “Profiling” i cili të bëjë të mundur raportimin e të dhënave të detajuara në sistemin e sigurisë për kontrollin e aksesit Dashboards për onboarded devices.
 - Guest Access përmes Guest portals dhe Sponsor Portals.
 - Implementimi i autentikimit bazuar mbi MAC për pajisjet e vjetra.
 - Implementimi i “Dual factor authentication” përmes sistemit të sigurisë për kontrollin e aksesit për përdoruesit e lidhur nga VPN.
- Realizim punime civile jo të specializuara sipas detajeve të mëposhtme

-
- Realizim punime për spostim të paisjeve ekzistuese dhe riorganizim të dhomës së serverave
 - Implementim sistem i detektimit dhe fikjes së zjarrit
 - Implementim sistem i monitorimit, kontrollit dhe menaxhimit
 - Implementim sistem akses kontrolli
 - Implementim sistem i videomonitorimit CCTV

2.4 Supozimet e Projektit

Supozimet kryesore për suksesin e Projektit:

- Kontraktimi i nje kontraktori me eksperiencën e nevojshme në implementimin dhe upgrade të zgjidhjeve të infrastrukturës wireless duke ofruar funksionalitete dhe veçori të reja si dhe në implementimin e zgjidhjeve të reja të politikave të sigurisë të infrastrukturës wired dhe wireless.
- Kontraktimi i nje kontraktori me eksperiencën e nevojshme në implementimin dhe zgjerimin e infrastrukturës IT
- Angazhim dhe mbeshtetje e plotë nga personat e përfshirë në zbatimin e kontrates;
- Qasje e plotë dhe e detajuar në infrastrukturën TIK aktuale në ambientet e godines së zyrave qendrore të KESH sha.

2.5 Rrisqet

Rreziqet kryesore që duhen marre në konsiderate përfshijne:

- Disponueshmeria e informacioneve mbi gjendjen e infrastrukturës aktuale
- Integrimi me infrastrukturën ekzistuese
- Feedback objektiv dhe i sakte nga personeli i KESH i përfshirë në zbatimin e kontrates
- Alokimi i burimeve njerezore të nevojshme për implementimin e ketij projekti

2.6 Hapsira gjeografike dhe vendodhja

Shërbimet dhe produktet e kërkuara do të lëvrohen dhe implementohen në Zyrat Qendrore të KESH SHA, Tirane.

3. Detyrat specifike

Ne kuader të qëllimit kryesor të ketij projekti, i gjithë projekti do të ndërtohet mbi detyrat e mëposhteme:

1. Përcaktimi i planit të punës për ekzekutimin e projektit
2. Ngritja e grupeve të punës nga të dy palët e interesuara
3. Mbledhja, specifikimi dhe dokumentimi i analizës së kërkesave
4. Planifikimi dhe realizimi i punimeve për zgjerimin e infrastrukturës IT
5. Dizenjimi dhe përcaktimi i infrastrukturës së rrjetit
6. Implementimi i zgjidhjes wireless
7. Implementimi i zgjidhjes së sigurisë
8. Integrimi me infrastrukturën ekzistuese

-
9. Përgatitja e materialeve udhëzuese dhe trajnimi i përdoruesve për politikat e sigurisë
 10. Raportimi i çdo faze të projektit të menaxheret e projektit ose ndjekësit e kontratës.
 11. Dokumentimi dhe marrja në dorëzim e zgjidhjes

3.1. Përcaktimi i planit të punës për ekzekutimin e projektit

- Planifikimi i burimeve njerezore dhe materialeve të nevojshme për realizimin e projektit.
- Realizimi i nje plani të detajuar mbi zhvillimin e projektit dhe implementimit të zgjidhjes teknike.
- Realizimi i dokumentacionit teknik ku të detajohet dhe percaktohet me saktësi skema dhe arkitektura e zgjidhjes së propozuar për implementimin e zgjidhjes teknike për të qene sa me e pershtatur me nevojat aktuale.

3.2. Ngritja e grupeve të punës nga të dyja palët e interesuara

- Identifikimi i specialisteve të punës brenda KESH sh.a dhe krijimi i grupit të punës.
- Identifikimi i specialisteve të punës nga kontraktori sipas kërkesave teknike.
- Koordinimi dhe shkembimi i kërkesave midis dy grupeve të punës

3.3. Mbledhja, specifikimi dhe dokumentimi i analizës së kërkesave

- Mbledhja e kërkesave funksionale dhe teknike nga departamenti IT i KESH sh.a sipas kërkesave teknike.
- Analizimi i kërkesave.
- Dokumentimi i kërkesave dhe konfirmimi në grupin e punës

3.4. Realizim punime civile jo të specializuara

1. Zgjerim i derës ekzistuese të ambientit të ri, që do të perdoret si dhome teknike. Ky ambjent momentalisht është me derë me gjerësi 90 cm. Duhet të hiqet dera ekzistuese dhe të vendoset një derë e re zjarrduruese me gjerësi 120 cm.
2. Patinim dhe lysterje e mureve në ambientin e ri dhe në dhomën ekzistuese të serverave.
3. Trajtim i dyshemese në ambientin e ri (lysterje me boje kunder lageshtise dhe pluhurit).
4. Ri-nivelim i dyshemese teknologjike ekzistuese në dhomën e serverave dhe pastrimi i saj.
5. Instalim i dyshemese teknologjike në ambientin e ri. të dy dhomat jane në të njejtin nivel, dhe dyshemeja që duhet të instalohet në ambientin e ri duhet të jete në të njejten lartësi me dyshemene e dhomës ekzistuese të serverave. Dyshemeja ekzsituese është në lartësine 40 cm e perfunduar.
6. Instalim i sistemit të ndricimit në ambientin e ri. Vendorsja e kater ndricuesve LED 60 cm x 60 cm me kase të jashtme, direkt në tavan.
7. Zëvendësim i ndricuesve ekzistues (neona fleuroshente) me kater ndricues LED me dimensione 60 cm x 60 cm në dhomën e serverave.
8. Mbyllja e dritës së ambientit për të arritur standartin e kërkuar

3.5. Spostim të pajisjeve ekzistuese dhe riorganizim të dhomës së serverave

1. Spostim i tre njesive të sistemit të ftohjes ekzistues në ambientin e ri.
Njesite e brendshme ekzistuese të sistemit të ftohjes duhet të vendosen në dhomën teknike mbi dyshemene teknologjike, ngjitur me murin ndares midis dhomës së serverave dhe dhomës teknike. Nen dyshemene teknologjike, në murin ndares midis dhomës së serverave dhe dhomës teknike, duhet të hapen 3 zgavra ajri me dimensione 30 x 60 cm, që të lejojnë ajrin e ftohte që fryhet nen dysheme nga njesite e sistemit të ftohjes të kalojë në dhomën e serverave. Ndërsa mbi njesite e sistemit të ftohjes, në murin ndares midis dhomës së serverave dhe dhomës teknike, duhet të hapen 3 zgavra ajri me dimensione 30 cm x 60 cm që të lejojnë thithjen e ajrit të ngrohte që çlirohet nga dhoma e serverave. Zgavrat e hapura duhet të pajisjen me grila ajrimi murale. Njesite e jashtme të sistemit të ftohjes nuk duhet të spostohen, por do të zgjaten vetëm tubat e bakrit nga dhoma ekzistuese e serverave deri tek pozicioni i ri ku do të instalohen njesite e ftohjes në dhomën teknike. Gjithashtu linjat elektrike për furnizimin me energji të njesive të jashtme nuk duhet të nderrohen. Duhet të instalohen të reja vetëm linjat e furnizimit për 3 njesite e brendshme nga paneli elektrik ekzistues deri tek pozicioni i ri i njesive të brendshme në dhomën teknike.
2. Spostim i UPS ekzistues nga dhoma e serverave në ambientin e ri në dhomën teknike. Paneli elektrik ekzistues i dhomës nuk duhet të ndryshohet. Duhet të behen të reja vetëm linja e hyrjes dhe linja e daljes nga paneli elektrik ekzistues deri tek pozicioni i ri i UPS.
3. Ripozicionim i 4 kabineteve ekzistues në dhomën e servereve ekzistuese. Kabllimet janë realizuar nen dysheme, dhe ka rezerva të mjaftueshme për levizje të kabineteve. Pozicionimi i kabineteve brenda dhomës ekzistuese duhet të behet në një formë të tillë, që të optimizohet ftohja e pajisjeve të instaluar në kabinete, të rritet eficensa e sistemit të ftohjes, e cila automatikisht ndikon në uljen e konsumit të energjisë elektrike. KESH sh.a, kërkon riorganizimin e kabineteve. Tre prej kabineteve ekzistuese janë me lartësi 42U, 600 mm x 1000 mm, dhe një kabinet ekzistues është me dimensione 42U, 800 mm x 1000 mm. Kabinetet ekzistuese janë me dyer të perforuara para dhe mbrapa. Dyert mbrapa janë vertikalisht të ndara. Kapaket anesore të kabineteve mund të hiqen. Kabinetet kanë shina vertikale të cilat lejojnë bashkimin e kabineteve me njëri tjetrin dhe kanë kembe të rregullueshme të cilat mund të hiqen për tu mbeshetur direkt në dyshemene teknologjike. Operatorët ekonomike, janë të lire të ofrojnë zgjidhjen e tyre, duke përdorur çfaredo lloj aksesori që ata shohin të nevojshme, duke pasur parasysh që të plotësohen kërkesat e mëposhtme:
 - Ne dysheme teknologjike, para rreshtit të kabineteve të ketë grila ajrimi që lejojnë fryrjen e ajrit të ftohte përpara rack-eve. Grilat duhet të kenë permasa 60 cm x 60 cm.
4. Riorganizim i kabllimeve brenda kabineteve ekzistuese. Sistemim i patch cordave të bakrit (ethernet) dhe të patch cordave fibër optike. Instalim i sistemuesve vertikal dhe horizontal në secilin prej kabineteve. Etiketim i të gjitha kablllove.

3.6. Furnizim dhe vendosje i pajisjeve të reja në dhomën e servereve dhe dhomën teknike

1. Zëvendësim i dorezave dhe bravave të rack-eve ekzistues, me doreza rrotulluese të pajisura me lexues RFID dhe me brave elektrike/magnetike.
2. Instalim i një sistemi shuarje zjarri me agjent të paster në ambientin e ri (dhoma teknike).
3. Instalim i një sistemi monitorimi për të dy ambientet, dhomën e serverave dhe dhomën teknike.
4. Instalim i sistemit CCTV dhe kontrollit të aksesit në dhomën teknike.
5. Instalim i kontrollit të aksesit në dhomën e serverave dhe në raket e dhomës së serverave

3.7. Dizenjimi dhe përcaktimi i infrastrukturës së rrjetit

- Analizimi i kërkesave për infrastrukturën e rrjetit
- Paraqitja në mënyrë skematike e infrastrukturës së rrjetit.
- Dizenjimi i skemes teknike dhe logjike të rrjetit.
- Përgatitja e ambienteve të punës.

3.8. Implementimi i zgjidhjes wireless

- Implementimi i zgjidhjes, në perputhje me kërkesat teknike të percaktuara, duke respektuar standardet dhe praktikat me të mira për implementimin e rrjetave wireless.

3.9. Implementimi i zgjidhjes së sigurisë

- Implementimi i sigurisë së infrastrukturës kabllore si dhe wireless, nëpërmjet dizenjimit dhe Implementimit të një sistemi të sigurisë për kontrollin e aksesit.

3.10. Integrimi me infrastrukturën ekzistuese

- Vlerësim i infrastrukturës ekzistuese të rrjetit dhe sistemeve në ambientet e godines qendrore të KESH sha.
- Integrimi me infrastrukturën ekzistuese
- Integrimi me rrjetin ekzistues për pajisjet Layer 2 si dhe Layer 3.

3.11. Përgatitja e manualeve udhëzuese dhe trajnimi i përdorueseve për politikën e sigurisë

- Identifikim i nevojave për trajnim dhe materialeve të nevojshme për trajnim.
- Organizim i trajnimeve për administratoret e sistemit.
- Dorëzimi i manualeve të përdorimit.

3.12. Raportimi i çdo faze të projektit

Kompleksiteti dhe rëndësia e implementimit të kësaj zgjidhjeje teknike do të kërkojë një koordinim dhe bashkepunim të ngushtë midis kontraktorit dhe specialistëve të KESH sh.a. për të patur koherencë në vendimmarrje dhe zhvillim dhe për të eliminuar keqkuptimet që mund të lindin, do të duhet që çdo fazë e zbatimit të projektit të ndiqet nga përfaqësuesit e të dy paleve të shoqeruara me raportet përkatëse.

3.13. Dokumentimi përfundimtar dhe marrja në dorëzim

- Testimi i zgjidhjes teknike sipas planit dhe dokumentimi i rezultateve.

-
- Dokumentimi i zgjidhjes teknike të aplikuar
 - Dorëzimi i dokumentacioneve përfundimtare dhe fatures
 - Marja në dorëzim nga autoriteti kontraktor
 - Mbyllja e projektit

4. Logjistika dhe koha

4.1. Vendndodhja

Takimet e punës, instalimet dhe konfigurimet do zhvillohen në Zyrat Qendrore të KESH sh.a, Tirane. KESH sh.a do të ofrojë akseset e nevojshme si dhe mbeshetje logjistike duke përfshirë sallat e takimit.

4.2. Data e Fillimit dhe Periudha e Implementimit të Detyrave

Data e destinuar e fillimit është data e nënshkrimit të kontrates dhe periudha e zbatimit të kontrates do të jete katër (4) muaj nisur nga kjo datë.

5. Raportimi

5.1. Kërkesat e Raportimit

Kontraktuesi do të paraqese raportet e mëposhtme në gjuhën shqipe, në origjinal dhe të pakten një (1) kopje:

- **Raporti Fillestar** në raport Kontraktuesi duhet të pershkruaj p.sh. gjetjet fillestare, progresi në mbledhjen e të dhënave, çdo vështiresi të pritura ose të hasura. Kontraktuesi duhet të vazhdoje me punën e tij / saj derisa Autoriteti Kontraktues të dergoj komente mbi raportin fillestar.
- **Drafti i raportit përfundimtar** në këtë dokument do të duhet të përfshihet informacion i detajuar në implementimin e zgjidhjes, licencat e përdorura, informacion mbi sigurinë e sistemit, informacionet shtese të nevojshme, etj. Ky raport duhet të dorëzohet jo më vonë se dy javë para përfundimit të periudhës së zbatimit të detyrave.
- **Raporti final** me të njëjtat specifika si drafti i raportit përfundimtar përfshin inkorporimin e komenteve të pranuar nga palët në draft raport. Afati i fundit për dërgimin e raportit përfundimtar është 10 ditë pas marrjes së komenteve në draft raportin përfundimtar. Raporti përfundimtar duhet të sigurohet së bashku me faturën përkatëse.

Përmbyllja e seciles nga fazat e projektit dokumentohet me procesverbal të përpiluar nga ofruesi i shërbimit dhe të firmosur nga punonjësit përgjegjës të të dy palëve.

5.2. Dorëzimi dhe Miratimi i Raporteve

Raportet e përmendur më sipër duhet t'i dorëzohet ndjekësit të projektit të identifikuar në kontratë. Ndjekësi i projektit është përgjegjës për aprovimin e raporteve.

Raporti do të dorezohet:

- Ne forme elektronike me email
- Me shkrim i firmosur nga ndjekesit e projektit për të dyja palët.

6. Planifikimi i buxhetit për levrimin e projektit

Nr.	Emërtimi	Njesia	Sasia	Cmimi
1	F.V Punime civile jo të specializuara	Set	1	
2	FV. Derë zjarrdurese	Cope	1	
3	FV. Dysheme teknologjike	m2	14	
4	FV. Punime për spostim të paisjeve ekzistuese dhe riorganizim të dhomës së serverave (spostimi i 3 njesive ftohese, zgjatimi i tubave të bakrit, linjave të furnizimit me energji, spostimin e UPS, linjave hyrje/dalje të UPS, ripozionimin e kabineteve)	Set	1	
5	F. V. Sistem i detektimit dhe fikjes së zjarrit (perfshi panelin e kontrollit, detektorët e tymit dhe të temperaturës, sirenat, cilindrin me agentin e shuarjes, pajisjet e sinjalizimit (Alarmit), butonat e aktivizimit dhe ndalimit manual, tubat dhe nozolat e shkarkimit, Valvulat e shkarkimit, sprucatorët etj).	Set	1	
6	F.V Sistemi i monitorimit, kontrollit dhe menaxhimit	Set	1	
7	F.V. Sistem akses kontrolli për dert e dy dhomave dhe për kabinetet (Kontrollera, lexues RFID, brava elektrike / magnetike...etj)	Set	1	
8	FV. Sistem i videomonitorimit CCTV	set	1	
9	F.V. Patch corda bakri Cat.6A, 0.5m	cope	96	
10	F.V Patch corda optike OM5 duplex LC-SC, 1m	cope	48	
11	F.V Sistemues kabllosh horizontal me kapak 1RU	cope	16	
12	F.V Sistemues kabllosh vertikal me kapak	cope	8	
13	F.V Wireless Access Point	cope	12	
14	F.V Kontroller Wireless	set	1	
15	F.V Switch Akses	cope	2	
16	F.V Platformë Sigurie për akses kontroll (Virtual)	set	2	
17	Implementim projekti		1	
Totali (Lek me tvsh)				

7. Kërkesat Funktionale

Per të zgjidhur problemet e evidentuara është e nevojshme implementimi i nje zgjidhje teknike e cila mund të bllokojë aksesin në rrjet për ato pajisje të cilat nuk jane në perputhje me politikat e sigurisë ose t’iu jape pajisjeve akses të limituar me qëllim sigurimin e rrjetit nga risqet që mund të injektohen. Gjithashtu kjo zgjidhje duhet të garantoje kapacitete teknike për të mundesuar transferimin e shpejte të informacionit.

Zgjidhja teknike do të fokusohet në dy objektiva kryesore si me poshtë:

- Rritja e sigurisë për kontroll të aksesit në rrjetit për zyrat qendrore
- Përmirësim i rrjetit radio për zyra qendrore

Kërkesa kryesore është implementimi i nje infrastrukturë e cila zbaton ose detyron politika sigurie për të gjithë përdoruesit e rrjetit gjatë fazes së aksesit në rrjetin kabllor ose radio. Gjithashtu, e rëndësishme për përmirësimin e rrjetit radio është implementimi i nje infrastrukturë me kapacitet dhe funksionalitete të përmirësuar për përdoruesit në ambientet e zyrave qendrore të KESH. Rritja e sigurisë në aksesin e rrjetit dhe përmirësimi i infrastrukturë së rrjetit radio duhet të fokusohet në disa komponente kryesore të pershkruar si me poshtë. Per rritur sigurinë dhe kontrollin e aksesit në rrjet, kerkohet nje zgjidhje e avancuar për kontrollin e aksesit në rrjet i cili do të implementoje politikat e sigurisë në rrjetin kabllor dhe ate radio. Kjo zgjidhje duhet të arrije të aplikojë rolet e Autentifikimit, Autorizimit dhe ate të mbajtjes së llogarive. Gjithashtu zgjidhja teknike duhet të kryejë raportim në lidhje me përdoruesit të cilët aksesojne pajisjet e rrjetit, cfare komandash apo ndryshimesh behen dhe kohen kur kryehen keto veprime. për të patur dijeni në lidhje me perdruesit e brendshem të organizates, sistemi duhet të ketë mundësi për tu integruar me Windows Active Directory.

Zgjidhja teknike duhet të bazohet mbi protokollin 802.1x dhe për ato pajisje të cilat nuk e suportojne këtë protokoll sic mund të jenë IP printer, etj, të ketë mekanizma ku të kryhet procesi i autentifikimit si psh, me ane të MAC adresave. Zgjidhja teknike duhet të ofrojë mundësinë për të kontrolluar lidhjen e pajisjeve personale të përdoruesave, ku përdoruesit e brendshem ose ata jashte organizate të mund të sjellin pajisjet e tyre personale si psh laptop, telefona smart, etj, dhe serisht të marrin atributet e duhura për të aksesuar burimet apo sistemet në infrastrukturën e brendshme. Kjo zgjidhje duhet të mundësojë funksion profilizimi ku me ane të te cilit të identifikoje dhe klasifikojë pajisjet të cilat lidhen në rrjet kabllor dhe ate radio me qëllim aplikimin e politikave të sigurisë.

Per të rritur kapacitetet dhe funksionalitetet zgjidhja teknike duhet të perfshije pajisjet e rrjetit të cilat duhet të sigurojne kapacitetet fizike të nevojshme për të mundesuar lidhjen e përdoruesave me pajisje mobile sic jane laptop, celular, etj. Pikat e aksesit radio do të sherbejne si ure lidhese midis pajisjeve mobile dhe rrjetit kabllor apo infrastrukturës së brendshme LAN. Ndërfaqet radio të tyre duhet të mundësojnë të dy bandat e frekuencave 2,4GHz dhe 5GHz për të suportuar standartet e reja të transmetimit të te dhënave sic jane 802.11n/ac/ax si edhe ato të vjetra sic jane 802.11b/g. Gjithashtu, pikat e aksesit radio duhet të mundësojnë ndërfaqe ethernet me protokollin Power over Ethernet, me qëllim për të lehtësuar lidhjet me rrjetin fizik duke shmangur përdorimin e Power Injector dhe lidhjen nëpër priza elektrike. Ndërfaqet radio për pikat e aksesit radio duhet të suportojne konfigurimin dhe trafikun nga disa identifikues sherbimi njekohesisht.

Zgjidhja teknike për rrjetin e aksesit radio duhet të jete e menaxhueshme nga nje sistem qendror ku administratoret e rrjetit të mund të aplikojne funksione sic jane konfigurimet, monitorimet, aplikimet e politikave të trafikut dhe sigurisë së rrjetit radio. Kjo zgjidhje duhet të siguroje menaxhim të burimeve radio të pikave të aksesit sic jane fuqia e sinjalit dhe kanaleve radio me qëllim optimizimin dhe krijimin e nje ambienti radio sa me efektiv dhe me performancë të lartë. Gjithashtu, zgjidhja teknike e ofruar duhet të menaxhoje funksionet e sigurisë në ambientin radio të tilla sic jane detektimi i pikave të aksesit radio të huaja të cilat interferojne me rrjetin lokal, mbrojtje nga nderhryjet keqdashese në ambientin radio, enkriptimin e trafikut të sinjalizimit midis pikave të aksesit dhe radio kontrollerit. Autentifikimi i përdoruesave në rrjetin radio mund të behet me ane të mekanizmave lokale të kontrollerit ose integrimin me nje sistem AAA të jashtem i cili i ofron keto mekanizma në nje nivel me të avancuar. Zgjidhja teknike duhet të mundësojë funksionet e ruajtjes së log-eve si edhe të siguroje informacion mbi statusin e rrjetit radio me ane të dashboard

dhe funksioneve analitike. Zgjidhja teknike duhet të bazohet mbi nje infrastrukturë të shtreses së dyte të modelit OSI e cila duhet të ketë si rol kryesor nderlidhjen e të gjithë pikave të aksesit radio me infrastrukturën e rrjetit LAN. Zgjidhja teknike duhet të ketë pajisje me funksione të shtreses së dyte të rrjetit dhe suport për PoE.

Gjithashtu zgjidhja teknike duhet të kene ndërfaqe uplink-e redundante me qëllim nderlidhjen e pajisjeve me pjesen ekzistuese të rrjetit sic mund të jenë switchet qendror ose ato të Agregimit. Zgjidhja teknike duhet të mundësojë kapacitete të mjaftueshme për të garantuar kalimin e trafikun drejt dhe nga rrjeti radio pa ndikuar në performancën dhe cilesine e sherbimeve.

7.1. Funksionalitete dhe bllokskema të infrastrukturës

Per të permbushur objektivin dhe qëllimet e projektit, duhet të ofrohet nje zgjidhje teknike e cila do të perfshije produktet me funksionet e mëposhtme si dhe konfigurimet përkatëse për të mundesuar keto funksione.

7.2. Kërkesat funksionale për zgjidhjen teknike mbi kontrollin e aksesit në rrjet

1. Zgjidhja duhet të mbështesë vertetimin e pajisjes dhe të përdoruesit duke përdorur protokollin standard IEEE802.1X dhe të pakten metodat e mëposhtme të Protokollit të Zgjerueshem të Autentifikimit: EAP-MD5, EAP-TLS, PEAP, EAP-FAST.
2. Zgjidhja duhet të siguroje komunikim me pajisjet e tjera të rrjetit duke përdorur protokollet e sigurisë sic jane RADIUS dhe TACACS.
3. Zgjidhja duhet të mbështesë vertetimin e përdoruesit dhe pajisjes duke përdorur bazat e të dhënave të mëposhtme:
 - a. Baza e të dhënave lokale të përdoruesve,
 - b. Baza e të dhënave lokale të pajisjes,
 - c. Serveri i jashtem RADIUS,
 - d. Serveri i jashtem LDAP,
 - e. Drejtoria e jashtme aktive e Windows,
 - f. Certifikatat dixhitale
4. Zgjidhja duhet të mbështesë integrimin e plotë me bazen e të dhënave të drejtorise aktive për të kryer funksionin “Sign-On”. Emri i përdoruesit dhe fjalekalimi i përdorur në vertetimin e Windows duhet të perdoren gjithashtu për kontrolle të tjera aksesi pa pasur nevoje të rifuten serisht.
5. Zgjidhja duhet të mbështesë vertetimin e përdoruesit nëpërmjet portalit HTTPS duke e ridrejtuar automatikisht përdoruesin.
6. Zgjidhja duhet të mbështesë vertetimin specifik të pajisjes 802.1x sipas adresave fizike MAC ose metodave të pershtatshme. Zgjidhja duhet të mbështesë nje baze të dhenash të brendshme që regjistron adresat MAC të pajisjes përmes nje procesi automatik të zbulimit të pajisjes.
7. Zgjidhja duhet të mbështesë vertetimin e certifikatave dixhitale sipas kritereve të mëposhtme:
 - a. Mbeshtetje për regjistrimin e të pakten dy CA-ve të jashtme
 - b. Mbeshtetje për shkarkimin e CRL (Lista e Revokimit të Certifikatave) nëpërmjet protokollit HTTP
 - c. Mbeshtetje për protokollin e verifikimit të statusit të protokollit OCSP

-
8. Zgjidhja duhet të mbështesë rregulla fleksibel të vertetimit në lidhje me zgjedhjen dhe renditjen e bazes së të dhënave ku do të kryhet vertetimi ose përdoruesi. Autorizimi duhet të sigurojë:
 - a. Caktim i VLAN
 - b. Mbeshtetje për krijimin e nje profili përdoruesi që të pakten duhet të perfshije:
 - Mbeshtetje për ndryshimin e autorizimit të protokollit RADIUS (CoA).
 - Mbeshtetje për autorizimin e protokollit TACACS të aksesit në pajisjet e rrjetit
 9. Zgjidhja duhet të sigurojë menaxhimin e llogarive të perkohshme të përdoruesve - Vizitore / Konsulentet. Krijimi i llogarive të perkohshme të përdoruesve duhet të mbështesë profile të ndryshme me privilegje të ndryshme, të pakten si me poshtë:
 - Profili i vizitorit vetëm me qasje në internet HTTP
 - Profili i konsulentit me akses HTTP vetëm në internet dhe intranetAdministratori i llogarive të përdoruesve mund të percaktojë fillimin dhe përfundimin e vlefshmerise për secilen llogari të perkohshme individualisht.
 10. Zgjidhja duhet të mbështesë krijimin e grupeve të shumta të autorizimit me privilegje të ndryshme për krijimin e porosive të perkohshme - me privilegjet e mëposhtme:
 - Krijimi i shume porosive të rastesishme
 - Import i skedarit të llogarise në formatin “.csv”
 - Dergimi i kredencialeve me email dhe SMS
 - Mundësia për të pare fjalekalimin e llogarise së perkohshme
 - Printim i detajeve të porosive të perkohshme
 - Menaxhim i porosive nga të gjitha grupet për autorizimin e porosive të perkohshme
 - Menaxhim i porosive nga i njeiti grup për autorizimin e porosive të perkohshme
 - Pezullimi i urdhrave nga të gjitha grupet për autorizimin e urdhrave të perkohshem
 - Caktimi i nje profili aksesi në rrjet me nje llogari të vizitorit
 - Caktimi i nje profili kohor për të hyre në llogarine e vizitorit
 11. Zgjidhja duhet të mbështesë vendosjen e nivelit të sigurisë së fjalekalimit që do të gjenerohet për porosite e perkohshme në lidhje me numrin minimal të karaktereve, karaktereve speciale dhe numrave që do të perdoren për të krijuar nje fjalekalim të perkohshem
 12. Zgjidhja duhet të sigurojë menaxhimin, konfigurimin dhe monitorimin e të gjithë sistemit përmes nje ndërfaqe grafike.
 13. Nderfaqja grafike duhet të mundësojë nje panel qendror për nje pasqyre të shpejte të informacionit me të rendesishem në 24 oret e fundit, e cila perfshin:
 - Numri i pajisjeve aktive, numri i vizitoreve aktive
 - Numri i pajisjeve të zbuluara
 - Statistikat e performancës - CPU, memoria e secilit komponent
 - Numri dhe arsyeja e vertetimit të deshtuar në 24 oret e fundit
 14. Zgjidhja duhet të ketë nje ndërfaqe grafike për monitorimin e vazhdueshem të vertetimit në kohe reale me nje shfaqje të menjehershme të informacionit të meposhtëm të vertetimit:
 - Koha dhe data,
 - Satusi i vertetimit,
 - Emri i përdoruesit / pajisja dhe adresa MAC,
 - Adresa IP,
 - Pajisja
 - Nderfaqja,
 - Profili i autorizimit,
 - Metoda e vertetimit,
-

-
- Protokoli i vertetimit
15. Zgjidhja duhet të mbështesë aftësitë e administrimit dhe monitorimit të pajisjes duke përdorur protokollin TACACS+.
 16. Zgjidhja duhet të mbështesë shërbimin e profilizimit, i cili mbledh informacion për një pajisje duke degjuar komunikimin e saj në rrjet.
 17. Zgjidhja duhet të mbështesë Zbatimin e politikave të Aseteve duke përdorur kategorizimin e pikave fundore sipas profileve në politiken e aksesit në rrjet.
 18. Zgjidhja duhet të mundësojë automatizimin e të gjithë procesit të kycjes në rrjet për pajisjet të përdoruesave të cilat janë personale. Ky proces përfshin që nga regjistrimi i pajisjes, sigurimi i kërkesës deri të instalimi i certifikates. Kjo mund të mbështetet në pajisje në platforma të ndryshme OS: iOS, Android, Windows, macOS dhe ChromeOS.
 19. Zgjidhja duhet të mbështesë një Portal që është plotësisht i personalizueshem, për të lejuar përdoruesit fundore të hyjnë në rrjet dhe të menaxhojnë pajisje të ndryshme.
 20. Zgjidhja duhet të zbatohet si një pajisje virtuale e dyfishtë dhe duhet të jete e zgjerueshme për të mbështetur një arkitekturë të shpërndare dhe një mekanizëm të disponueshmerise së lartë për funksionet e menaxhimit dhe monitorimit.
 21. Zgjidhja duhet të mbështesë vertetimin dhe autorizimin e njekohshem të 100 pajisjeve.

7.3. Kërkesat funksionale për përmirësim të rrjetit LAN të HQ

- Zgjidhja teknike duhet të jete për përdorim në ambiente të brendshme dhe të mundësojnë standartin 802.11-ax.
- Zgjidhja teknike duhet të ofrojë mundësinë për tu montuar në tavan, në mur dhe kapese (t-rail).
- Zgjidhja teknike duhet të mundësojë të pakten 1 porte GE RJ45 me PoE për lidhjen fizike me rrjetin e aksesit (switchet e aksesit).
- Zgjidhja teknike duhet mundësojë të pakten 2 radio dhe 4 antena për të ofruar akses në bandat 2.4 GHz dhe 5 GHz.
- Zgjidhja teknike duhet të suportoje integrimin dhe menaxhimin nga një radio kontrollor për të ofruar zgjidhje të qenderzuar.
- Zgjidhja teknike duhet të suportoje disa identifikues shërbimi radio njekohesisht të cilat mund të funksionojne në menytrat tunel, ure-lokale, mesh.
- Zgjidhja teknike duhet të suportoje funksionimin si pika aksesi të vecuara ose të integruara me ane të një kontrolleri.
- Zgjidhja teknike duhet të suportoje gjerësi kanali 20/40/80/160 MHz.
- Zgjidhja teknike duhet të suportoje funksionet për skanim dhe detektim së pikave të aksesit të huaja (jashtë organizate).
- Zgjidhja teknike duhet të suportoje funksionet për analizim të spektrit të frekuencave dhe detektim të paketave.
- Zgjidhja teknike duhet të suportoje funksionet e sigurisë për detektim dhe parandalim të sulmeve në ambientin radio.
- Zgjidhja teknike duhet të jenë e certifikuar nga “Wi-Fi Alliance”.

7.4. Kërkesat funksionale për zgjidhjen teknike mbi Sistemin e menaxhimit dhe supervizimit për pikat e aksesit radio

- Zgjidhja teknike duhet të mundësojë provizionim të qenderzuar të pikave të aksesit radio.
- Zgjidhja teknike duhet të mundësojë funksionin e Roaming për të garantuar levizshmeri të përdoruesave radio

-
- Zgjidhja teknike duhet të mundësojë menaxhim të burimeve radio sic është fuqia e sinjalit, kanali radio, etj.
 - Zgjidhja teknike duhet të mundësojë funksion sigurie për detektimin e burimeve radio të huaja.
 - Zgjidhja teknike duhet të mundësojë funksion sigurie për enkriptim të trafikut të kontrollit radio.
 - Zgjidhja teknike duhet të mundësojë funksion sigurie për parandalimin e nderhyrjeve në ambjentin radio.
 - Zgjidhja teknike duhet të suportojë standartin e IEEE për të kontrolluar aksesin në rrjet bazuar mbi porten.
 - Zgjidhja teknike duhet të suportojë Autentikim të qenderzuar të përdoruesave me ane të Radius, LDAP.
 - Zgjidhja teknike duhet të suportojë mekanizmat e Autentikimit me ane të WPA2, 802.1x, MAC adrese, dhe autentikim me portal.
 - Zgjidhja teknike duhet të suportojë mekanizma të cilesise së shërbimit për të garantuar nje performancë të lartë në shërbimet ze, video dhe data.
 - Zgjidhja teknike duhet të suportojë role të ndryshme për përdoruesit në nivelet e administratorit, përdoruesave dhe vizitoreve.
 - Zgjidhja teknike duhet të suportojë funksionet e shfaqjes dhe analizimit të eventeve të sistemit radio.
 - Zgjidhja teknike duhet të jete nga i njejeti vendor/brand me ate të pikave të aksesit radio për të garantuar nderveprueshmeri dhe maksimizim të funksionaliteteve.
 - Zgjidhja teknike duhet të ketë mundësi për menaxhim grafik, nga ku administratoret e rrjetit të kryejne provizionimin, monitorimin, etj. të infrastrukturës radio.
 - Zgjidhja teknike duhet të ofrojë versionin me të fundit të sistemit operativ ose versionin stabel të rekomanduar nga vendori.
 - Zgjidhja teknike duhet të jete e licensuar për të gjithë funksionet dhe mekanizmat të permendur me lart.
 - Zgjidhja teknike duhet të jete në formatin e nje makine virtuale për tu instaluar në ambientin Hypervisor sic është VMware (e preferueshme) ose HyperV, KVM.

7.5. Kërkesat funksionale për zgjidhjen teknike mbi rrjetin e aksesit

- Zgjidhja teknike duhet të mundësojë 24 porta për lidhjet fizike me shpejtesi 1 Gbps RJ45 të hosteve fundore dhe min 4 porta fizike me shpejtesi 1/10 Gbps SFP/SFP+, për të mundësuar nderlidhje me komponentet e tjere të infrastrukturës së rrjetit.
- Zgjidhja teknike duhet të suportojë protokollin PoE të portat donwlink për të furnizuar me energji pajisjet e rrjetit të cilat do të lidhen në to.
- Zgjidhja teknike duhet të mundësojë kapacitete fizike të mjaftueshme për të siguruar throughput të lartë të trafikut dhe reduktuar vonesat në komunikim midis pajisjeve.
- Zgjidhja teknike duhet të mundësojë teknologji të disponueshmerise së lartë si psh “stacking” ose dicka të ngjashme.
- Zgjidhja teknike duhet të mundësojë konfigurimin e lidhjeve redundante, dhe të siguroje balancim të trafikut midis lidhjeve.
- Zgjidhja teknike duhet të siguroje mbrojtje automatike ndaj problemeve të mundshme në rrjet sic jane L2 loop, etj.

- Zgjidhja teknike duhet të mundësojë funksionim në Layer 2 të modelit OSI dhe izolimin e paketave në VLAN-e të ndryshme.
- Zgjidhja teknike duhet të suportojë mekanizmat për menaxhim të trafikut sic është Cilesia e Sherbimit.
- Zgjidhja teknike duhet të mundësojë administrim dhe konfigurim të sistemit nëpërmjet ndërfaqe grafike, asaj të komandave, dhe nëpërmjet konsoles.
- Zgjidhja teknike duhet të mundësojë monitorim të sistemit dhe performancës nëpërmjet protokolleve SNMP, RMON, Syslog, Netflow dhe IP SLA.
- Zgjidhja teknike duhet të ofrojë versionin më të fundit të sistemin operativ ose versionin stabil të rekomanduar nga vendori.
- Zgjidhja teknike duhet të jete e licensuar për të gjithë funksionet dhe mekanizmat e permendur me lart.
- Zgjidhja teknike duhet të suportojë burim ushqimi të dyfishte ku të përfshihet të paktën nje burim ushqimi.
- Zgjidhja teknike duhet të montohet në rack në standartin 19” dhe të ketë kit të përfshire.

7.6. Shërbimet e kërkuara

Operatori Ekonomik duhet të kryejë aktivitetet kryesore si me poshtë:

- Projektim të infrastrukturës për të implementuar sistemin e aksesit në site HQ.
- Projektim të infrastrukturës për implementimin e sistemit të kontrollit në aksesin e rrjetit në site HQ.
- Instalimet fizike të paisjeve të reja për rrjetin radio dhe ate kabllor.
- Instalimet në ambient virtual të radio kontrollerit dhe sistemin për menaxhimin e kontrollit të aksesit.
- Konfigurime e nevojshme për të implementuar rrjetin kabllor dhe radio për ambientet e HQ dhe integrimet me rrjetin ekzistues.
- Konfigurimet e nevojshme për të implementuar sistemin e menaxhimit për akses të kontrollit të rrjetit.
- Konfigurimet e nevojshme në rrjetin ekzistues për të integruar pajisjet e rrjetit me sistemin qendror të kontrollit të aksesit.
- Dokumentimin e diagrameve të detajuara për implementimin e rrjetit radio dhe sistemit të kontrollit të aksesit.
- Dokumentimin e të gjithë shërbimeve të kryera në kuader të këtij projekti.

8. Specifikimet Teknike

Tabelat me poshtë paraqesin pajisjet dhe specifikimet teknike për secilin prej tyre.

Tabela permbledhese e produkteve që do të prokurohen:

Nr.	Emërtimi	Njesia	Sasia
1	Pike aksesi radio	cope	12
2	Platforme për kontrollin e pikave të aksesit radio (Virtual)	set	1
3	Switch aksesi	cope	2
4	Platformë Sigurie për kontrollin e aksesit në rrjet (Virtual)	set	2
5	Derë zjarrduruese	cope	1

6	Dysheme teknologjike	m2	14
7	Sistem i detektimit dhe fikjes së zjarrit	set	1
8	Sistemi i monitorimit, kontrollit dhe menaxhimit	set	1
9	Sistem akses kontrolli	set	1
10	Sistem i videomonitorimit CCTV	set	1
11	Patch corda bakri Cat.6A, 0.5m	cope	96
12	Patch corda optike OM5 duplex LC-SC, 1m	cope	48
13	Sistemues kabllorsh horizontal me kapak 1RU	cope	16
14	Sistemues kabllorsh vertikal me kapak	cope	8

8.1. Pike aksesi radio

Karakteristikat hardware	Specifikimet
Antenat	Dy antena të brendshme të integruara me parametrat me poshtë: <ul style="list-style-type: none"> ● 2.4 GHz, gain 3 dBi, azimuth omnidireksional ● 5 GHz, gain 4 dBi, azimuth omnidireksional
Fuqia e transmetimit në radio	2.4GHz (-4dBm – 23dBm) 5GHz (-4dBm – 23dBm)
Ndërfaqet	<ul style="list-style-type: none"> ● 1 ndërfaqe 100, 1000, 2500 Multigigabit Ethernet (RJ-45) – IEEE 802.3bz ● Port console për menaxhim (RJ-45) ● Port USB 2.0
Energjia	802.3at/802.3af (PoE/PoE+) Dhe suport për Power Injector
Memoria	<ul style="list-style-type: none"> ● 2048 MB DRAM ● 1024 MB flash
Suport për Kontroller Wireless	Po
Suport për protokollin 802.11n	<ul style="list-style-type: none"> ● 4x4 MIMO me kater stream spatial-e ● 802.11n and 802.11a/g beamforming ● gjerësia e brezit 20- and 40-MHz ● shpejtesi fizike deri 890 Mbps (40 MHz në 5 GHz dhe 20 MHz në 2.4 GHz) ● Packet aggregation: A-MPDU (Tx dhe Rx), A-MSDU (Tx dhe Rx) ● 802.11 Dynamic Frequency Selection (DFS) ● Cyclic Shift Diversity (CSD)
Suport për protokollin 802.11ac	<ul style="list-style-type: none"> ● 4x4 downlink MU-MIMO me kater stream spatial-e ● 802.11ac beamforming ● gjerësia e brezit 20-, 40-, 80-, dhe 160-MHz channels ● shpejtesi fizike deri 3.47 Gbps (160 MHz në 5 GHz) ● Packet aggregation: A-MPDU (Tx dhe Rx), A-MSDU (Tx dhe Rx) ● 802.11 DFS ● Cyclic Shift Diversity (CSD)
Suport për protokollin 802.11ax	<ul style="list-style-type: none"> ● 4x4 downlink MU-MIMO me kater stream spatial-e ● Uplink/downlink OFDMA ● TWT ● BSS coloring ● 802.11ax beamforming

	<ul style="list-style-type: none"> ● gjerësia e brezit 20-, 40-, 80-, and 160-MHz channels ● shpejtësi fizike deri 5.38 Gbps (160 MHz në 5 GHz dhe 20 MHz në 2.4 GHz) ● Packet aggregation: A-MPDU (Tx dhe Rx), A-MSDU (Tx dhe Rx) ● 802.11 DFS ● Cyclic Shift Diversity (CSD)
Periudha e mbulimit të garancise:	3 vjet

8.2. Platfome për kontrollin e pikave të aksesit radio (Virtual)

Karakteristikat hardware	Specifikimet
Standartet Wireless	IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, <u>802.11n</u> , 802.11k, 802.11r, 802.11u, 802.11w, 802.11ac Wave 1 and Wave 2, 802.11ax
Standartet e rrjetit	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX, 1000BASE-T, 1000BASE-SX, 1000-BASE-LH, IEEE 802.1Q VLAN tagging, IEEE 802.1AX Link Aggregation
Standartet e të dhënave	<ul style="list-style-type: none"> ● RFC 768 User Datagram Protocol (UDP) ● RFC 791 IP ● RFC 2460 IPv6 ● RFC 792 Internet Control Message Protocol (ICMP) ● RFC 793 TCP ● RFC 826 Address Resolution Protocol (ARP) ● RFC 1122 Requirements for Internet Hosts ● RFC 1519 Classless Interdomain Routing (CIDR) ● RFC 1542 Bootstrap Protocol (BOOTP) ● RFC 2131 Dynamic Host Configuration Protocol (DHCP) ● RFC 5415 Control and Provisioning of Wireless Access Points (CAPWAP) Protocol ● RFC 5416 CAPWAP Binding for 802.11
Standartet e sigurisë	<ul style="list-style-type: none"> ● Wi-Fi Protected Access (WPA) ● IEEE 802.11i (WPA2, RSN) ● Wi-Fi Protected Access 3 (WPA3) ● RFC 1321 MD5 Message-Digest Algorithm ● RFC 1851 Encapsulating Security Payload (ESP) Triple DES (3DES) Transform ● RFC 2104 HMAC: Keyed-Hashing për Autentikim të Mesazheve ● RFC 2246 TLS Protocol Version 1.0 ● RFC 3280 Internet X.509 Public Key Infrastructure (PKI) Certificate and Certificate Revocation List (CRL) Profile ● RFC 4347 Datagram Transport Layer Security (DTLS) ● RFC 5246 TLS Protocol Version 1.2
Standartet e enkriptimit	<ul style="list-style-type: none"> ● Static Wired Equivalent Privacy (WEP) RC4 40, 104 dhe 128 bits ● Advanced Encryption Standard (AES): Cipher Block Chaining (CBC), Counter me CBC-MAC (CCM), Counter wme CBC Message Authentication Code Protocol (CCMP)

	<ul style="list-style-type: none"> ● Data Encryption Standard (DES): DES-CBC, 3DES ● Secure Sockets Layer (SSL) dhe Transport Layer Security (TLS): RC4 128-bit dhe RSA 1024- and 2048-bit ● DTLS: AES-CBC ● IPsec: DES-CBC, 3DES, AES-CBC ● 802.1AE MACsec encryption
Standartet AAA	<ul style="list-style-type: none"> ● IEEE 802.1X ● RFC 2548 Microsoft Vendor-Specific RADIUS Attributes ● RFC 2716 Point-to-Point Protocol (PPP) Extensible Authentication Protocol (EAP)-TLS ● RFC 2865 RADIUS Authentication ● RFC 2866 RADIUS Accounting ● RFC 2867 RADIUS Tunnel Accounting ● RFC 2869 RADIUS Extensions ● RFC 3576 Dynamic Authorization Extensions to RADIUS ● RFC 5176 Dynamic Authorization Extensions to RADIUS ● RFC 3579 RADIUS Support for EAP ● RFC 3580 IEEE 802.1X RADIUS Guidelines ● RFC 3748 Extensible Authentication Protocol (EAP) ● Web-based authentication ● suport për TACACS
Standartet e Menaxhimit	<ul style="list-style-type: none"> ● Simple Network Management Protocol (SNMP) v1, v2c, v3 ● RFC 854 Telnet ● RFC 1155 Management Information for TCP/IP-based Internets ● RFC 1156 MIB ● RFC 1157 SNMP ● RFC 1213 SNMP MIB II ● RFC 1350 Trivial File Transfer Protocol (TFTP) ● RFC 1643 Ethernet MIB ● RFC 2030 Simple Network Time Protocol (SNTP) ● RFC 2616 HTTP ● RFC 2665 Ethernet-Like Interface Types MIB ● RFC 2819 Remote Monitoring (RMON) MIB ● RFC 2863 Interfaces Group MIB ● RFC 3164 Syslog ● RFC 3414 User-Based Security Model (USM) for SNMPv3 ● RFC 3418 MIB for SNMP ● RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs ● RFC 4741 Base NETCONF protocol ● RFC 4742 NETCONF over SSH ● RFC 6241 NETCONF ● RFC 6242 NETCONF over SSH ● RFC 5277 NETCONF event notifications ● RFC 6020 YANG
Menaxhimi	<ul style="list-style-type: none"> ● Web-based: HTTP/HTTPS ● Command-line interface: Telnet, Secure Shell (SSH) Protocol, serial port ● SNMP ● NETCONF

Periudha e mbulimit të garancise:	3 vjet
-----------------------------------	--------

8.3. Switch aksesi

Ndërfaqet dhe karakteristikat hardware	
Porta 10/100/1000Mbps RJ45 (Auto Negocim /Auto MDI/MDIX)	≥ 24 fixed 10/100/1000 RJ45 ports PoE
Porta SFP+	4
Porta Uplink (baker/fibër) 1000Mbps/10Gbps SFP+ Slots	4X 10GBase-X SFP+ porta fikse uplink
Porta Console RJ-45/RS-232	1
Instalimi në Rack	Rack Mountable
HYRJE "INPUT"	
Tensioni Nominal	100~240 V AC
Frekuenca	50/60 Hz
PERFORMANCA DHE FLEKSIBILITETI	
Switching Capacity	128Gbps
Forwarding Rate	≥ 95 Mpps
Flash Memory	≥ 4 GB
DRAM	≥ 2 GB
Ethernet Jumbo frame	Po 9198 bytes
Tabele të Adresave MAC	16k
Fan	Redundant fiks
STANDARDET	
IEEE 802.3 /u/ab/z-10BASE-T	
IEEE 802.3u - 100BASE-TX	
IEEE 802.3ab - 1000BASE-T	
IEEE802.3z - 1000BASE-X	
IEEE 802.3ad - Agregim linku	
IEEE 802.3x - full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports	
IEEE 802.1d - Spanning Tree Protocol	
IEEE 802.1s - multi STP	
IEEE 802.1w - RSTP	
IEEE 802.1x - Port-based Network Access Control	
IEEE 802.1p – Cos	
IEEE 802.3af - PoE	
IEEE 802.3at - PoE	
SISTEMI OPERATIV	
Te Jete i Orientuar për Operacionet LAN	
Te Ketë Mundësi për Upgrade	
QUALITY OF SERVICE	
Priority Queues	
Queue Scheduling: SRR, CIR	
VEÇORITË në LAYER 2 DHE 3	
IGMP Snooping	
Spanning Tree	

LLDP
BPDU Filtering/Guard
Detektim të Loopback
802.3x Flow Control
VLAN ID: 1024
Agregim të Linkeve 802.3ad LACP
Adresimi IPv6
DHCP/BOOTP, DHCP Snooping, DHCP Option82 për klientet
Dynamic ARP inspection (DAI)/ Dynamic ARP Protection (DAP)
Limitim të Shpejtesise: Port/Flow
Policy-Based Routing (PBR)
Routimi
SIGURIA
Access Control List
TCP/UDP Ports
Protokollin DSCP
Authentication: AES-128 MACsec, segmentim bazuar në policy
Storm Control: Broadcast, Multicast, Unicast
MENAXHIMI
Web-based GUI dhe CLI
RS-232 Console / RJ-45 Console
Telnet, SSH
Monitorim të CPU
SNTP / NTP
Upgrade të Firmware
Indikator LED
SNMP v1/v2c/v3
SYSLOG
Periudha e Mbulimit të Garancise: 3 vjet

8.4. Platformë Sigurie për kontrollin e aksesit në rrjet (Virtual)

Specifikimet
Sistemi NAC i cili do të implementohet të arrije të aplikojë Authentication, Authorization, Accounting si dhe reportim në lidhje me kush e aksesoi pajisjet e networkut, cfare komandash apo ndryshimesh beri dhe në cfare momenti
Sistemi NAC të jete virtual dhe të ofrojë High Availability për të gjitha funksionalitetet e perfshira.
Sistemi të mundësojë integrim të pajisjeve multi-vendor përmes protokolleve RADIUS dhe TACACS+.
Sistemi të ofrojë integrim me Multi-Forest LDAP, Radius Token, RSA identity, SAMLv2, Certificate authorities si dhe Internal Users.
Te ofrojë autentikim dhe autorizim wired dhe wireless përmes metodave të autentikimit Single-User, Multi-User, Multiple User.
Te ofrojë politika AAA për menaxhim administrativ të pajisjeve.

Te ofrojë gjenerim të raporteve lidhur me administrimin e pajisjeve dhe mundësinë për të shfaqur komandat e përdorura në nivel networku për pajisje e integruara nderlidhur me administratoret pergegjes.
Te ofrojë konfigurim politikash sigurie përmes segmentimit të përdoruesve pa u nevojitur VLAN-s duke therritur Tags.
Te ofrojë funksionalitet ndryshimit të Autorizimit (“Change of Authorization”) përmes politikave të sigurisë duke implementuar access list per-port dhe VLAN-e dinamike.
Te ofrojë mundësinë që përdoruesit të marrin të njëjtin shërbim dhe autorizim në çdo postacion pune panvaresisht pajisjes Endpoint që do të perdorin.
Te ofrojë mundësi autentikimi dhe autorizimi të sigurt për pajisje Jo Smart wired apo wireless përmes identifikimit të hardware-it me ane të metodës së “OUI lookup”.
Te mundësojë implementimin e AAA policy rules për lidhjet wireless dhe Guest Provisioning përmes Guest dhe Sponsor Portals integruar me SMTP për njoftime dinamike.
Te ketë mundësinë e implementimit të politikave profiling për të arritur koleksionimin e informacionit nga përdoruesit fundore përmes metodave si DHCP Relay, DNS, Local Web Authentication, Central Web Authentication, SNMP, Radius TLV Attributes, NMAP, HTTP, HTTPS dhe jo vetëm.
Te ofrojë shërbime kontrolli fundor të klienteve të lidhur në nivel networku bazuar në sistemet e operimeve të endpoints, patches apo aplikacione të instaluar. të ndaloje aksesin e përdoruesve nese politikat e sigurisë
Te ofrojë informacion të detajuar në lidhje me Endpoints për vendodhjen e tyre në korporate, mënyrën e autentikimit, politikat e autentikimit dhe autorizimit si dhe kohën e hyrjes në fuqi të këtyre të dhënave
Te suportoje monitorim të serverave fizike përmes metodave me agjent ose pa agjent.
Te ofrojë mundësi integrimi të pajisjeve hardware dhe software.
Te ofrojë komunikim të enkriptuar përmes protokollit TLS, pre-shared key encryption dhe me ane të certificateve.
Te ofrojë template për menaxhim të pajisjeve.
Te ofrojë redundance duke implementuar disponueshmeri të lartë.
Te ofrojë mundësi për ruajtjen e të dhënave duke mundësuar raporte historike për data, events, audit logs, sesione aktive.
Te suportoje protokolle integrimi dhe kontrolli si SNMP, ICMP, CDP, LLDP, HTTP, FTP, Ping sweeping.
Te mundësojë zbulim aktiv të shërbimeve të sistemeve hardware apo software duke perfshire, por jo duke u limituar në ndërfaqet e rrjetit, shërbimet, parametrat e sistemit RAM, CPU, Storage, të ofrojë zbulim të SNMP MIB-s, sensors, file systems.
Te ofrojë opsjon instalimi dhe raportimi përmes Agjenteve dhe ndarjes automatike të pajisjeve në grupe.
Te ketë suport aktiv nga vendori duke ofruar update dhe patche të reja.
Te ketë suport për pajisje nga vendore të ndryshem për rrjetin, sigurinë e rrjetit si dhe server & storage për vendore si Cisco, HPE, F5, Juniper, Hyper-V, Vmware dhe jo vetëm.
Te bëjë gjurmim në mënyrë dinamike ndryshimet e kryera në pajisje fundore dhe të gjeneroje audit logs si dhe reports.
Te ofrojë integrimi me sisteme të njohura ITSM.
Te ofrojë mundësi integrimi me self-defined apo third-party API.
Te ofrojë mundësi monitorimi përmes SLA tracking.
Te krijojë në mënyrë dinamike inventar të pajisjeve dhe informacione në lidhje me to.
Te gjeneroje automatikisht harta për infrastrukturën bazuar në të dhenat e gjeneruara dhe të mbledhura.

Te ofrojë mundësi rehabilituese në rast incidentesh të incizuara në sistem, si dhe të ndermare veprime automatikisht.

Te ofrojë dashboard dinamik për monitorim grafik dhe të jete fleksibel në ndryshim të te dhënave të paraqitura.

Periudha e Mbulimit të Garancise: 3 vjet
--

8.5. Derë zjarrduruese

Ne dhomën teknike duhet të instalohet nje derë zjarrduruese me permasa minimalisht 120 cm x 220 cm për të lejuar futjen dhe nxjerrjen lehtësisht të pajisjeve të permasave të medha (Kondicioner, UPS etj);

- Dera duhet të jete zjarrduruese me kohe minimale 60 minuta;
- Te jete me hapje nga jashte me doreze antipanik dhe me mekanizem vetëmbylles;
- Te jete me sistem hapjeje të kontrolluar me elektromagnet të lidhur me sistemin e akses kontrollit;

8.6. DysHEME teknologjike

Ne ambientin e ri duhet të montohet dysHEME teknologjike, me pllaka të levizshme dhe grila ajrimi. Lartësia e dysHEMESE teknologjike nga dysHEMEJA e dhomës duhet të jete rreth 40 cm për të bere të mundur që poshtë saj të realizohet pjesa me e madhe e instalimeve elektrike, kondicionimit, senseve të ndryshem si dhe të mundësojë qarkullimin e ajrit të ftohte nga njesite e kondicionimit drejt Rack-eve nëpërmjet aksesoreve të ventilimit. Pajisjet e renda si kondicioneret duhet të instalohen mbi bazament të vecante për të eliminuar mbingarkesen në dysHEMESE teknologjike. DysHEMEJA duhet të suportohet nga nje bazament me perberje celiku të galvanizuar i fiksuar nen strukture me adezive/silikon.etj dhe me dy fiksues mekanike për të siguruar lartësine e nevojshme. Bazamenti duhet të kompletohet me nje veshje anti-vibruese (gomina).

DysHEMEJA teknologjike duhet të perbehet nga:

- Pllaka me dimensione 600 mm x 600 mm;
- Strukture mbeshtese e perbere teresisht nga celiku i galvanizuar; kembe me lartësi të rregullueshme;
- Tranversa të perbera prej profili “C”, (Tranversat – bashkueset jane të vendosura në pjesen e poshtme për të rritur qëndrueshmerine ndaj perkuljeve);
- Material plastik i zi kundra zjarrit i montuar në pjesen e sipërme të tranverses (gomine kundra zjarrit) për të shmangur vibrimet;

8.6.1. Pllakat

Materiali i pllakave të përdorura për dysHEMESE teknologjike duhet të jete material mineral i perforcuar me fibra për të permbushur nevojat për peshembajtje.

8.6.2. Aksesorët e ajrimit

Per të siguruar nje efikasitet sa me të mire të fryrjes së ajrit të ftohte, dyshemeja teknologjike duhet të jete e pajisur me aksesore ventilimi për të bere të mundur qarkullimin e ajrit të ftohte nga poshtë dyshemese në pjesen ballore të rack-eve. Ky ventilim duhet të realizohet nëpërmjet grilave të ajrimit (panelet metalike).

8.6.3. Rampë ose Shkallë

Per lehtësimin e futjes së pajisjeve të renda si dhe për të mundesuar hyrjen e personelit në dhomë (lartësi e dyshemese rreth 40 cm) duhet të ndërtohet nje rampë (pedane) ose strukture me dy shkallë brenda dhomës teknike. Duhet të mbahet në konsiderate siguria e përdoruesve në zgjidhjen që do të propozohet. për të garantuar sigurinë e përdoruesve, në të dy rastet, rampa (pedana) ose struktura me dy shkallë duhet të jete sipërfaqe jo e rreshqitshme. Dyshemeja teknologjike, para dorëzimit duhet të pastrohet në mënyrë profesionale duke siguruar që në dhomë mos të ketë pluhura dhe ndotje të cilat janë të demshme për pajisjet e vendosura në të si UPS, kondicioner etj.

8.7. Sistemi i shuarjes së zjarrit

Brenda dhomës teknike (ambientit të ri) duhet të instalohet nje sistem për shuarjen e zjarrit. Sistemi duhet të jete i ndare në dy zona: zona nen-dyshemene teknologjike dhe ambienti i dhomës. në secilen prej këtyre zonave duhet të instalohet nga nje dedektor tymi si edhe nga nje nozole 180 grade. Sistemi i detektimit dhe shuarjes së zjarrit duhet të ketë komponentet e mëposhtme:

- Paneli i kontrollit
- Detektorët e tymit dhe të temperaturës
- Cilindrin me agjentin e shuarjes
- Paisjet e sinjalizimit (alarmit)
- Butonat e aktivizimit dhe ndalimit manual
- Tubat dhe nozolat e shkarkimit

8.7.1. Paneli i kontrollit

Paneli i kontrollit duhet të ketë minimalisht 2 zona dedektimi, që i korrespondojne 2 zonave në ambientin e dhomës, si edhe nje zone shuarje që do të perdoret për aktivizimin e valvules solenoide në cilindrin ku ruhet agjenti i shuarjes. Paneli duhet të ketë minimalisht 3 dalje për paisje sinjalizimi (sirena alarmi), dhe minimalisht 3 rele dalese (Zjarr, Fault dhe 1 të programueshme). Minimalisht duhet të ketë 5 hyrje të programueshme, 1 për shkarkim manual, dhe 4 që lidhen me shkarkimin e agjentit shuares (Mode Select, Valve Monitor, Pressure Monitor, Hold, Abort). Duhet të jete i pajisur me ekran LCD, me tastjere alfa-numerike, butona për navigim lart / poshtë / majtas / dhjathtas / konfirmim. Paneli i kontrollit duhet të jete konform standardit EN12094-1 (Standardi European për sistemet fikse të shuarjes së zjarrit – komponentet për sistemet e shuarjes me gaz) dhe EN54 - Parts 2 dhe 4. Duhet të jete i pajisur me bateri për të siguruar autonomi në rast problemesh me energjine elektrike.

8.7.2. Detektorët e tymit dhe të temperaturës

Ne secilen prej zonave të dedektimit duhet të instalohen nga një dedektor tymi dhe nga një dedektor temperature. të këne shpërndarje të tillë që të mbulojnë të gjithë hapësirën e dhomës. të jenë në përputhje të plotë me sistemin e panelit të kontrollit. në dhomën teknike duhet të instalohen 2 detektor tymi dhe 2 detektor temperature.

8.7.3. Butonat e aktivizimit dhe ndalimit manual

Në hyrje të dhomës teknike duhet të instalohet një buton aktivizimi manual dhe një buton ndalimi. Butoni i aktivizimit manual mund të përdoret nëse kërkohet aktivizim i menjëhershëm i sistemit të shuarjes (supozojmë se vetëm njëri nga dedektorët është aktivizuar dhe paneli ka kaluar në gjendjen “Pre-activated”, kur personi përgjegjës shkon të kontrollojë nëse është alarm fals apo është zjarr dhe verën që në dhomë ka zjarr, atëherë për të mos pritur sa të aktivizohet dhe dedektori tjetër, ai shtyp këtë buton dhe aktivizon në këtë mënyrë manualisht sistemin e shuarjes). Butoni i Ndalimit (ose vonimit) mund të përdoret në rastet kur paneli ka kaluar në gjendje “Activated”, por duam të vonojmë ose ndalojmë aktivizimin e sistemit të shuarjes për disa momente, atëherë shtypet ky buton. Pra supozojmë se nëse paneli ka kaluar në gjendjen “Activated”, dhe personeli përgjegjës verën se në dhomë është një zjarr që mund të shuhet edhe me një fikse dore, atëherë shtypet butoni i ndalimit dhe mund të ndërhyhet me një fikse dore për të shuar zjarrin.

8.7.4. Pajisjet e sinjalizimit

Në hyrje të dhomës teknike, mbi derë duhet të instalohet një sirene alarmi me ze dhe drite, si edhe një tabelë sinjalizimi e cila ndricon në rastin e rënies së zjarrit dhe leshimit të shuarjes së zjarrit.

8.7.5. Sprucatorët

Sprucatorët duhet të instalohen një për çdo zonë. Sprucatorët duhet të përlogariten për të arritur një kohë zbrazje minimalisht 2.0 sekonda dhe një maksimum prej 6.3 sekonda. Shpërndarja e tubacioneve nga cilindri deri tek sprucatorët, dhe bashkuesit duhet të jenë në përputhje me EN 15004, sipas standardeve të aprovuara për tubacionet dhe kërkësat inxhinierike të sistemit të shuarjes së zjarrit.

8.7.6. Cilindri dhe agjenti i shuarjes

Cilindri duhet të jetë prej materiali metalik, dhe duhet të jetë konform direktives TPED (2010/35/EU), Pi (π) 0589 Marking dhe DIN EN ISO 11363-1. Cilindri duhet të jetë i paisur minimalisht me:

- Aktivizuesin automatik të valvulës së shkarkimit
- Aktivizuesin manual
- Aktivizuesin pneumatik
- Mates presioni
- Valvulën e kontrollit të gazit
- Etiketën me të dhënat e cilindrit, presionin e punës dhe agjentin e shuarjes

Agjenti i shuarjes së zjarrit duhet të veprojë sipas përcaktimeve të mëposhtme

- Te arrije nje koncentrim të shuarjes 5.3% (v/v) për rreziqet e Klases A
- Te arrije nje koncentrim të shuarjes 5.9% (v/v) ose me shume për rreziqet e Klases B
- Te arrije nje koncentrim të shuarjes 5.6% (v/v) për rreziqet e Klases A+
- Brenda 4 sekondave agjenti i shuarjes së sistemit të zjarrit duhet të zbrase 95% të masës së kërkuar për të maksimizuar shuarjen dhe minimizojë demtimet gjatë zjarrit dhe nuk duhet të kalojë 10 sekondeshin.
- Zgjidhja për shuarsin duhet të jetë e bazuar në cilindra nën presion, pa lene asnjë lloj mbetje
- Shuaresi i zjarrit duhet të jetë kompatibel me prezencën e njeriut dhe presion gjatë veprimit jo me shume se 34.5 Bar.
- Kohezgjatja e jetëgjatësisë në atmosfere jo me shume se 5 dite
- Koncentrimi i përdorur të jetë me i vogël se 6%
- Marzhi i sigurisë të jetë jo me i vogël se 60%
- Marzhi i ruajtjes së hapësirave të zena (NOAEL) të jetë jo me pak se 10%
- Garanci të prodhuesit ndaj ndalimit dhe kufizimit të agjentit për shkak të ndryshimit të një prej parametrave të mesiperm, për të pakten 15 vjet.

8.8. Sistemi i monitorimit

Në të dy ambientet, dhomën e serverave dhe dhomën teknike, si edhe në secilin rack, duhet të monitorohen parametrat operacional të punës, dhe të gjenerohen alarme sa here që një parameter kalon “trigerat” e percaktuar në sistem.

Me konkretisht, sistemi i monitorimit duhet të monitorojë:

- Temperaturën dhe lageshtinë në secilin kabinet (4 cope).
- Temperaturën dhe lageshtinë në ambientin e dhomës së serverave (1 cope).
- Temperaturën dhe lageshtinë në dhomën teknike (1 cope).
- Hapjen/Mbylljen e çdo derë; të dy dhomave dhe të secilit prej kabineteve (6 cope).
- Prezencën e ujit në dhomën e serverave dhe në dhomën teknike, me anë të dedektoreve të tipit “litare” me gjatësi të dedektorit minimalisht 10 m (2 cope).
- Prezencën e levizjeve në dhomën e serverave dhe në dhomën teknike (2 cope).
- Nderprerjen e energjisë elektrike nga rrjeti (1 cope).

Temperatura në dhomë duhet të mbahet $+21^{\circ}\text{C}$, dhe lageshtia relative rreth 60 %. Do të konsiderohen Paralajmerim çdo rritje temperature me $\pm 4^{\circ}\text{C}$ dhe çdo rritje lageshtie me +10%. Ndërsa kritike do të konsiderohet çdo rritje temperature mbi $\pm 7^{\circ}\text{C}$, dhe çdo rritje lageshtie me +15%. Operatorët ekonomik, janë të lire të ofrojnë zgjidhje dhe arkitektura të ndryshme, mjafton që parametrat e mesiperme të jenë të monitoruara. Sistemi i monitorimit duhet të ketë webserver të integruar, për konfigurim dhe operim lokal, “data logging” të integruar dhe duhet të ruajë trendin/historikun e sistemeve apo sensoreve lokalisht.

Alarmet duhet të kategorizohen minimalisht në 3 kategori:

- Njoftim
- Paralajmerim
- Kritik

Njoftimet duhet të dërgohen me email, ndërsa paralajmerimet dhe kritik duhet të dërgohen me email dhe me SMS. Sistemi duhet të ketë gjithashtu një aplikacion, në të cilin të ndërtohet planimetria e

dhomave me të gjitha komponentet e tyre dhe shfaqjen e parametrave për secilen komponente në planimetri. Gjithashtu sistemi duhet të suportojë integrimin e pajisjeve / sistemeve nëpërmjet protokolleve të hapura të industrise, minimalisht SNMP, ModBUS, dhe BACnet.

8.9. Sistemi i kontrollit të aksesit

Kontrolli i aksesit duhet të realizohet për dhomën ekzistuese të serverave, për dhomën teknike, si dhe për të gjithë kabinetet (4 kabinete ekzistuese). Aksesit në dhomën teknike, në dhomën e serverave, dhe në secilin rack do të jete i kontrolluar, dhe do të lejojë aksesin vetëm për personat e autorizuar në zonen peraktese. Kontrolli i aksesit do të behet me ane të teknologjise RFID. në hyrje dhe në dalje të dhomës së serverave dhe të dhomës teknike duhet të instalohen lexues RFID. për çdo hyrje/dalje duhet të ruhen “loget” përkatëse me oren e hyrje/daljes si edhe emrin e përdoruesit. në secilin prej kabineteve ekzistuese, duhet të nderrohen dorezat dhe bravat ekzistuese mekanike të kabineteve, me doreza rrotulluese që kane të integruar lexues RFID dhe me brava elektrike ose magnetike. Sistemi i kontrollit të aksesit duhet të jete i pajisur me softin perkates për administrimin e sistemit; për shtim përdoruesish, shtim kartash, përcaktimin e profileve të secilit përdorues si edhe me gjenerimin e raportit të aksesit.

Gjithashtu, duhet të jete i pajisur me aplikim për kontrollin vizual të dhomës, ku të ngarkohet planimetria si edhe të shihen në kohe reale “event loget”. Nga i njejt aplikacion të behet edhe hapja/mbyllja e detyruar e dyerve.

8.10. Sistemi CCTV

Në dhomën teknike duhet të instalohet nje sistem CCTV për të monitoruar aktivitetin brenda dhe jashte dhomës. Sistemi që do të instalohet duhet të jete IP, me rezolucion 5Mpixel. Brenda në dhome duhet të instalohen dy kamera. Nje kamera duhet të vendoset jashte derës së dhomës për të monitoruar hyrje/daljet në dhome. Kamerat duhet të regjistrojne gjatë gjithë kohes në nje NVR me 4 kanale, të pajisur me HDD për të ruajtur për minimalisht 30 dite videot me rezolucion maksimal dhe 10 fps. Sistemi CCTV duhet të integrohet me sistemin e kontrollit dhe menaxhimit, në mënyrë që sistemi i kamerave të monitorohet nga i njejt software operimi.

8.11. Sistemues kabllosh horizontale

Per menaxhimin e kablllove, për çdo patch panel të instaluar duhet të instalohet nga nje patch guide horizontal 1U, tipi kreher me kapak. E pershtatshme për menaxhimin e kablllove fibër optike dhe baker (ethernet). Ngjyra e zeze.

8.12. Sistemues kabllosh vertikale

Per menaxhimin e kablllove në rack duhet të perdoren menaxhues kabllosh vertikale, në të dy anet, në pjesen perpara rack-ut. Dimensionet minimale: 10 cm x 11 cm (gjeresi x thellesi). Tipi: kreher me kapak. Ngjyra: e zeze.

8.13. Patch Cord OM5

Patch cord-at e fibrave optike duhet të nderrohen. Patch cord-at që do të perdoren duhet të jenë OM5, me gjatësi 1 m, duplex dhe me konektore SC/UPC-LC/UPC. Patch cord-at duhet të jenë me veshje PVC që vonojne djegien.

8.14. Patch Cord ethernet Cat.6A

Patch cord-at ethernet që do të perdoren duhet të jenë të kategorise Cat.6A, FTP. Duhet të jenë me veshje zjarr duruese, pa halogen LSZH/LS0H.

9. Dorëzimi i dokumentacionit

Kontraktori me përfundimin e implementimit dhe testimit, duhet të kryeje dokumentimin e të gjithë procesit të implementimit sic është paraqitur edhe në planin e punës. të gjitha dokumentat duhet të jenë në gjuhen shqipe.