LËNDA: Plani për sigurinë e rrjetit dhe informacionit sipas Rregullores së AKEP Nr. 37, datë 29.10.2015 "Mbi masat teknike dhe organizative për të garantuar sigurinë dhe integritetin e rrjeteve dhe/ ose shërbimeve të komunikimeve elektronike (Aneksi 3)

Ky informacion përfshin të gjitha pikat e Aneksit 3 të rregullores së AKEP

Pika D1: Qeverisja dhe Menaxhimi i Riskut

- Përgjegjësi i rrjetit kujdeset në çdo moment për menaxhimin e riskut duke bërë të mundur në rast identifikimin, përcaktimin, prioritizimin e riskut duke përdorur mjete sa më ekonomike dhe të koordinuara për të minimizuar, monitoruar apo për të zvogëluar probabilitetin që një risk të ndodhë.
- Të gjithë punonjësit e Nisatel Sh.p.k vihen në dijeni për sigurinë dhe janë subjekt i një kontrolli vjetor nëse janë konform zbatimit të rregullave dhe standardeve të sigurisë.
- Të gjithë punonjësit e Nisatel Sh.p.k janë në dijeni për punën që duhet të kryejnë dhe çfarë lidhet me ta duke mos cënuar as privatësinë e të tjerëve si dhe as sigurinë e sistemeve duke u pajisur secili me account të dallueshëm nga tjetri.
- Politikat e sigurisë rishikohen në mënyrë periodike nga përgjegjësi i rrjetit duke bërë të mundur shmangien e incidenteve, shkeljet, që mund të kenë ndodhur më parë ofruesve të tjerë.
- Në mënyrë periodike bëhen kontrolle apo skanime të sistemeve dhe programeve të implementuara për punë në mënyrë që të identifikohet apo ndalohet sulmi nga ndonjë virus, malware, apo sulm pirat.
- Punonjësit janë përgjegjës për mbrojtjen dhe trajtimin me kujdes të pasurive të shoqërisë. Të gjitha llojet e informacioneve mbrohen me sisteme, me standarde të larta të sigurisë si nga prodhuesit edhe nga instalimet e implementuara prej shoqërisë sonë.
- Në rast të incidenteve me palët e treta mbahen rekorde për këto incidente duke bërë të mundur rishikimin e rregullores për sa i përket sigurisë për palët e treta.
- Personi përgjegjës për risqet ka për detyrë zbulimin dhe identifikimin e kërcënimeve përpara se ato të ndodhin duke bërë të mundur planifikimin dhe veprimtarinë parandaluese gjatë kohës kur një proces, aktivitet apo shërbim është duke u ekzekutuar.
- Personi përgjegjës për risqet zbaton një procedurë standarte për identifikimin e kërcënimeve dhe raportimit menjëherë te Përgjegjësi i Departamentit dhe Administratori.
-

Pika D2: Siguria e Burimeve Njerëzore

- Të gjithë punonjësit ndjekin trajnime të herëpashershme për sa i përket sigurisë teknike të tyre apo dhe sigurisë së sistemeve që janë duke përdorur.
- Të gjithë punonjësit janë të detyruar të zbatojnë kërkesat e rregullores së sigurimit teknik për mbrojtjen në punë. Shkelja ose mos-zbatimi i këtyre rregullave dhe udhëzimeve, përbën shkelje të disiplinës në punë dhe sipas shkallës së shkeljes ngarkon me përgjegjësi punonjësin, i cili ka kryer këtë shkelje, (shkeljet trajtohen në bazë të rregullores së brendeshme të shoqërisë).
- Punonjësve, mbi bazën e udhëzimeve të Kodit të Punës, u është vendosur në dispozicion, pranë qendrës së punës, kutia e ndihmës së shpejtë.
- Ne baze te Udhezimeve dhe Protokolleve te Ministrise se Shendetesise dhe Mbrojtjes Sociale, ne sportelet e sherbimit ndaj klientit, jane vendosur barriera fizike prej peçikllasi si dhe punonjesit jane te pajisur me maska dhe disinfektues me baze alkoli. Ambientet e punes disinfektohen cdo dite.

- Secili prej punonjesve ne momentin e deklarimit si punonjes i Nisatel paraqet prane zyrave Qendrore raportin mjeko-ligjor si nje vertetim se eshte i shendetshem dhe i afte per pune.
- Punonjesit u nenshtrohen testeve per sa i perket sigurise ne pune dhe ne baze te pergjigjeve marrin nje vleresim i cili nese rezulton i ulet punonjesi do te ritrajnohet duke organizuar ritrajnime dhe sesione per ceshtjet e sigurise te organizates referuar nga nje person pergjegjes per sigurine e personelit.
- Te gjithe punonjesit kane marr pjese ne trajnimin e organizuar per fiksen e zjarrit me perfaqesues te kualifikuar te »La Fenice Zjarrfikes sh.p.k«.Fiksja e zjarrit eshte vendosur ne nje ambjent te dukshem dhe lehtesisht te aksesueshem nga te gjithe punonjesit ne rast zjarri duke ndjekur procedurat per shuarrjen e zjarrit .
- Cdo punonjesi i eshte vene ne dijeni procedura qe ndiqet ne raste thyerjeje rregulloreje apo moszbatim te masave mbrojtesve te percaktuara per ta.
- Cdo punonjes i ri trajnohet per sigurine teknike dhe perdorimin e masave mbrojtese per sigurine gjate punes dhe cdo punonjes mban pergjegjesi per mosperdorimin dhe moszbatimin e masave mbrojtese duke iu nenshtruar procedurave te percaktuara ne rast thyerjeje rregullash .
- Ne rregullore e brendeshme pershkruhet qarte se cdo punonjes, duhet te perdori ne menyre esplicite dhe unike, kredencialet e tij, dhe jo te dikujt tjeter per te aksesuar apo monitoruar sisteme/software, apo burime te kompanise.
- Punonjesit te cilet nuk jane me pjese e kompanise, (largohen nga puna) u revokohen ne menyre te menjehershme privilegjet dhe kredencialet, te gjitha llogarite qe dispononin kalojne ne statusin **Jo-aktive**.
- Mbivendosja e fjalëkalimit bëhet vetëm nga personi i autorizuar i teknologjisë së informacionit pas një kërkese me shkrim, derguar ne departamentin e IT-se.
- Largimi i punonjesve nga pozicionet e tyre te punes, rezulton me revokimin e badge-it dhe akses-card-es ne varesi te pozicionit dhe aksesit qe i jane caktuar.
- Administratori është personi përgjegjes për mbajtjen e të dhënave në lidhje me të gjitha aksesimet e autorizuara, ku përfshihen detaje si: emri i punonjësit, pozicioni i punes, data, ora dhe dita deri kur i lejohet aksesimi.

Ndër politikat kryesore, përfshihen referencat tek logset e sistemeve/software-ve, apo burimeve te tjera të kompanisë.

Të gjithë punonjesit e kompanise instruktohen në lidhje me mënyrat e krijimit dhe administrimit të fjalëkalimeve per zgjedhjen e fjalëkalimit fillestar, ndryshimin e fjalëkalimit dhe këshilla të njohura sigurie për zgjedhjen e tij, mbrojta e fjalëkalimit si dhe ndalimi i dhënies së fjalëkalimit midis përdoruesve.

Përdoruesve u kërkohet ne kontrate te pranojnë se ata i kanë lexuar dhe i kanë kuptuar rregullat dhe qe do t'i zbatojnë ato rigorozisht.
I gjithë personeli i kompanise është përgjegjës për respektimin dhe për ruajtjen e nivelit të kërkuar të sigurisë gjatë kryerjes së detyrave per te cilat jane ngarkuar.

- Personat, të cilët nuk janë punonjës të kompanise, nuk lejohen të aksesojnë ne asnje moment pajisjet, sisteme dhe pasurite e kompanise.
- Personat që kanë akses në sistemin dhe pajisjet e kompanise janë të detyruar të jenë të vetëdijshëm për rregullat dhe standardet e sigurisë, keto te fundit, azhornohen se bashku me rregulloren e brendeshme te kompanise, me nje periodicitet 90-ditor.

- Ripozicionimi i punonjesve eshte nje metode e fuqishme e kompanise ne menyre te tille qe te rris dhe forcoje aftesite e punonjesve dhe te shmang boshlleqet duke fuqizuar punen ne grup .

- Per cdo departament ka nje pergjegjes perkatesisht ne listen me poshteshenuar:

- Pergjegjes rrjeti fiber	Adriatik Karameta
- Pergjegjes centrali dhe transmetimi	Kostjan Kekezi/ Detion Jahaj
- Pergjegjes Koordinimi	Klodjan Goclari
- Pergjegjes i Punimeve Civile	Astrit Hitaj

- Kompania ben nje pasqyre te personave te larguar dhe ripozicionim e punonjesve, tabela meposhte pasqyron ripozicionimet e fundit qe kane ndodhur ne hierarkine e kompanise:

- Administrator (CEO)	Lorena Haxhiraj
- Pergjegjese marketing	Brixhilda Bregasi

- Punonjesit e rinj trajnohen per punen.
- Me poshte disa nga trajnimete zhvilluara, shkeputur si fragment nga regjistrat e kompanise per trajnimin dhe hyrjet e reja te punonjesve:
- Shkurt 2020 - Trajnim per rrjetin fiber, problematikat aktuale, krijimi i konektoreve fundor.
- Qershor 2020 – Trajnim per teknologjite e perdorura ne Nisatel Sh.p.k
- Shtator 2010 – Tetor 2010 – Trajnim per teknologjine VOIP
- Dhjetor 2010- Mediat e Transmetimit, fiber, baker.

Pika D3: Siguria e sistemeve dhe pajisjeve

- Të gjitha pajisjet e kompanise mbrohen fizikisht nga kërcënimet e sigurisë dhe nga rreziqet e mjedisit, qofshin keto nga faktore atmosferike, apo faktore njerezor me qellime keqdashese.
- Pajisjet jane te alokuara në dhoma të mbyllura e të sigurta. Dhomat e pajisjeve jane pajisur me mjete sigurie te larte, celes me alarm, ajër të kondicionuar, kamera, UPS dhe me fikese-zjarri, si dhe sistem per detektimin e tymrave. Ambientet ne te cilat jane alokuar pajisjet kane te siguruar autonomi per emergjencat elektrike, mund te punojne deri pa hasur probleme ne momentin qe mungon rryma elektrike,(si pasoje e faktoreve te jashtem). Roli kryesor ne kete rast luhet nga UPS-et te cilet revizionohen here pas here per tu siguruar qe performanca e tyre nuk ka rrene.
- Format e komunikimit ne sistem qe perdor kompania jone, jane të mbrojtura kundër humbjeve, ndërhyrjeve dhe korruptimit, respektojne rigorozisht privatesine e komunikimit.
- Ne raste kur kerkohet pergjimi i ligjshem nga autoritetet e ngarkuara me ligj, kompania zbaton te gjitha masat, e percaktuara ne rregulloren e brendeshme per te vendosur ne dispozicion informacionin e kerkuar nga organet e siper-permendura.
- Të gjitha të dhënat sensitive te sistemit u bëhet *backup* (kopje) i rregullt në përputhje me procedurat teknike periodikisht sic parashikohet ne rregulloren e brendeshme, te departamentit perkates, te IT-se.
- Kopjet (backup-et) e të dhënave ruhen në vende të mbrojtura nga zjarri dhe jashtë ambienteve ku mbahen serverat prej të cilëve janë marrë ato,
- Kopjet (backup) e të dhënave testohen rregullisht per integritetin e tyre, ne menyre te tille për t'u siguruar që mund të përdoren në raste të nevojshme.
- Procedurat e rikrijimit (restore) të të dhënave testohen rregullisht për t'u siguruar që ato janë të efektshme dhe që ato mund të ekzekutohen brenda kohës së lejuar, kjo kohe, eshte e varjueshme per

makina te ndryshme, virtuale apo fizike. Te gjtha hapsirat e kohes qe nevojiten per te rikthyer funksionale, nje apo me shume sherbime te afektuara ne nje apo me shume makina, jane marre parasysh ne RT (Recovery Time).

- I gjithë personeli i kompanise të cilit i lejohet akses në Internet dhe në shërbim email-i te kompanise me kusht qe te te tregojne kujdes nga viruset duke zbatuar masat e sigurise, per te cilat azhornohen here pas here, ne formatin elektronike cdo 30 dite dhe ate te fizik ne cdo 90 dite.(I printuar , hardcopy)
- Identifikimi i përdoruesit mbulon procedurat për t'u siguruar që çdo sistem është i aftë të njohë personat e autorizuar dhe të kryejë veprimet e duhura penguese, në rastet e përpjekjeve për aksesim të paautorizuar.

Çdo përdorues identifikohet në mënyrë individuale nëpërmjet një llogarie unike përdoruesi, pra nje username dhe passëord,(ku ky i fundit kerkohet nga ana e sistemit automatikisht te nderrohet pas nje periudhe te caktuar kohe, duke zbatuar nje nga pikat kyce te sigurise se te dhenave).

Personelit u ndalohet rreptësisht shpërndarja e llogarisë personale/klienteve. Thyerja e këtij rregulli do të trajtohet si shkelje e rëndë, per te cilen merren masat perkatese.

Një llogari unike përdoruesi siguron vetëm mënyrën e autentifikimit për përdoruesit/klientit, ndalohet rreptësisht dy ose më shumë aksesime të njëkohshme me të njëjtën llogari përdoruesi,

kjo fale politikave te sistemeve dhe burimeve te kompanise per mos-lejimin e dublikimit te hyrjeve ne sistem.

Pika D4: Menaxhimi i Operacioneve

Operacionet jane dy llojesh, operacione pjese e nje sistemi apo sherbimi te planifikuar per implementim dhe operacione te cilat kane funksion mirembajtes, update-ues apo ndryshues ne sistemet ose sherbimet ekzistuese te infrastruktures se rrjetit.

Sherbimet e mirembajtjes se sistemit jane 100 % efektive ne cdo dite perfshire backup, etj.
Të gjitha procedurat që lidhen me teknologjinë e informacionit dokumentohen dhe ruhen per referenca te mevonshme.

Këto përfshijnë, në mënyrë të veçantë, procedurat e hapjes dhe të mbylljes,se portave te pajisjeve te cilat ofrojne sherbim, si dhe *backup*-et dhe mirëmbajtjen rutinë për të gjitha elementet e mjedisit të sistemit dhe rrjetit të kompanise.

Te renditura sipas shkalleve te ekzigjencave, operacionet e mirembatjes nisin nga Core-Netëork, te skeduluara dhe te kryera ne orare te pershtetshme per nderhyrje. Me tutje procedurat menaxhuese perfshijne Edge-, ne te cilin po ashtu skedulohen nderhyrje, si dhe shkalla e nderhyrjeve.

Procedurat e operimit mbulojnë si operacionet normale ashtu edhe administrimin e incidenteve te parashikueshme, duke përfshirë keqfunksionimin e pajisjeve ose të programeve, të dhënat jo të sakta ose të dëmtuara, difektet në pjesët që i përkasin providerit te internetit, sulmet keqdashëse dhe tentimet per thyerjet e konfidencialitetit.

Çdo përdorues identifikohet në mënyrë individuale nëpërmjet një llogarie unike përdoruesi, pra nje username dhe passëord,(ku ky i fundit kerkohet nga ana e sistemit automatikisht te nderrohet pas nje periudhe te caktuar kohe, duke zbatuar nje nga pikat kyce te sigurise se te dhenave).

Personelit u ndalohet rreptësisht shpërndarja e llogarisë personale/klienteve. Thyerja e këtij rregulli do të trajtohet si shkelje e rëndë, për të cilen merren masat përkatese.

Një llogari unike përdoruesi siguron vetëm mënyrën e autentifikimit për përdoruesit/klientit, ndalohet rreptësisht dy ose më shumë aksesime të njëkohshme me të njëjtën llogari përdoruesi, kjo fale politikave te sistemeve dhe burimeve te kompanise per mos-lejimin e dublikimit te hyrjeve ne sistem.

Pika D5: Menaxhimi i Incidenteve

Një incident sigurie është ngjarja e cila mund të ndikojë në integritetin, disponueshmërinë dhe në konfidencialitetin e informacionit, por jo vetem, incidentet mund te afektojne mbare-vajtjen e sherbimeve, qofshin keto te fundit telefoni, internet apo iptv.

Dëmtimet si pasojë e incidenteve të sigurisë dhe të keq-funksionimeve minimizohen ne maksimum dhe, sa herë që është e mundur parandalohen. Ne rregulloren e brendeshme te kompanise, eshte perfshire nje seksion i vecante per manaxhimin e incidenteve I kategorizuar ne disa shkalle. Ndarja e tyre behet bazuar ne rendesine e pasojes qe sjell incidenti.
Meposhte jepet nje liste e incidenteve qe kemi parashikuar ne rregulloren e brendeshme:

1) Incidente te shkaktuara nga ***sulmet e jashtem*** kundrejt pajisjeve qe per hire te rolit te tyre jane te ekspozuara nepermjet IP publike, (normalisht keto pajisje jane te mbrojtura me fireëall dhe aksimi ne to eshte i pasijur me ACL filter).

2) Incidente te shkaktuara nga ***demtimi/deshtimi i pajisjeve***, te cilat jane pjese ofruese e sherbimeve, telefoni, iptv, internet.

3) Incidentet te shkaktuar nga ***kompromenimi i informacioneve sensitive*** te kompanise nga punonjesit, apo ish-nenpunesit e kompanise.

4) Incidente te shkaktuara nga ***shkaqe natyrore,***si termetet, zjarret, permbytjet, etj.

Incidentet që ndikojnë mbi sigurinë vlerësohen me seriozitet dhe të raportohen menjëherë tek Shefi Sigurise dhe Administratori.
Për të gjitha rastet e ngjarjeve që lidhen me sigurinë ndiqet një procedura *për* raportimin e incidenteve sipas raportimit te percaktuar nga AKEP ne rregulloren nr.37.
I gjithë personeli eshte i detyruar për të raportuar çdo dobësi të sigurisë ose çdo kërcënim të vënë re në procedura, në sisteme dhe në shërbime.
Për të minimizuar çdo ndërprerje të shërbimit internet apo çdo dëmtim të të dhënave, i jepet prioritet si pune që keqfunksionimi i programeve të korrektohet sa më shpejt që të jetë e mundur.
Kur pergjegjesi apo administratori veren se veprimtaria e një punonjësi nuk është në përputhje me rregullat dhe procedurat e sigurisë, për çfarëdolloj arsyeje, ai organizon një takim me punonjësin për të diskutuar çështjen dhe për të planifikuar veprimet korrigjuese te tij ne nje kohe sa me te shkurter.

Pika D6: Menaxhimi i Vazhdimit të Biznesit

Duke patur parasysh se veprimtaria e Nisatel , ne tregun e telekomunikacioneve, monitorohet , nga autoritete si AMA dhe AKEP per sherbime qe ofrohen prej Nisatel, nuk hezitohet asnjehere qe tu referohemi rregulloreve perkatese per implementimet e sherbimeve te reja, apo atyre ekzistuese.
Nder qellimet kryesore te Nisatel eshte dhe do te jete shtrirja dhe ekspansioni sa me i gjere gjeografikisht.
Titullaret e kesaj kompanie kane implementuar poliktika te tilla, qe sherbimet te cilat ofron Nisatel te jene ne redundace te vazhdueshme , duke parandaluar faktin qe mund te mos kete sherbim(kjo per arsye te cilat nuk lidhen drejte per drejte me Nisatel)
Ndërprerje jashte kontrollit tone mund të shkaktohen nga shkaqe natyrore, nga aksidente, nga difekte të pajisjeve, nga veprime të qëllimshme ose nga difekte të shërbimeve.Nder masat e marra jane si meposhte:

1) Te gjitha pajisjet te cilat jane me rendesi te vecante kane minimalisht nje tjeter (pajisje te ngjashme) rezerve, qofte kjo ne sektorin e magazines, ose ne site ku eshte e alokuar pajisja aktive. Kjo pajisje mund te jete rendunte –aktive,/pasive ne varesi te rendesise se sherbimeve qe kalojne nepermjet saj.
2) Te gjitha pikat e shperndarjes se sherbimeve , te alokuara neper zona te ndryshme te
3) qytetit, jane te lidhura me sallen qendrore te pajisjeve , me minimalisht 2 rruge fizike, kjo per efekt redundance.
4) Gjate instalimit te pajisjeve simulohet koha qe u nevojitet sherbimeve ne rast keq-funksionimi per tu ribere aktive. Ne baze te procedurave, percaktohet shkalla e defektit
5) dhe kohezgjatja per ta ri-vendosur ne pune pajisjen ne fjale. Trajtohen me rigorozitet te gjitha mundesite duke marre ne konsiderate edhe rastin qe pajisja eshte difektuar ne masen 100%, procedurat qe ndiqen, jane te percaktuara ne BCP-ne e kompanise, e cila perfshin , kalimin ne pajisjen reduntante te sherbimeve, (ne rastin kur keto te fundit nuk kane kaluar automatikisht)
6) Ndikimi I faktoreve natyror, si permbytjet, termetet, etj, jane marre masa qe sherbimi te jene redundant nga disa pika shperndarje , duke mos lejuara mungesen totale te sherbimit.

Pika D7: Monitorimi, Auditimi dhe Testimi

Pajisjet e rrjetit duke perfshire routerat, sëitchet dhe modemet kabllore, gjenerojne informacione prej logseve pra informojne sallen operative mbi aktivitetet e kryera ne keto pajisje.
Aplikacionet identifikojne veprimet e kryera ne to, kohen e kryerjes dhe qellimin prej logseve te regjistruara. Sistemet apo sherbimet jane te kategorizuar ne elemente te infrastruktures se rrjetit ne te cilat implementohet sistemi i regjistrimit te logseve per aktivitet qe kryhen ne to.
Informacionet qe gjenerohen nga keto sisteme logs-esh jane te ndryshme dhe ja disa prej tyre:

1. IP Addressa e pikave fundore te rrjetit
2. Parametrat teknike te rrjetit per aktivitetin e nje pajisje apo klienti
3. Sherbimi i kryer
4. Ora dhe Data e aktiviteteve

5. Vlerat e trafikut te gjeneruar
6. Veprimtaria e marre nga pajisja per kerkesat e mesiperme.

Logset e aplikacioneve ofrojne nje sherbim te rendesishem ne infrastrukturen e kompanise dhe ketu perfshijme logset nga programi i menaxhimit te klienteve, ne te cilin perfshihet edhe faturimi, kapaciteti i paketes perkatese, kontrolli prinderor, etj.
Keto informacione perdoren ne menyre te vazhduar nga pergjegjesi i sigurise vetem per detyrat e caktuara dhe per te analizuar veprimtarite e meparshme nga sistemet, pajisjet apo sherbimet per vlerat e gjeneruara.
Keto informacione perdoren per te identifikuar anomali, sulme apo sjellje jo brenda standartit te lejuar te pajisjeve, sistemeve apo personave punonjes ose kliente te kompanise.
Sistemet e Logseve ruajne te dhena deri ne 1 muaj nga momenti i regjistrimit te logeve ne sistem.
Testimet: Ne fazen e kryerjes se testit, regjistrohet me menyrat e percaktuara ne planifikim cdo rekort i kerkuar ne dokumentacionin e testit.
Ne raportin e testit pershkruhen te gjithe procedurat e ndjekura dhe perkrah tyre vlerat e nxjerra nga keto procedura.
Gjithashtu pershkruhen konfigurimet e ndryshuara ne sisteme apo sherbime per realizimin e testit si dhe procedurat e kthimit te konfigurimeve ne gjendjen e meparshme, te gjitha keto te dhena, rruhen ne nje server te vecante qellimi i te cilit eshte pasqyrimi i nje historiku per fazen e testime.
Faza e fundit e sistemit te testimit eshte kryerja e analizes se vlerave te gjeneruara nga procesi i testimit nga ana e pergjegjesit te sistemit apo sherbimit dhe personit pergjegjes per kryerjen e testimit.
Auditimi: Personi pergjegjes per kryerjen e auditimit e realizon kete proces me kerkese te Administratorit te Kompanise dhe autorizimit me shkrim te tij. Ne rastin kur nje punonjes i kompanise dyshon ne keqfunksionim te nje elementi te infrastruktures se rrjetit ai i drejtohet pergjegjesit te departamentit perkates, dhe ku i fundit kerkon me nje kerkese te vecante , ne dijeni te administratorit , nderhyrjen e personit auditues per sherbimin perkates, mbi te cilin eshte bere auditimin.

Personi pergjegjes kryen auditimin e problemit dhe perpilon nje dokumentacion mbi raportimin e situatave te zbuluara te cenuesshmerise. Materiali i dergohet Administratorit dhe pergjegjesit te departamentit per te ndermarre veprimet e duhura teknike per te parandaluar riskun e mundshem.

Regjistri incidenteve

TABELA PER VLERESIMIN E IMPAKTIT TE INCIDENTIT TE SIGURISE		
Sulm pirat karshi serverave te DNS-ve	*>30min*	*>60min*
Numri i perdoruesve te prekur nga incidenti ose % e tyre ndaj numrit total te perdoruesve te ofruesit te sherbimit	260	260
>1000ose>5%	*Mesatar*	*I Larte*

Ne rast te nje numri te panjo hur te perdoruesve te prekur nga incidenti i sigurise, zona gjeografike e shtrirjes se in cidentit te sigurise	-	-
>20km²	*Mesatar*	*I Larte*
Vleresimi Perfundimtari Impaktit:	*Mesatar*	*I Larte*

DEKLARATA E APLIKIMIT		
SO 2.1	a) Bëj një listë të risqeve kryesore për sigurinë dhe vazhdimësinë e rrjeteve dhe/ose shërbimeve të ofruara të komunikimit, duke marrë në konsideratë kërcënimet kryesore për burimet e rëndësishme. b) Vendos në dijeni personelin kyc për risqet kryesore dhe sesi ti trajtosh ato.	Rregullorja e brendeshme perfshin planin e manaxhimit te rrezikut.
SO 2.2	c) Krijo dhe vendos një metodologji të menaxhimit të riskut dhe/ose mjetet bazuar në standartet e industrisë. d) Siguro që personeli kryesor përdor metodologjinë dhe mjetet e menaxhimit të riskut e) Rishiko vlerësimet e riskut pas ndryshimeve ose incidenteve. f) Siguro që risqet e mbetura pranohen nga menaxhimi.	Perfshihet ne Risk Management, seksioni i rregullores se brendeshme
SO 2.3	g) Rishiko metodologjinë dhe/ose mjetet e menaxhimit të riskut, në mënyrë periodike, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.	Si me siper.
SO 3: Rolet e Sigurise dhe Pergjegjesite		
SO 3.1	a) Caktoji personelit rolet e sigurisë dhe përgjegjësitë. b) Siguro që rolet e sigurisë janë të arritshme në rast se ndodhin incidente sigurie.	Aktivitetet e sigurisë së informacionit koordinohen nga përfaqësues nga pjesë të ndryshëm të NISATEL të përcaktuara / rolet dhe përgjegjësitë përkatëse sipas funksioneve të tyre të punës. Rrjedhimisht një skuadër SMSI është formuar për të mbështetur në mënyrë aktive sigurinë brenda NISATEL dhe rolet dhe përgjegjësitë e tyre janë të përcaktuara në mënyrë të qartë, trajnuar dhe në bazë të njohjes (pershkrimet e posteve te punes)
SO 3.2	c) Personeli emërohet zyrtarisht në rolet e sigurisë. d) Vendos personelin në dijeni të roleve të sigurisë në organizatë dhe kur duhet të kontaktohen.	
SO 3.3	e) Struktura e roleve të sigurisë dhe përgjegjësive rishikohet rregullisht, si pasojë e ndryshimeve dhe/ose incidenteve të mëparshme.	Rregullorja e brendeshme, seksioni i Drejtimit.
SO 4: Siguria e asteve te pales se trete		
SO 4.1	a) Përfshini kërkesat e sigurisë në kontratat me palët e treta.	
SO 4.2	b) Vendos një politikë sigurie për kontratat me palët e treta.	Marredheniet me palet e treta rregullohen nga kontratat e lidhura konform ligjit. Ne kontrate
D1: Qeverisja dhe Menaxhimi i Riskut		
SO 1: Politika e Sigurise se Informacionit		

SO 1.1	a) Vendos një politikë sigurie të nivelit të lartë që adreson sigurinë dhe vazhdimësinë e rrjeteve të komunikimit dhe/ose shërbimeve të ofruara prej tyre.	Nisatel, zoteron nje plan politikash per manaxhimin dhe permiresimin e sherbimit IT, lidhur me sigurine e informacionit, planifikimet financiare etj.
	b) Vëje ne dijeni personelin kyc për politikën e sigurisë.	Plani i politikave shperndahet elektronikisht tek personat pergjgegjes, pas cdo azhornimi.
SO 1.2	c) Vendos politika të detajuara të sigurisë së informacionit për asetet kritike dhe proceset e biznesit d) Vendos në dijeni gjithë personelin për politikën e sigurisë dhe për cfarë lidhet me punën e tyre. e) Rishiko politikën e sigurisë pas incidenteve nese konsiderohet e nevojshme.	Perfshihet ne planin e politikave.
SO 1.3	f) Rishiko politikat e sigurisë së informacionit në mënyrë periodike dhe merr në konsideratë shkeljet, përjashtimet, incidentet e mëparshme, testet/ushtrimet e mëparshme dhe incidentet që kanë prekur ofruesit e tjerë në sektor.	Plani i politikave, rishikohet cdo 90 dite, dhe perditesohet ne rast nevojash te kompanise.
SO 2: Qeverisja dhe Menaxhimi i Riskut		
	c) Siguro që të gjitha prokurimet e shërbimeve/produkteve nga palët e treta janë në përputhje me politikën. d) Rishiko politikën e sigurisë për palët e treta, pas incidenteve ose ndryshimeve nese konsiderohet e nevojshme e) Redukto risqet e mbetura që nuk janë të adresuara nga pala e tretë.	percaktohen qarte te drejtat dhe detyrimet qe lindin perpalet, bashkelidhur me kontraten, firmoset nga pala kontraktuese, nga "Deklarata e Pergjegjesive Civile dhe Penale"
SO 4.3	f) Mbaj rekorde të incidenteve të sigurisë të lidhura ose të shkaktuara nga palët e treta. g) Rishikim dhe përditësim të politikës së sigurisë për palët e treta në intervale të rregullta, duke marrë në konsideratë incidentet dhe ndryshimet e mëparshme.	Nuk kemi patur raste incidentesh
D2: Siguria e Burimeve Njerezore		
SO 5: Kontrollet e Background-it		
SO 5.1	a) Kontrollo referencat profesionale të personelit kyc(administratorit të sistemit, oficerëve të sigurisë, etj)	Rregullorja e brendeshme , seksioni i Burimeve Njerezore
SO 5.2	b) Kryej verifikime të background-it për personelin kyc, kur nevojitet dhe lejohet ligjerisht. c) Vendos një politikë dhe procedurë për kontrollet e background-it.	Rregullorja e brendeshme , seksioni i Burimeve Njerezore

SO 5.3	d) Rishiko dhe përditëso politikën/procedurat për kontrollet e background-it dhe referencës në mënyrë periodike, duke marrës në konsideratë ndryshimet dhe incidentet e mëparshme.	Rregullorja e brendeshme, seksioni i Drejtimit.
SO 6: Njohuria mbi sigurine dhe trajnimi		
SO 6.1	a) Garanto personelin kyc me trajnime dhe materiale të përshtatshme mbi cështjet e sigurisë.	Personelit i vihen ne dispozicion Manualet me politikat perkatese te miratuara nga kompania dhe trajnohen ne lidhje me implementimin dhe zbatimin e tyre. Cdo punonjes nenshkruan deklaraten per njohjen e politikave
SO 6.2	b) Implemento një program për trajnimin, duke bërë të sigurt që personeli kyc ka njohuri të përditësuara dhe të mjaftueshme mbi sigurinë. c) Organizo trajnime dhe sesione ndërgjegjësimi për personelin në cështjet e sigurisë për organizatën.	Eshte perpiluar nje plan trajnimi ne lidhje me sigurine e informacionit, mbi mbrojtjen e te dhenave dhe shperndarjes se informacionit. Trajnimi i pare zhvilluar me departamentin NOC. Cdo departament e ka pjese te objektivave tremujore trajnimin e staffit.
SO 6.3	d) Rishiko dhe përditëso programin e trajnimit në mënyrë periodike, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme. e) Testo nivelin e njohurive mbi sigurinë të personelit.	Rregullorja e brendeshme, seksioni i Drejtimit.
SO 7: Ndryshimet e personelit		
SO 7.1	a) Kur ka ndryshime në personel, hiq të drejtat e aksesit, badget, pajisjet, etj kur nuk nevojiten më. b) Eduko personelin e ri për politikat dhe procedurat.	Zbatojme procedurat e perfundimit te marredhenies se punes. Plotesohet formular dhe nenshkruhet nga te gjithe menaxheret e kompanise Cdo punonjes i ri ploteson formularin e trajnimit ne cdo departament
SO 7.2	c) Implemento politikë/procedura për ndryshimet e personelit, duke marrë në konsideratë heqjen në kohë të të drejtave të aksesit, badget, pajisjet. d) Implemento politikën/procedurat për edukimin dhe trajnimin për personelin në rolet e reja.	Rregullorja e brendeshme , seksioni i Burimeve Njerezore
SO 7.3	e) Kontrolle periodike që politika/procedurat janë efektive. f) Rishiko dhe vlerëso politikën/procedurat për ndryshimet e personelit, duke marrë në konsideratë ndryshimet ose incidentet e mëparshme.	Punonjesi ka akses sipas pozicionit te punes. Aksesi ne sistem autorizohet nga dep ICT. Aksesi eshte i mundur vetem brenda rrjetit te zyrave ose nepermjet VPN. Aksesi monitorohet dhe verifikohet periodikisht nga Auditi i Brendshem i kompanise.
SO 8: Trajtimi i shkeljeve		

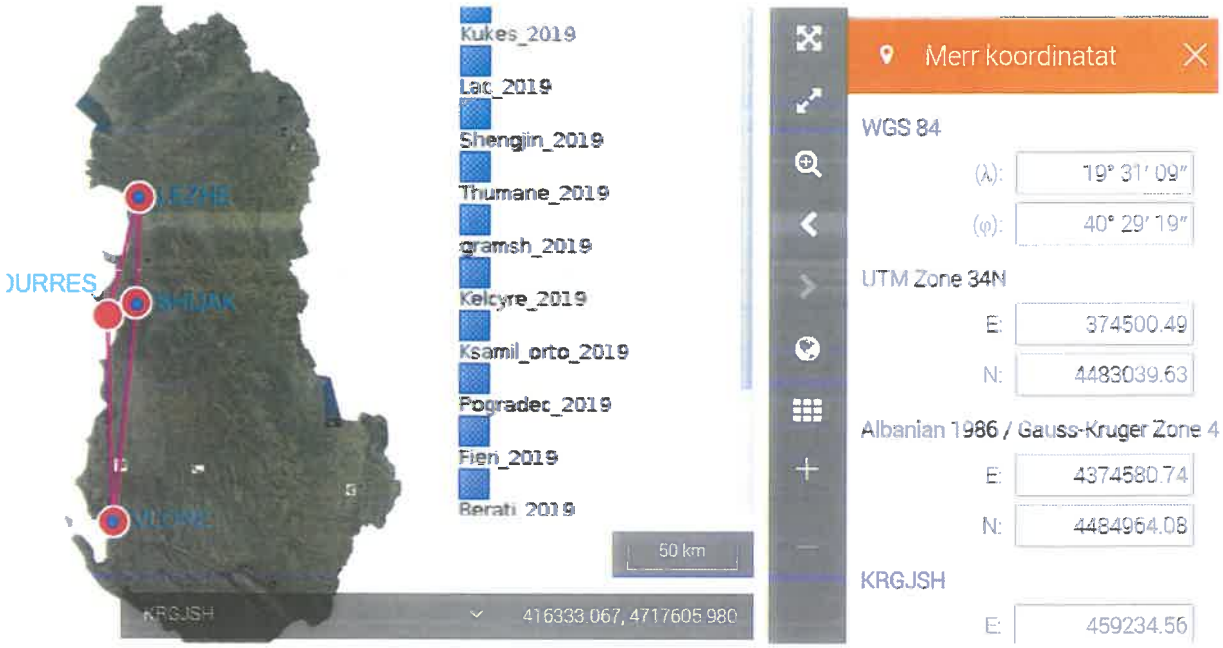
SO 8.1	a) Mbaj personelin të përgjegjëshëm për thyrjet e sigurisë të shkaktuara nga shkeljet e politikave, për shembull përmes kontratave të punes	Cdo punonjes nenshkruan Kontraten e Punes, Kontrate Konfidencialiteti, Kod Sjellje, Manualin e Sigurise ne Pune, Manualin Mbi Parandalimin e Zjarrit, Rregullore mbi Sigurimin Teknik ne pune, Kodi i Mbrojtjes, Përpunimit, Ruajtjes dhe Sigurisë të të dhënave Personale etj.
SO 8.2	b) Vendos procedura për shkeljet e politikave nga personeli.	I referohemi procedurave te Auditit te Brendshem. Ne rast konstatimi te shkeljeve perpilohen masat peratese duke respektuar legjislacionin ne fuqi, te Rep. se Shqiperise.
SO 8.3	c) Rishikim dhe përditësim periodik i procesit disiplinor duke u bazuar në ndryshimet dhe incidentet e mëparshme.	
D3: Siguria e Sistemeve dhe Pajisjeve		
SO 9: Siguria Fizike dhe e Mjedisit		
SO 9.1	a) Elemino aksesin fizik të paautorizuar te pajisjet dhe infrastruktura dhe kryej kontrolle mjedisore për mbrojtjen ndaj hyrjes së paautorizuar, vjedhjes, zjarrit, përmbytjeve etj.	Kompania ne kuader te sigurise fizike ka lidhur kontrate me agjensi e jashtme "Security" sipas nje rregulloreje te miratuar. Ne ambientet e brendshme te sigurise se larte si psh hyrja ne datacenter, ka akses me karte magnetike me gjurme ne sistem vetem per persona te autorizuar. Agjent sigurie 24x7 . Kontroll me kamera. Siguri e larte
SO 9.2	b) Implemento një politikë të masave të sigurisë fizike dhe kontrolleve të mjedisit.	
	c)Implementim i standarteve të industrisë mbi kontrollet fizike dhe të mjedisit.	ne datacenter. Monitorim 24x7. Alarm automatik me SMS,senore per tymin, lageshtine dhe zhurmat.
SO 9.3	d) Vlerëso efektivitetin e kontrolleve fizike dhe të mjedisit periodikisht. e) Rishiko dhe përditëso politikën për masat e sigurisë fizike dhe kontrollet e mjedisit duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.	I referohemi Manualit mbi Rregullat e Sigurimit Teknik dhe Manuali per parandalimin dhe mbrojtjen nga zjarri Rregullorja e brendeshme , seksioni i Drejtimit.
SO 10: Siguria e Burimeve		
SO 10. 1	a) Garanto sigurinë e burimeve si energjia elektrike, karburanti ose ftohësi.	Ne cdo pike sherbimi eshte instaluar nje gjenerator i cili furnizohet rregullisht me karburant. Sistem i mbrojtjes automatike. Ne cdo moment sistemi ushqehet nga baterite. Sistemi energjise nga Emerson Poëer dhe Gamatronic Poëer. Njoftim automatik me SMS. Jane perdorur kabllo te cilesise se larte me rezerve te pakten 5 here (psh nese konsumi nominal i nje pajisjeje eshte 5Amp kablli suporton te pakten 25Amp). Sistem i sinjalizimit automatik ne e-mail per temperaturen dhe energjine jashte normave. Alarm automatik ne e-mail nese nje pajisje eshte e shkeputur nga rrjeti. Pajisje per shuarjen e zjarrit. Procedurat dhe politikat e kompanise te cilat dergohen me e-mail te gjithe punonjesve ose dep te interesuar.
SO 10. 2	b) Implemento një politikë për sigurinë e burimeve kryesore, si energjia elektrike, karburanti etj. c) Implemento masat e sigurisë sipas standarteve të industrisë për të mbrojtur burimet dhe pajisjet.	
SO 10. 3	d) Implemento masat e sigurisë për të mbrojtur burimet. e) Rishiko dhe përditëso politikën dhe procedurat rregullisht, duke marrë në konsideratë ndryshimet dhe incidentet dhe ndryshimet e mëparshme.	
SO 11: Kontroll i Aksesit ne rrjet dhe sistemet e informacionit		

SO 11.1	a) Përdoruesit dhe sistemet kanë identifikim unik dhe autentikohen kur aksesojnë shërbimet ose sistemet. b) Implemento mekanizmin e duhur të kontrollit logjik për rrjetin dhe sistemet e informacionit për të lejuar vetëm kontrollin e autorizuar.	Cdo log ne akses monitorohet nepermjet sistemit. Punonjesi ka akses sipas pozicionit te punes. Aksesi ne sistem autorizohet nga dep ICT. Aksesi ne sistem autorizohet nga dep ICT dhe Aksesi eshte i mundur vetem brenda rrjetit te zyrave ose nepermjet VPN. Perdoruesit mund te ndryshojne passëord vete. Passwordet jane te enkriptuara MD5 ne sistem. Ne sisteme jane gjurmet e nderrimit te passë. Te drejtat e aksesit ne PC/Laptop kontrollohen nga ICD (niveli user jo admin). Te drejtat ne sistemin ABS verifikohen nga ICT cdo 3 muaj dhe auditohen te pakten 1 here ne vit. Limitimi aksesit percaktohet sipas pozicionit te punes te cdo punonjesi te kompanise.
SO 11.2	c) Implemento politikë për mbrojtjen e aksesit në rrjet dhe sistemet e informacionit, duke adresuar rolet, të drejtat, përgjegjësitë dhe procedurat për vendosjen dhe revokimin e të drejtave të aksesit. d) Zgjidh mekanizma të duhur të autentikimit në varësi të tipit te aksesit	
	e) Monitoro aksesin në rrjet dhe sistemet e informacionit, vendos një process të miratimit të përjashtimeve dhe regjistrimit të thyerjeve të aksesit.	
SO 11.3	f) Vlerëso efektivitetin e politikave të kontrollit të aksesit dhe procedurave dhe implemento kontrolle në mekanizmat e kontrollit të aksesit. g) Politika dhe mekanizmat të kontrollit të aksesit rishikohen dhe kur nevojitet ndryshohen.	
SO 12: Integriteti i Rrjetit dhe Sistemeve te Informacionit		
SO 12.1	a) Siguro që programet e rrjetit dhe sistemet e informacionit nuk janë deformuar ose ndryshuar, duke përdorur kontrollin e inputeve dhe fireëall-et. b) Siguro që të dhënat kritike të sigurisë si passëord-ët, sekretet, celsat privatë, nuk bëhën publike dhe as ndryshohen. c) Kontrollo për programme të dëmshme në rrjet dhe sistemet e informacionit.	Sistem njoftimi automatik me e-mail nese ka tentativa brute-force ndaj sisteme te informacionit. Te gjithe sistemet jane te mbrojtuar me fireëall dhe jane te pa aksesueshme nga jashte zyrave. Sistemet e perdoruesave ne kompani jane te bllokuar kundrejt instalimit te programeve te paautorizuara. Kontroll periodik mujor per sistemet ne perdorim.
SO 12.2	d) Implemento masa sigurie sipas standarteve të industrisë, duke ofruar mbrojtje në thellësi ndaj modifikimit të sistemeve.	Sistemet operative dhe database behen upgrade mbi baza te rregullta 1 mujore si dhe kur ka nevoje per patche emergjente, te cilat permiresojne sistemet.
SO 12.3	e) Vendos kontrolle të mbrojtjes së integritetit të sistemeve. f) Vlerëso dhe rishiko efektivitetin e masave për të mbrojtur integritetin e sistemeve.	Kontroll periodik 1 javor mbi loget e gjeneruara nga sistemi Snapshot I perditshem i makinave virtuale, automatik.
D4: Menaxhimi i Operacioneve		
SO 13: Procedurat Operacionale		

SO 13.1	a) Vendos procedura operacionale dhe përgjegjësi për funksionimin e sistemeve kritike.	Procedure e brendshme ku departamenti HR percakton te drejtat e aksesit ne sistem per departamente dhe perdorues te ndryshem. Aksesi mundesohet vetem nga PC/IP te paracaktuara
SO 13.2	b) Implemento një politikë për funksionimin e sistemeve për të garantuar që sistemet kryesore funksionojnë dhe menaxhohen sipas procedurave të paracaktuara.	Si me siper Takime me drejtuesit e departamenteve ne baza te pakten 3 mujore per modifikimin rishikimin moduleve te ndryshme te sistemit.
SO 13.3	c) Rishiko dhe përditëso politikën/procedurat për funksionimin e sistemeve kritike, duke marrë në konsideratë incidentet dhe/ose ndryshimet.	
SO 14: Ndryshimi i Menaxhimit		
SO 14.1	a) Ndiqni procedurat e paracaktuara, kur bën ndryshime në sistemet kritike.	Ndryshimet e procedurave te sistemeve kritike behen sipas vendimeve te posacme.
SO 14.2	b) Zbatimi i politikave / procedurave për menaxhimin e ndryshimeve, për të siguruar që ndryshimet e sistemeve kritike janë bërë gjithmonë duke ndjekur një mënyrë të paracaktuar. c) procedurat e menaxhimit të ndryshimit te dokumentit, dhe rekordet për secilen ndryshojnë sipas hapave të procedurës së ndjekur. d) procedurat e menaxhimit të rishikimit dhe	Zbatimi i procedurave qe lidhen me sistemet kritike I nenshtrohen auditimit periodik Procedurat e ndryshme se bashku me ndryshimet ruhen ne databazen e informacionit te kompanise si dhe ne nje guide informative per punonjesit e rinj
SO 14.3	përditesimit ndryshojne rregullisht, duke marrë parasysh ndryshimet dhe incidentet e shkuara.	
SO 15: Menaxhimi i Burimeve		
SO 15.1	Menaxhimi i burimeve kritike dhe konfigurimi i sistemit kritik	Vendim mbi percaktimin e pajisjeve kritike ne rrjet, oraret e lejuara te nderhyrjeve dhe skema e autorizimit te personelit per nderhyrje.
SO 15.2	Implementimi i politikave / procedurave per menaxhimin e burimeve dhe kontrollin e konfigurimit.	Rregullore e brendshme e departamentit AARR (inventarizimi I pajisjeve aktive dhe pasive te rrjetit perfshire dhe burimet kritike). Ruajtje e versioneve te konfigurimeve, fotove, skemave autocad si dhe ndryshimeve ne konfigurim per nje periudhe 3 mujore
SO 15.3	Rishikimi dhe perditesimi i herepashershem te politikave te menaxhimit te burimeve , bazuar ne ndryshimet dhe incidentet e shkuara	
D5: Menaxhimi i Incidenteve		
SO 16: Procedurat e menaxhimit te incidenteve		
SO 16.1	a) Sigurimi qe personeli eshte ne gadishmeri dhe i pergatitur te menaxhoje dhe ti perballoje incidentet b) Te regjistroje incidentet kryesore	Trajnim dhe guide e shkruar per punonjesit mbi manaxhimin dhe trajnimin e incidenteve Regjistrimi i cdo incidenti ne sistemin e informacionit OTELLO

SO 16.2	c)Implementimi i politikave/procedurave per menaxhimin e incidenteve	Guide permbledhese per problematikat kryesore ne rrjet perfshin dhe incidentet e cila behet update vazhdimisht.
SO 16.3	d) Investigimi i incidenteve kryesore dhe raportimi i tyre final, duke perfshire veprime te ndermarra dhe rekomandime per te zvogeluar incidente te ngjashme	
	e) Vleresimi i politikave te menaxhimit te incidenteve / procedurave bazuar ne incidente te shkuara.	
SO 17: Procesi i zbulimit te incidenteve		
SO 17.1	a) Ngritja e proceseve apo sistemeve për zbulimin e incidentit.	Jane implementuar zgjidhje softëare qe bejne kontrolle rutine.
SO 17.2	b) Implementimi i sistemeve standarde të industrisë dhe procedurat për zbulimin e incidentit. c) Implementimi i sistemeve dhe procedurave për regjistrimin dhe përcjellja incidente ne kohë te njerëzit e duhur.	Jane impementuar disa softëare/scripte qe monitorojne automatikisht portat e ndryshme te rrjetit dhe raportojne anomali te ndryshme. Vazhdimisht behen kerkime per sisteme/softëare/zgjidhje te reja.
SO 17.3	d)Rishikimi i Sistemeve dhe procesit për zbulimin e incidentit rregullisht dhe përditësimin e tyre duke marrë parasysh ndryshimet dhe incidenteve të fundit	
SO 18: Raportimi i incidentit dhe komunkimi		
SO 18.1	a)Të komunikojnë dhe të raportojnë në lidhje të vazhdueshme ose incidente të fundit të palëve të treta, konsumatorët, dhe / ose autoritetet qeveritare, kur është e nevojshme.	Departamenti Kujdesi ndaj Klientit njofton grupe klientesh nese ka incidente qe mund te afektoje kete grup klientesh. Per cdo incident te mundshem merren masa qe te mos perseritet ne kliente te tjere (upgrade/zevendesim pajisjesh fundore etj)
SO 18.2	b) Implementon politika dhe procedura per komunikimin dhe raportimin ne lidhje me incidentet	
SO 18.3	c) Vlerësoni komunikimet e shkuara dhe raportimin në lidhje me incidentet. d) Rishikimi dhe përditësimin e planeve të raportimit dhe komunikimit, bazuar në ndryshimet apo incidenteve të fundit.	
D6: Menaxhimi i Vazhdimit te Biznesit		
SO 19: Strategjia e Vazhdimit të Shërbimit dhe Planet e Emergjencës		
SO 19.1	a) Implemento një strategjie ne vazhdimësinë e shërbimi për rrjetet e komunikimeve dhe / ose shërbimeve të ofruara.	Plan I detajuar per vazhdueshmerine e sherbimit me keto pika kryesore: Snapshote te perditshme te makinave kryesore virtuale. Ruajtje e te dhenave kritike ne cluster njekohesisht ne 2 datacenterat Rrjet unazor me disa ringje dhe linke te dubluara drejt providerve.
SO 19.2	a) Zbatimi plane rezervë për sistemet kritike. b) Aktivizimin i monitorimit dhe zbatimin e planeve të paparashikuara, regjistrimi herëve të suksesshme dhe të kohes se dështimit.	

SO 19.3	c) Rishikimi e sherbimeve strategjike ne menyre te vazhdueshme dhe periodikisht d) Rishikimin plane emergjence, bazuar në incidentet e fundit dhe ndryshimet.	Datacenter sekondar qe mundeson te gjitha sherbimet ne rast shkeputje totale te datacenterit primar
SO 20: Kapacitetet per rimekembjen nga katastrofat ne rrjet		
SO 20.1	a) Pergatitja per rikthimin ne gjendje normale e sherbimeve ne katastrofen e rradhes	Katastrofa ne rrjet eshte ngjarje me probabilitet 0. Te gjitha sistemet jane konfiguruar ne menyre redundante N+1. Per te gjitha pajisjet kryesore jane gati spare-parts.
SO 20.	b) Implementimi i proçedurave/policive per efektivitetin	



Sistemi ring Vlore – Dures -Lezhe – Shijak – Vlore siguron fizikisht privacine e rrjetit dhe njekohesisht backup per nderhyrje ne raste sigurie te demtimeve fizike

PREGATITUR NGA SHOQERIA ECHOSTAR shpk

NR. LICENCES VSh.1018/1

NR. LICENCES MK20696/2

NR. LICENCES N.6720/2

SHOQERI E LICENSUAR NE PROJEKTIM DHE SIGURINE E RRJETEVE INFORMATIKE DHE TELEKOMUNIKACION

NIPT : L56809205L

Ing. Altin KARALLI ING. KRISTAQ GJERGJI

Cel : 0682065849

E – Mail echostaralbania@gmail.com

№ 2502

Altin Karalli

Digitally signed by Altin Karalli
Date: 2021.01.08 06:16:38 +02'00'

REPUBLIKA E SHQIPËRISË
MINISTRIA E INFRASTRUKTURËS DHE ENERGJISË
Komisioni i Posaçëm i Dhënies së Licencave Profesionale në Fushën e Studimit e Projektimit dhe Mbikëqyrje e Kolaudimit të Punimeve të Ndërtimit

LICENCË
N.6720/2

SHOQËRIA:	**" E C H O S T A R "**
DREJTUES LIGJOR:	**ALTIN KARALLI**
DREJTUES TEKNIK:	**ALTIN KARALLI, LEONORA DUPI, DORIANA BEHARI, TOLJON MIHALAJ, KRISTAQ GJERGJI (PROFI), VIRGJIL GRILLO, MIMOZA GRILLO, PELIVAN MUSKAJ**
ADRESA:	**VLORË**
Regjistruar në Regjistrin profesional që nga data:	**29.12.2020**

NE PROJEKTIM

Kat.	1	c	Plane të detajuara vendore.
Kat.	2	a	Projektim arkitekturor për objekte banimi – objekte industriale – objekte turistike.
		c	Projektim interiere.
		d	Projektim peizazhi, sistemim sipërfaqe të gjelbërta, lulishte e parqe.
Kat.	3	a	Projektim objekte civile – industriale – turistike prej murature e skelet beton arme deri në 5 kate.
		b	Projektim: 1. Objekte civile – industriale – turistike mbi 5 kate – 2. objekte me skelet metalik.
		c	Projektim: 1. Objekte me shkallë të lartë vështirësie Beton-arme – metalike – 2. troje dhe shpate me qëndrueshmëri të ulët.
Kat.	4	a	Projektim të instalimeve hidro-termosanitare.
		b	Projektim të instalimeve termoteknike – kondicionimi, si dhe të impianteve të prodhimit të energjisë termike nga burime të rinovueshme.
		c	Projektim të linjave e rrjeteve elektrike, për objekte civile e industriale.
		d	Projektim të sistemeve komplekse të telekomunikacionit.
		e	Projektim të sistemeve të furnizimit me gaz.
		f	Projektim të sistemeve kundra zjarrit.
		j	Projektim të rrjeteve të telefonisë, citofonisë, fonisë, internetit, TV, access kontroll, CCTV, sistemet e alarmit, sistemet e dedektimit të zjarrit, etj., për objektet civile e industriale.
Kat.	5	b	Projektim furnizim me ujë – kolektorë shkarkimi.
		c	Projektim ujësjellës kanalizime urbane – rurale.
		d	Projektim vepra ujitje – kullimi – impiante vaditëse – diga të vogla (ato që nuk plotësojnë kushtin e digave të mëdha) – damba, sifona, kaskada, kapërderdhëse, rryméshpejtues, priza, baraze, porta, tombino.
		g	Projektim vepra naftësjellës – gazsjellës – vajsjellës etj.
Kat.	6	a	Projektim rrugë lokale, rrugë urbane dytësore dhe rrugë interurbane dytësore.
		b	Projektim rrugë urbane kryesore dhe rrugë interurbane kryesore.
		d	Projektim aeroporte – heliporte – hidroporte.
Kat.	7	a	Projektim ura dhe vepra arti të vogla deri 10 m.
		b	Projektim ura dhe vepra arti mbi 10 m.
		c	Projektim ura/viadukte me hapësira të mëdha drite, ura të varura, ura me sisteme të pacaktuar statikisht dhe sisteme të tjera speciale.
		d	Projektim ura metalike.
Kat.	8	a	Rilevime inxhinierike.
		b	Rilevime inxhinierike kadastrale.
		c	Sisteme GIS.
		d	Bazamente gjeodezike.
Kat.	10	c	Projektim impiante të prodhimit të energjisë elektrike të rinovueshme, diellore, era, etj.
		d	Projektim nënstacione elektrikë, primar sekondar – linja të tensionit të lartë.
		e	Projektim kabina elektrike të rrjetit shpërndarës – linja të tensionit të ulët – të mesëm.
Kat.	11	a	Projektim sinjalistikë jondriguese në rrugë lokale, rrugë urbane dytësore, rrugë interurbane dytësore, sheshe e parkime.
		b	Projektim sinjalistikë jondriguese në autostrada, rrugë urbane kryesore dhe rrugë interurbane kryesore dhe në degëzime me hekurudhën.
		c	Projektim sinjalistikë jondriguese në aeroporte dhe heliporte.

KRYETARI I KOMISIONIT

GERTA LUBONJA

Shënim: Kjo licencë është e vlefshme deri më datën 29.09.2023.

REPUBLIKA E SHQIPËRISË MINISTRIA E INFRASTRUKTURËS DHE ENERGJISË TIRANË

Altin Karalli

Digitally signed by Altin Karalli
Date: 2021.02.25 08:23:35 +02'00'

REPUBLIKA E SHQIPËRISË

MINISTRIA E FINANCAVE DHE EKONOMISË
QENDRA KOMBËTARE E BIZNESIT

EKSTRAKT I REGJISTRIT TREGTAR PËR TË DHËNAT E SUBJEKTIT " SHOQËRI ME PËRGJEGJËSI TË KUFIZUAR"

GJENDJA E REGJISTRIMIT

1. Numri unik i identifikimit te subjektit (NUIS)	L56809205L
2. Data e Regjistrimit	09/06/2015
3. Emri i Subjektit	ECHOSTAR
4. Forma ligjore	SHPK
5. Data e themelimit	01/06/2015
6. Kohëzgjatja	Nga: 01/06/201531/05/2025
7. Zyra qendrore e shoqërisë në Shqipëri	Vlore Vlore VLORE Lagjja 29 Nëntori, Rruga Ismail Qemali, Pallati Nr.544, Kati 3
8. Kapitali	10.000,00
8.1 Numri i përgjithshëm i kuotave	1,00
9. Objekti i aktivitetit	Per punime dhe per vleresim, kolaudim, projektim embikqyrje punimesh per aktivitete e poshte shenuara: Ndertime civile dhe industriale rikonstruksion dhe mirembajtje godinash civile dhe industriale, veshje te fasadave, rruge , autostrada, ura, mbikalime, hekurudha , linja tramvaji , metro hekurudhore me kavo dhe pista aeroportuale, punime nentokesore , ure e vepra arti, diga dhe tunele hidroteknike, ujesjellesa, gazesjellesa, vepra kullimi e vaditje , ndertime detare dhe punime thellimi ne uje, punime dhe mbrojtje lumore , sisteme hidraulike dhe bonifikime , ndertimi i impianteve per prodhimin e enegjise elektrike, ndertime per nen/stacionet, kabinat e transformatoreve , linja TN te mesem dhe shperndarjen e energjise, punime te inxhinierise se mjedisit, punime per prishjen e ndertimeve , impiante hdrosanitare, kuzhina, lavanderi, mirembajtja e tyre.Impiante ngritese dhe transportues(ashensore, shkalle levizese, trasportues), punime rifiniture te muratures dhe te lidhura me to, rifiniture me materiale druri , plastik, metalik dhe xhami dhe rifiniture te natyres teknike ndertuese,

	impiante te sinjalistikes ndriçuese te trafikut, sinjalistika rrugore jo ndriçuese, barriera dhe mbrojtje rrugore, ndertime parafabrikat beton arme, struktura metalike dhe druri, punime strukturore speciale, shtresa dhe mbistruktura speciale, punime mbi shina dhe traversa.Impiante teknologjike, termike dhe te kondicionimit, impiante dhe linja telefonie, rrjete kabllore me fibra optike per telekomunikacion, impiante te brendshme , elektrike, telefoni, radiotelefoni, TV etj, pastrimi i ujrave detare , liqenore dhe lumore , ndertimi i impianteve te ujit te pijshem dhe te pastrimit te tij, ndertimi i impianteve te grumbullimit dhe trajtimit te mbetjeve urbane.Punime topogjeodezike , sistemet kundra zhurmes per infrastrukture, shpime gjeologo-inxhinierike, puse e shpime per uje, vleresim i pasurive te paluajtshme dhe konsulencene tregun e shit-blerjeve te pronave.Aktivitet ne fushen e tregtise:tregtimi me shumice dhe pakice i artikujve te ndryshme industriale , materialeve te ndertimit , artikuj te perzier, artikuj ushqimore, elektrike dhe elektroshtepiake, artikujve informatike dhe te telekomunikacionit, pajisje zyrash , import-eksporti i tyre	
10. Administratori/ët	Altin Karalli	
10.1 Afati i emërimit	Nga: 01/06/2015	Deri: 31/05/2020
11. Procedura e emërimit nëse ndryshon nga parashikimet ligjore		
11.1 Kufizimet e kompetencave (nëse ka)		
12. Ortakët	AltinKaralli	
12.1 Vlera e kapitalit	Para: 10.000,00	Natyre:
12.2 Numri i pjesëve	1,00	
12.3 Pjesëmarrja në përqindje (%)	100,00	
**Të përfaqësuarit, (Plotësohet vetëm nëse një kuotë zotërohet në bashkëpronësi)*		
12.4 Komente (nëse ka)		
13. Vende të tjera të ushtrimit të aktivitetit		
14. Të dhëna që njoftohen vullnetarisht	Emri Tregtar: ECHOSTAR E-Mail: echostar.shpk@gmail.com Telefon: 0682065849	

REPUBLIKA E SHQIPËRISË

MINISTRIA E FINANCAVE DHE EKONOMISË
QENDRA KOMBËTARE E BIZNESIT

15. Statusi:	Aktiv

Datë: 25/02/2021

Emri, Mbiemri, Nënshkrimi
(i nëpunësit të sportelit)