# Drejtuar: Autoritetit të Komunikimeve Elektronike dhe Postare

# Operatori: Ervis Cina (person fizik)

## Të nderuar,

Kjo është Politika për "Sigurinë dhe/ose integritetin e shërbimeve dhe rrjeteve".

Kjo Politikë ka si objekt përcaktimin e masave teknike dhe organizative për Sigurinë dhe Integritetin e rrjeteve në kompani si ofrues të shërbimit të internetit.

Nëpërmjet Politikës së Sigurisë synohet të realizohet mbrojtja e informacionit të abonenteve dhe mbrojtja e aseteve të kompanisë (mbrojtja e rrjetit, e pajisjeve hardware dhe software, burimeve njerëzore si dhe cdo shërbim tjetër i ofruar nga ne).

Gjatë hartimit të saj kemi zbatuar Rregulloren nr 37 datë 29.10.2015 "Mbi masat teknike dhe organizative për të garantuar sigurinë dhe integritetin e rrjeteve dhe/ ose të shërbimeve të komunikimeve dhe/ose të shërbimeve elektonike në AKEP"si dhe në përputhje me Aneksin nr1, 2, 3 të kësaj Rregulloreje.

Ju faleminderit!

Ervis Cina

# Politika mbi sigurinë dhe integritetin e rrjetit në ofrimin e shërbimit internet

## 1.Qeverisja dhe Menaxhimi i Riskut.

Informacioni, sistemet dhe rrjetet janë asete të rëndësishme të kompanisë dhe janë të mbrojtur nga një nivel i lartë sigurie.

### 1.1.Politikat e sigurisë së informacionit

Për të realizuar mbrojtjen e informacionit nga kërcënimet e jashtme kemi hartuar **"Politikën e Sigurisë"** që njihet jo vetëm nga personi përgjegjës për incidentet e sigurisë por njihet edhe nga punonjësit e kompanisë. Punonjësit e kompanisë sonë e mbajnë të printuar politikën e sigurisë përgjatë orarit të punës dhe e zbatojnë atë me përikmëri.

Informacioni gjithmonë duhet të transmetohet në mënyrë të sigurt. Një infromacion i sigurt për ne arrihet duke zbatuar nje sërë rregullash dhe procedurash për të gjithë punonjësit.

Cdo punonjës i kompanisë tonë mban përgjegjësi të plotë për informacionet të cilat arrin të aksesojë si edhe duhet të mundësojë uljen e rrezikut ndaj sulmeve të jashtme që sjellin dëmtime. Në kompani është është asolutisht e NDALUAR që cdo person i punësuar me kontratë të rregullt pune, të nxjerrë jashtë saj informacione konfidendale që mund të aksesojë në vendin e tij të punës. Gjithashtu ka nje hierarki të mirëfunksionuar të kalimit të informacionit brënda kompanis. Realizojmë azhornimin e sistemeve dhe ndryshimin e herëpashershëm të pasëordeve.

Cdo informacion që kalon në rrjetin e kompanisë sonë është i kontrolluar. Kontrolli i aksesit realizohet në të gjitha hallkat e sistemit dhe vetëm nga persona të autorizuar.

Sipërmarrësi Ervis Cina ka realizuar mbylljen e të gjitha faqeve të paligjshme të kërkuara nga autoriteti i AKEP. Ka marrë masa për bllokimin e komunkimeve të paligjshme dhe që cënojnë të drejtat e autorit.

### 1.2.Qeverisja dhe menaxhimi i riskut

Cdo punonjës në kompani në momentin që gjatë punës konstaton një incident sigurie duhet ta regjistrojë dhe raportojë menjëherë te përgjegjësi i tij.

Disa prej llojeve të incidenteve janë:

1. Ndërprerja e shërbimit
2. Cilësia e shërbimit jo e mirë
3. Thyerja e sigurisë nga neglizhenca.

4. Dëmtimi i hardëare ose softare
5. Gabimet njerëzore etj.

Personi përgjegjës i ngarkuar me detyrën për të parandaluar incidentet dhe risqet e sigurisë është vetë personi fizik z. Ervis Cina, i cili njëkohësisht është edhe inxhinieri elektronik i biznesit.

### 1.3.Rolet e sigurisë dhe përgjegjësitë

Personi përgjegjës kujdeset që të realizojë të gjitha masat e sigurisë. Detyrat që ai zbaton janë:

6. Identifikon incidentin e sigurisë ose riskun që ai ka për të ndodhur.
7. Parashikon propabilitetin sesa i dëmshëm mund të jete incidenti i sigurisë.
8. Raporton riskun\ incidentin e sigurisë te punonjesit e tjerë të kompanise.
9. Njofton punonjësit nga kërcënimet që mund të ndodhin.
10. Bën vlerësimin e riskut dhe periudhën kohore të përsëritjes së këtij risku.
11. Bën vendosjen nën kontroll\minimizimin\ eleminimin e riskut
12. Ndërmerr të gjitha masat për ta parandaluar.

**Tabela e Inventarit te Riskut**

| **Nr. i riskut** | **Emertimi i riskut** | | **Plani \ Veprimet \ Trajtimi** | | | | |
|---|---|---|---|---|---|---|---|
| Nr. | Mbrojtja e të dhënave personale | Veprimi identifikues | Operacionet | Trajtimi | Verimet | Përgjegjësi | Data e konstatimit |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Ne si kompani e rishikojme njeherë në vitë Politikën e sigurisë në mënyrë periodike dhe marrim në konsideratë incidentet e mëparshme që kanë ndodhur të cilët mund të kenë perkur edhe ofruesit e tjerë të shpërndarjes së shërbimit internet, pra në të njëjtin sektor.

Në bazë të incidenteve të sigurisë që ndodhin ne ndryshojmë Politikën e Sigurisë dhe këtë informacion ia vendosim në dispozicion personelit.

### 1.4.Siguria e aseteve të pales së tretë.

Në kontratën që kemi nënshkruar me Operatorin që na furnizon me internet kemi të parashikuar detyrimin të na njoftojë nqs në rrjetin e tij vihen re incidente sigurie.

Të gjithë abonetët e kompanisë kanë nënshkruar kontatën dypalëshe ku parashikohet mbrojtja e të dhënave personale në një aneks të vecantë. Abonentët sigurohen se të dhënat e tyre personale janë ruajtur në mënyrë kofidenciale dhe nuk bëhen objekt sulmi ose vjedhje nga palë të treta të cilat janë jashtë kompanisë.

## 2.Siguria e Burimeve Njerëzore

### 2.1 Kontrollet e backgrund-it.

Për kompaninë tonë është e rëndësishme që puna e kryer nga punonjësit të jetë sa më efikase, për këtë arsye për përzgjedhjen e tyre kemi vendosur disa kritere. Ky kontroll konsiston në përzgjedhjen e tyre nëpërmjet CV, eksperiencës së punës dhe nivelit të arsimit.

### 2.2 Njohuria mbi sigurinë dhe trajnimin

Për të pasur një performancë sa më të mirë cdo punonjësi të ri i bëhet një trajnim i detajuar sipas pozisionit që do të ketë në kompani në bazë të një programi të përditësuar . Këtu punonjësi njihet me përgjegjesitë në lidhje me konfidencialitetin e informacionit apo cështjeve të tjera të një rëndësie të lartë. Në fund realizohet një test për të kontrolluar njohuritë që ai ka marrë gjatë trajnimit.

### 2.3 Ndryshimi i personelit

Kur kemi ndryshime të pozicioneve të personelit në kompani këtij të fundit i hiqet aksesi dhe të drejtat që ka pasur në pajisjet dhe sistemet e mëparshme. Punonjësit që ka ndryshuar pozicionin i vendosen në dispozicion sistemet me kredenciale të reja (user name dhe passëord) dhe mjetet e duhura për të realizuar procesin e punës.

### 2.4 Trajtimi i shkeljeve.

Disa nga detyrimet e punonjësve për ruajtjen e konfidencialitetit janë:

1. Mospërdorimi i informacioneve të kompanisë për interesa të palëve të treta.
2. Punonjësve nuk u lejohet të kopjojnë apo shesin informacionin që gjendet brenda në kompani gjatë mardhënies së punës apo edhe pas përfundimit të saj.
3. Cdo informacion që trajtohet brenda në kompani është pronë e kompanisë.

Punonjësi duhet të dorëzojë cdo asset të kompanisë në përfundim të marredhënies së punës.

Në rastet kur thyhen masat e sigurisë kundrejt punonjësve merren masa disiplinore, si heqja e ditëve të punës. Gjithmonë masat merren në varësi të shkeljes së rregullave dhe varijojnë:

1. Vënia në dijeni për shkeljen e kryer dhe ditët e punës që mund të hiqen.
2. Paralajmërim për ndërprerje të ditës së punës
3. Ndërprerje të mardhënieve të punës
4. Padi penale në rastete e shkeljeve të rënda, ose mase administrative referuar kodit të punës, te tilla si shkelje të informacionit konfidencial të kompanisë, të shkatërrimit të pajisjeve apo keqpërdorim të informacionit, etj.

Këto masa disiplinore jane parashikuar edhe ne kontraten individuale te punes.

## 3.Siguria e Sistemeve dhe Pajisjeve

Të gjitha pajisjet e kompanisë mbrohen fizikisht nga kërcënimet e sigurisë dhe nga rreziqet e mjedisit.

### 3.1Siguria fizike dhe e mjedisit

Në zonat fizike të siguruara do të përfshihen godina e komanisë, server room, rrjeti fizik kabllor i brendshëm dhe i jashtëm. Të ndërtuar në përputhje me standartet e sigurisë dhe rregullave të urbanistikës. Janë të instaluar kamerat e sigurisë, sistemi i alarmit dhe paisjet e zjarrit të cilat funksionojnë 24 orë.
Aksesimi i të gjitha ambienteve të sistemeve të informacionit në kompani do të kontrollohet rreptësisht dhe në çdo kohë, në mënyrë që të parandalohen humbjet ose kompromentimet e aseteve të informacionit dhe të aseteve të tjera.

Vizitorëve të kompanisë nuk duhet t'u lejohet lëvizja e lirë, e pakontrolluar në ambient.
Vizitorët, punonjësit e mirëmbajtjes dhe persona të tjerë të huaj, duhet të shoqërohen gjatë gjithë

kohës nga punonjës të autorizuar nga kompania. Në veçanti, vizitorëve nuk duhet t'u lejohet të aksesojnë ambientet me akses të kufizuar, sidomos në vendndodhjet e serverave, të pashoqëruar nga një person i autorizuar.

**3.2Siguria e burimeve.**

Mjetet dhe asetet që garantojnë sigurinë dhe vazhdimësinë e punës së përditshme do të quhen burime të kompanisë. Si burime të tilla do të përmendim:
-Gjeneratorin i cili ndizet automatikisht,
-Kondicionerët të cilët realizojnë ftohjen e pajisjeve në server room.
-Ristartimi automatic i pajisjeve në rastin e ndërprerjes së energjisë eleketrike.
- Bateri dhe inverterat që mbajnë në punë pajisjet.

Këto burime janë në gjendje pune 24 orë në 24.

**3.3Kontrolli i aksesit në rrjet dhe sistemet e informacionit.**

Rrjeti i kompaisë sonë është i ndarë në disa segmente duke u bazuar edhe në mënyrën se si janë të vendosur abonentët e cdo zonë. Lidhja midis pjesëve të brendshme të rrjetit dhe lidhja me rrjetet e tjera kontrollohet nëpërmjet fireëall.

Cdo informacion që kalon në rrjetin e kompanisë sonë është i kontrolluar. Kontrolli i aksesit realizohet në të gjitha hallkat e sistemit dhe vetëm nga persona të autorizuar. Më poshtë po rendisim rregullat nëpërmjet të cilave ne punojmë për të pasur akses në rrjet.

**Rregullat për aksesin:**

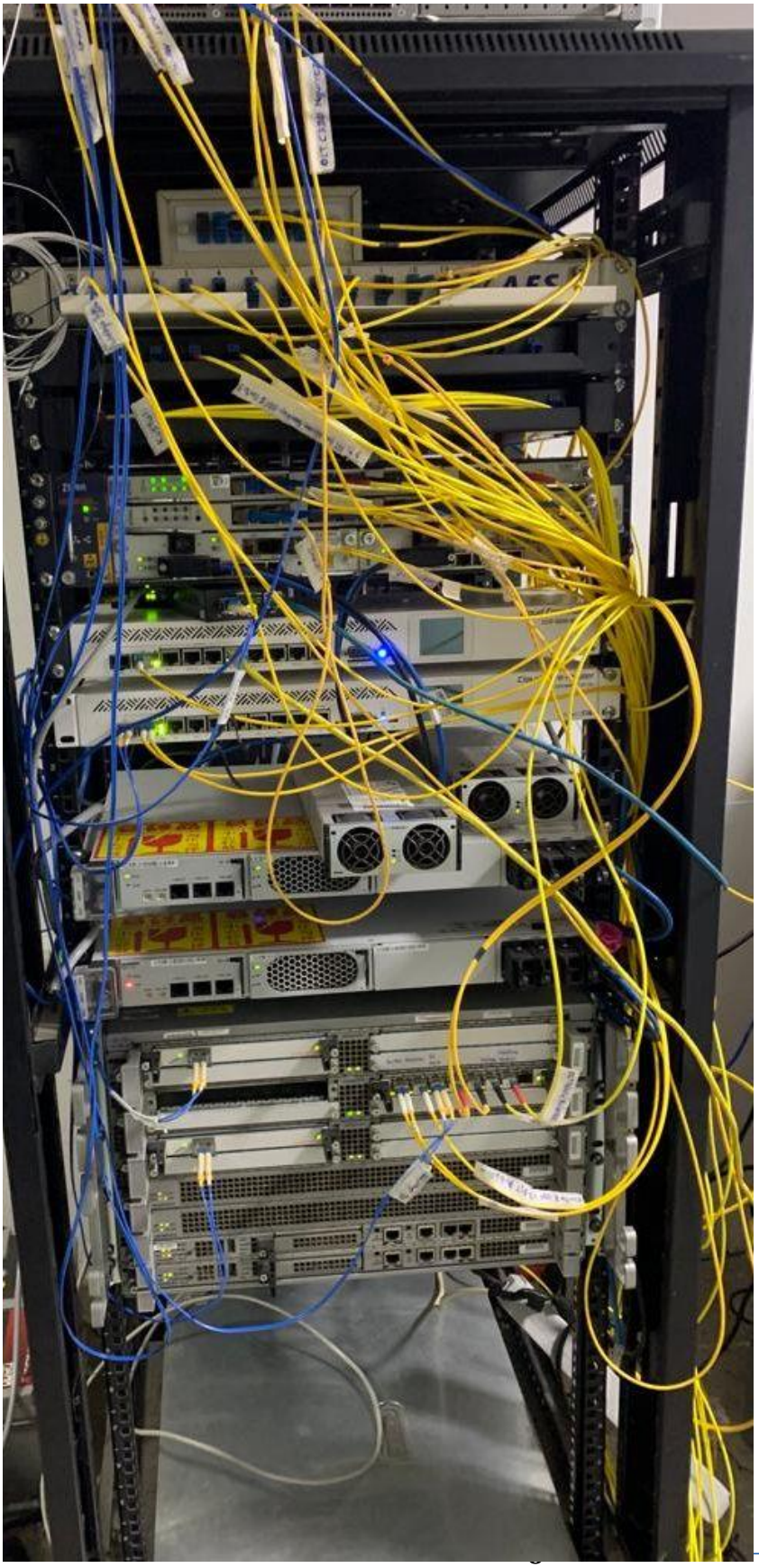
1. Aksesi në informacion bëhet vetëm nga personi përgjegjës i kompanisë ose kur institucionet e ngarkuara me ligj e kërkojnë këtë gjë.
2. Të gjithë punonjësit e kompanisë kanë të drejtën të aksesojnë mbi të dhënat dhe pajisjet për aq sa i duhet në punën e tyre.
3. Për të rritur sigurinë e paisjeve të sistemit tonë të dhënat e llagarisë së përdoruesve username dhe passëord ndryshohen cdo një herë në muaj.
4. Për privilegjet që u jepen përdorueseve ato caktohen drejtperdrejt nga administratori.
5. Për rritjen e nivelit të sigurisë përdoren fjalekalime me shkallë të lartë vështirësie duke futur karaktere të ndryshme dhe jo më pak se 8 të tilla.
6. Në rastin kur dikush largohet nga kompania automatikisht i hiqen të gjithë privilegjet dhe mundesitë e aksesit.

Aksesi në rrjetin tone bëhet vetëm sipas rregullave që kemi vendosur për kontrollin e aksesit.

Foto të pajisjeve:

# Politika mbi sigurinë dhe integritetin e rrjetit në ofrimin e shërbimit internet

# Politika mbi sigurinë dhe integritetin e rrjetit në ofrimin e shërbimit internet



### 3.4.Integriteti i rrjetit dhe sistemeve të informacionit.

Për sigurinë e rrjetit ne kemi instaluar:

1. **Cisco ASR 1000, qëndron për Router Shërbimet e Agregimit**. Ruterin në këtë seri e përdorim kryesisht për routime fundore. Ai është ideal për aplikime me gjerësi bande të lartë, të tilla si transmetimi i audios ose videos, ose video konferenca.
   Performanca kryesore e kriptimit, shërbimet e shtresezuara të sigurisë dhe një dizajn rezistent ndaj manipulimit ndihmojnë Cisco ASR 1000 të zvogëlojë sulmet dhe të sigurojë trafikun.

**2.Sistemin fireëall,** i cili përbëhet nga routeri microtik dhe shërben mbrojtjen e rrjetit nga aksesi i jashtëm i paautorizuar.

**3.Routera microtik** të cilët janë të dubluar për garantimin e uptime –it në rast të dështimit të njërit prej tyre.

**4.Sistemin database** i realizuar me kopjutera me sistem operativ ëindoës dhe rrjetin e kompjuterave të brendshëm për menaxhimin e sistemeve me kompjutera me system operativ ëindoës**.**

**5.Dublimin e rrjetit të aksesit,** duke marrë dy linja me fibër optike në rrugë të ndryshme fizike të cilat lidhen me Albtelecomin për garantimin e uptime –it të linjës hyrëse.

Linja kryesore që sjell internetin në kompaninë tonë është me fiber optike të dubluar. Abonentët janë të menaxhueshëm nga një database i cili përbëhet nga një server fizik në të cilin është instaluar system operativ linux mbi të cilin është instaluar database radius. Ky server e ka totalisht të bllokuar aksesin nga jashtë, mund të aksesohet vetëm nga LAN i brendshëm nëpërmjet një kompjuteri që ndodhet në server room. Nëpërmjet kësaj skeme realizohet edhe mbrojtja nga aksesi i paautorizuar.

1. Në rastet e ndërprerjes së energjise elektrike për të garantuar vazhdimesinë e punës së pajisjeve në server room ne kemi në gjendje gadishmërie gjeneratorin elektrik dhe inverterat të cilët hyjnë në punë menjëherë pas ndërprerjes së energjisë.
2. Kur është nevoja aktivizohet edhe sistemi I ftohjes I cili garanton punimin ne performance maksimale te gjithe pasijeve.

Për sigurinë e rrjetit ne kemi instaluar disa paisje dhe programe të cilat mbrojnë sistemin nga ndërhyrjet e paautorizuara jashte rrjetit. Në kompjutera kemi të instaluar systemin operativ ëindoës dhe antivirus Avast. Mbrojtja e sistemit përbëhet nga fireëall microtik i cili ka rulle per bllokimin e sulmeve që mund të vijnë nga jashtë si psh DDOS dhe shmangia e keqpërdorimit të DNS duke e bllokuar aksesin nga jashtë dhe duke bërë rrjetin në anën e brendshme të sigurtë nga sulmet e jashtme. Kjo skemë realizohet nëpërmjet ruterave, serverave dhe mbrojtjes me username passëord në pajisjet fundore.

# 4.Menaxhimi i Operacioneve

## 4.1.Proceduart operacionale

Shpërndarja e internetit realizohet nëpërrmjet fibrës optike duke avantazhuar up time-t e rrjetit dhe performancën në total të internetit kundrejt abonentëve. Klientët lidhen të gjithë në router me autentikim PPPOE nëpërmjët një server autentikimi në rastin tonë Radius. Rrjeti është i ndarë në disa Vlan për arsye segmentimi të rrjetit për zona të ndryshme. Si lloje të Vlan-ve mund të përmendim: Vlan e menaxhimit, Vlan e abonentëve etj. Ndarja e rrjetit në Vlan ndihmon në mbrojtjen e të dhënave dhe menaxhimin e mirë të tyre.

Të dhënat mbrohen në një server database i cili është i aksesueshëm vetëm nga personeli i autorizuar, i mbrojtur nga disa nivele passëordesh dhe izoluar totalisht nga aksesi i jashtëm. Aksesimi i këtij sistemi database është bërë i aksesueshëm nga brenda rrjetit nga një kompjuter i cili në vetëve është i mbrojtur me username dhe passëord duke e bërë të pamundur hakerimin e këtyre serverave.

Vetëm pajisjet e autorizuara mund të lidhen me rrjetin e kompanisë. Pajisje të autorizuara përfshijnë PC dhe pajisje në pronësi të abonentit të cilat përputhen me udhëzimet e konfigurimit të kompanisë. Pajisje të tjera të autorizuara përfshijnë paisjet e infrastruktures së rrjetit të përdorura për menaxhimin e rrjetit dhe monitorimin. Abonenti nuk duhet të lidhë në rrjet paisje që nuk janë të autorizuara.

Asetet e informacionit në kompani janë të përbëra nga:
-kompjuter hardëere, server
-hardëere dhe softëere duke përfshirë fireëalls, fibër optic, sëitch optic, media converter optic dhe sfp.

## 4.2.Nryshimi i menaxhimit

Proceduarat që do të ndiqen për të realizuar ndryshimet në sisteme janë :

1.Sistemi i ri vendoset në punë për një periudhë testi 1-3 muaj.
2. Konkludohet që sistemi punon në rregull dhe nuk kemi dështime
3.Konkludohet që është rritur cilësia dhe performance e rrjetit.
4.Realizojmë implementimin e sistemit te ri në rrjet.
5. Pajisjet e mëparshme ose sistemet e mëparshme do vazhdojnë të mbahen në gjendje active back-up.

## 4.3Menaxhimi i burimeve

Për sigurinë e rrjetit ne kemi instaluar disa paisje dhe programe të cilat mbrojnë sistemin nga ndërhyrjet e paautorizuara jashte rrjetit. Në kompjutera kemi të instaluar systemin operativ ëindoës dhe antivirus Avast. Mbrojtja e sistemit përbëhet nga fireëall microtik i cili ka rulle per bllokimin e sulmeve që mund të vijnë nga jashtë si psh DDOS dhe shmangia e keqpërdorimit të DNS duke e bllokuar aksesin nga jashtë dhe duke bërë rrjetin në anën e brendshme të sigurtë nga sulmet e jashtme. Kjo skemë realizohet nëpërmjet ruterave, serverave dhe mbrojtjes me username passëord në pajisjet fundore.

## 5.Menaxhimi i Incidenteve

### 5.1. Procedurat e menxhimit te incidenteve

Cdo punonjës në kompani zbaton hapat e mëposhtëm për menaxhimin e një incidenti:

1. Raporton te personi përgjegjës.
2. Regjistron incidentin në aneksin e incidenteve.
3. Merren masa per izolimin dhe rekuperimin e incidenteve.
4. Merren masa ndaj shkakut të ndodhjes së incidentit.

Në varësi të llojit të incidentit përcaktohet edhe shkalla e tij nëse është e lehtë, mesatare, apo e rëndë. Për ne incidentet më të rëndësishme do të konsiderohen ata që lidhen me cënueshmërinë e sigurisë së informacionit.

### 5.2. Procesi i zbulimit të incidenteve.

**Monitorimi i incidenteve kryhet nga personi përgjegjës i kompanisë, ky i fundit monitoron disa gjendje të sistemit:**

1. Funksionimi i sistemeve.
2. Rëniet e rrjetit në mënyrë të paparalajmëruar.
3. Sulmet që i bëhen sistemit nga jashtë.
4. Monitoron aksesin e pakontrolluar në rrjet

### 5.3. Raportimi i incidentit dhe komunikimi

Pasi janë marrë masat për eleminimin e icidentit personi përgjegjës harton një gjendje të ndodhjes së këtij incidenti (Raport) dhe ndërmerr hapa për të përmirësuar sistemet, pajisjet, kanfigurimet etj.

Disa nga hapat që ai ndërmerr janë:

1. Analizon me detaje incidentin që ka ndodhur.

2. Identifikon shkakun e incidentit.
3. Izolon problemin që mund ta ketë shkaktuaur në mënyrë që ai të mos ndodhë më.
4. Parashikon masa që ky lloj icidenti të mos ndodhë më.

**Veprimet e rikuperimit janë të përshkruara në tabelën e mëposhtme:**

| Niveli i prioritetit | Përshkrimi i sistemit | Koha e përgjigjes |
|---|---|---|
| Kritike | -Rënia e të gjithë sistemeve<br>-një pjesë kritike e sistemit nuk funksionon<br>-humbja e të dhënave sensitive të kompanisë | 0 – 6 orë |
| I lartë | -Disa pjesë të rëndësishme të sitemit nuk funksionojnë<br>- aksesi në sisteme është i pjesshëm | 7-14 orë |
| Mesatar | Nje pjesë e vogël e sistemeve nuk funksionon brenda standarteve | 15-24 orë |
| I Ulët | Probleme minimale që nuk ndikojnë në fuksionimin e punës | 24-72 orë |

**Masat për eleminimin e incidenteve.**

1. Cdo incident vleresohet nga shkalla e vështirësisë së tij.
2. Pasi janë gjetur portat hyrëse në sistem në bazë të logeve bëhet mbyllja e tyre.
3. Aktivizojmë linjën e back up dhe rimbyllim portat.
4. Ringremë fireëall-in e microtikut pas rikonfigurimeve.
5. Ky incident mbahet shënim dhe trajnohen punonjësit për të mos u përsëritur më.

## 6.Menaxhimi i vazhdimit te biznesit

### 6.1. Strategjia e vazhdimit te sherbimit dhe planet e emrgjences.

Kompania jonë për të siguruar vazhdimësinë e punës së sistemeve ka ngritur sistemet e backup-it:

1. Në rastin e fireëall kemi një mikrotik të dytë në gjendje gadishmerie i cili rri i ndezur dhe realizon azhornimet e të gjitha ruleve që bëhen edhe në fireëall-in kryesor.
2. Routerat të cilët i shpërndajnë internetin abonenteve janë gjithashtu të dublikuar dhe azhornohen në kohë reale me të gjitha ndryshimet.
3. Radiusi i cili mban abonentët është gjithashtu i dublikuar për pjesën e sistemeve kopjuterike. Të dhënat ruhen në kompjuter dhe në një server i cili është standalone vetëm për ruajtjen të dhënave në rast të dështimit të sistemeve kompjuterike. Të dhënat rikuperohen automatikisht nga serveri duke siguruar në këtë mënyrë vazhdueshmërinë e punës së sistemeve pa shkëputje.
4. Në rastet e ndërprerjes së energjise elektrike për të garantuar vazhdimesinë e punës së pajisjeve në server room ne kemi në gjendje gadishmërie gjeneratorin elektrik dhe inverterat të cilët hyjnë në punë menjëherë pas ndërprerjes së energjisë.
5. Kur është nevoja aktivizohet edhe sistemi I ftohjes I cili garanton punimin ne performance maksimale te gjithe pasijeve.

## 6.2Kapacitetet për rimëkëmbjet nga katastofat në rrjet.

Në këtë seksion trajtohet politika dhe procedurat për vazhdimësinë e punës në
rastin e ndodhjes së një incidenti sigurie.

Kompania jonë në rast se do të ndodhet në kushtet e një incidenti të sigurisë ka krijuar një plan emergjence dhe një strategji për të mos ndërprerë shërbimin e internetit. Kështu për vazhdimin e punës në rast të ndonjë situate të jashtzakonshme ne kemi siguruar linja back up (rezervë), pajisje të dubluara të tilla si router, sëitch-a, lidhje me fibër optike back up me sitin kryesor dhe lidhje e dubluar interneti me operatorin e furnizimit me internet.
Kjo mundëson një up time afërsisht 100% duke garantuar vazhdimësinë e furnizimit me internet te abonentët dhe njëkohësisht vazhdimësinë e biznesit.

Gjithashtu punonjësit do të jenë në dispozicion kundrejt pagesave shtesë. Në rastet kur është e nevojshme kopania do të marreë konsulent të specializuar kundrejt pagesës.
Në raste incidenti apo kryerje punimesh të gjithë përdoruesit do njoftohen nëpërmjet telefonit, rrjeteve sociale apo mailbox-it.

## 7.Monitorimi, auditimi dhe testimi.

### 7.1. Politikat e Logeve dhe monitorimit.

Ne si kompani rujmë të gjitha loget e gjeneruara të sistemit. Loget na japin një informacion të detajuar të aktivitetit mbi pajisjet, sistemet, shërbimet dhe gjithë rrjetit tonë.
Loget e aplikacioneve idetifikojnë veprimet e kryera në to, kohën e kryerjes dhe qëllimin prej logeve të regjistruara.

Nëpërmjet ruajtjes së logove përfitohet informacion i rëndësishëm për sigurinë, performancën dhe menaxhimin e burimeve të ndryshme të sistemeve.
Personi përgjegjës ka detyrimin të bëjë ruajtjen dhe menaxhimin e logeve.
Nga informacioni që na sigurojnë loget ne arrijmë të identifikojmë sulme që mund të na vijnë nga jashtë ose nga burime të tjera.

### 7.2. Qeverisja dhe menaxhimi i riskut.

Kompania jonë në rast se do të ndodhet në kushtet e një incidenti të sigurisë ka krijuar një plan emergjence dhe një strategji për të mos ndërprerë shërbimin e internetit. Kështu për vazhdimin e punës në rast të ndonjë situate të jashtzakonshme ne kemi siguruar linja back up (rezervë), pajisje të dubluara të tilla si router, sëitch-a, lidhje me fibër optike back up me sitin kryesor dhe lidhje e dubluar interneti me operatorin e furnizimit me internet.

Kjo mundëson një up time afërsisht 100% duke garantuar vazhdimësinë e furnizimit me internet te abonentët dhe njëkohësisht vazhdimësinë e biznesit.

Gjithashtu punonjësit do të jene në dispozicion kundrejt pagesave shtesë. Në rastet kur është e nevojshme kopania do të marre konsulent të specializuar kundrejt pagesës.

Në raste incidenti apo kryerje punimesh të gjithë përdoruesit do njoftohen nëpërmjet telefonit, rrjeteve sociale apo mailbox-it.

### 7.3. Rrjeti dhe testimi i sistemit të informacionit.

**Testimi** është faza kur ka përfunduar i gjithë rrjeti dhe testohet funksionimi i tij. Këtu vërtetohet cilësia e linjes dhe kapaciteti midis pikës ku del shërbimi dhe pikës përfundimtare që shkon shërbimi në këtë rast është abonenti.
Gjatë këtij procesi bëjmë edhe prova në rastet e ndodhjes së një incidenti, të tilla si dalja nga puna e një pajisje në terren duke verifikuar njëkohësisht problemet që mund të japi në sisitem.

### 7.4. Vlerësimi i Sigurisë.

| Tabela mbi vlerësimin e incidenteve të sigurisë | | |
|---|---|---|
| **Kohëzgjatja e incidentit të sigurisë** | Më tepër se 1 orë ose më pak se 2 orë | Më tepër se 2 orë |
| Numri i përdoruesve të prekur nga incidenti ose % e tyre. | | |
| **>1000 ose> 5 %** | Mesatar | I lartë |
| Zona gjeografike e shtrirjes së incidentit të sigurisë | | |
| **> 30 km** | Mesatar | I lartë |
| Përfundimet mbi incidentin | | |

### 7.5. Monitorimi i pajtueshmerisë –Monitorimi i rregullt sipas ligjit.

**Monitorimi:** është faza kur zbatohet plani fizikisht në terren, si procese përfshihen punimet në rrugë, vendosja e shtyllave, shtrirja e fibres optice, instalimi i pajisjeve të internetit te abonenti. I gjithë rrjeti i shtruar projektohet në hartë. Pasi ka përfunduar puna njftohen institucionet ku është marrë leja.

Gjithashtu monitorimi përfshin vëzhgimin e punës së pajisjeve dhe rrjetit. Monitorimi mund të bëhet nga zyra, mund të bëhet direkt nga sistemi nga personi përgjegjës për incidentet e sigurisë ose monitorimi në terren që realizohet nga tekniket e instalimit të pajisjeve të internetit.

### 7.6. Auditimi:

Kontrollit i sigurisë në kopani kërkohet nga personi përgjegjës për sigurinë ( administratori).Ky i fundit therret ekspertë nga jashtë, për të bërë auditimin e infrastructurës së rrjtit në pajisjet e vjetra të sistemit apo në pajisjet e reja të sistemit.

Me anën e auditimit bëhet:

1.Identifikim i problematikave që nuk duken të rregullta dhe në standart.
2.Zbulim i pajisjeve me funksion jo standart.
3. Zbulim i problematikave në kabllot e fibrave optike.
4. Zbulimi i konflikteve të ndryshme në pajisjet e zyres ose në terren.
5. Zbulimi i infektimeve të pajisjeve ose serverave të kompanisë.
6.Zbulim i keqkonfigurimeve të pajisjeve të infrastructurës së rrjetit.

Në rastin kur një punonjës dyshon në keqfunksionimin e një elementi të infrastrukturës së rrjetit sic janë pajisje në zyrë, pajisje ne server room ose në terren ai i drejtohet personit përgjegjës për kryerjen e auditimit.
Personit përgjegjës për kryerjen e procedurave të auditimit ka aksesin  në cdo pajisje dhe shërbimet e ofruara, përgjatë kohës që do kryhet audidtimi.
Në fund të auditimit, ekspertët përpilojnë një dokument të cilin ia dorëzojnë Administratorit. Ky dokument do të përdoret më pas për mbarvajtjen e infrastructurës së rrjetit dhe ofrimit të shërbimit internet.

**Me respekt :**

Ervis Cina

# Aneks nr 1.

## Regjistri i incidenteve të sigurisë

## Informacion kontakti:

Data_____

Emri i Sipërmarrësit: _____

Emri dhe Mbiemri i personit të ngarkuar për eleminimin e incidenteve të sigurisë dhe/ose cënimit të integritetit: _____

Pozicioni i Punës: _____

Telefon, e-mail: _____

**Përshkrimi i Incidentit të Sigurisë dhe/ose Cënimit të Integritetit**

Lloji: _____
_____

Përcaktimi se cilat rrjete, sisteme ose shërbime preken nga incidenti i sigurisë:

---

Koha e ndodhjes dhe kohëzgjatja:
_____

Informacion rreth shkakut fillestar ose shkaqeve:
_____
_____

Përshkrimin e incidentit ( përcaktoni të dhënat në mënyrë sa më të detajuar):_____
_____

Numri i përafërt i përdoruesve të prekur nga incidenti i sigurisë ose cënimi i integritetit ose përqindja e tyre(%) nga perdoruesve total të rrjetit dhe/ose shërbimit:_____

Zona Gjeografike e prekur nga incidenti i sigurisë dhe/ose cënimi i integritetit (km2):_____

Burimet e prekura:

---

Pasojat :_____

_____

**Menaxhimi i incidentit të sigurisë dhe/ose cenimit të integritetit Veprimet e nëermarra( të planifikuara për tu ndërmarrë) për të eleminuar incidentin e sigurisë dhe per të reduktuar pasojat e tij:**

**_____**

Veprimet të ndërmarra për të reduktuar incidentin e sigurisë dhe për ta reduktuar atë:

Masat pas incidentit

_____

_____

**Informacione të tjera te rëndësishme**

Mësimet e
nxjerra_____

_____

**Data:**

_____.