“Masat teknike dhe organizative për të garantuar sigurinë dhe integritetin e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike”

- Politikat e perdorimit te sigurise se informacionit
- Politikat e sigurise se serverave
- Politikat e perdorimit te email-eve
- Politikat e mediave(paisjeve) te levizshme
- Politikat e Password-eve te DB(Data Base)
- Politikat e paisjeve DMZ te internetit
- Politikat e Extranet
- Politikat e aksesit nga rrjetet e jashtme
- Politikat e sigurise se Router-ave
- Politikat e Rrjetave Private Virtuale(VPN)

- **Politikat e perdorimit te sigurise se informacionit**

1.0 Rishikim i pergjithshem

Qellimet e Pergjegjesit te Sigurise se Informacionit nuk kane si qellim imponimin e kufizimeve te cilat jane ne kundershtim me kulturen e besimit dhe integritetit te Abissnet. Pergjegjesi i Sigurise se Informacionit eshte i angazhuar per mbrojtjen e punonjesve apo partnereve te Abissnet nga veprime ilegale apo demtuese nga individe te ndryshem qofshin keto veprime me dashje apo pa dashje.

Te gjitha sistemet, duke perfshire paisjet kompjuterike, software, sistemet operative, paisjet e ruajtjes se te dhenave, mail elektronik, navigimin ne internet(WWW) si dhe FTP(Protokolli i Transferimit te Dhenave) jane prone e Abissnet. Keto sisteme jane per tu perdorur per qellime biznesi dhe qe ju sherbejne interesave te kompanise si dhe klienteve tane.

Siguria Efektive eshte nje perpjekje ne grup qe perfshin mbeshtetjen e cdo punonjesi te Abissnet dhe bashkon te gjithe personat te cilet meren me sigurine e informacionit apo sistemet te cilat kane lidhje me te. Eshte pergjegjesi e cdo perdoruesi te kompjutervae te dije keto rregulla mbi sigurine dhe aktivitetet e tyre ne rrjetin e jashtem te jene sipas udhezimeve perkatese.

2.0 Qellimi

Qellimi I kesaj politike eshte qe te nxjerre ne pah limitimet e perdorimit te paisjeve kompjuterike ne Abissnet. Keto rregulla jane vendosur qe te mbrojne punonjesit dhe Kompanine Abissnet. Perdorimi i papershtatshem i ketyre pasijeve e ekspozon Abissnet drejt rreziqeve te ndryshme ne rrjetin e jashtem sic jane sulmet e viruseve, kompromentimi i sistemeve te rrjeteve dhe sherbimeve si dhe probleme ligjore.

3.0 Mbulimi

Kjo politike aplikohet tek te gjithe punonjesit e Abissnet, duke perfshire te gjithe stafin qe ka lidhje me keto paisje apo sherbime. Kjo politike aplikohet ne te gjitha paisjet te cilat jane prone e Abissnet.

4.0 Politikat

4.1 Perdorimi i pergjithshem dhe Pronesia

1. Nderkohe qe nje Administrator Rrjeti i Abissnet krijon nje nivel privatesie te arsyeshem, perdoruesit jane ne dijeni se te dhenat qe ato krijojne ne sistem mbeten prone e Abissnet. Per shkak te nevojes per mbrojtjen e rrjetit, pjesa menaxhuese nuk mund te garantoje konfidencialitetin e informacionit i cili ruhet ne cdo paisje rrjeti e cila eshte ne pronesi e kompanise Abissnet.
2. Punonjesit jane pergjegjes per te patur nje gjykim sa me te mire dhe te arsyeshem mbi limitin e perdorimit personal te paisjeve ne rrjet. Departamentet individuale jane pergjegjes per krijimin e udhezimeve mbi perdorimin personal te sistemeve.
3. Pergjegjesi i Sigurise se Informacionit rekomandon qe cdo informacion qe perdoruesit e konsiderojne sensitive apo te cenueshem duhet te enkriptohet.
4. Per qellime sigurie dhe mirembajtje te rrjetit individe te ndryshem ne Abissnet monitorojne paisjet, sistemet dhe trafikun e rrjetit ne cdo kohe, kjo gje ne Abissnet mbulohet nga Departamenti NOC(Qendra e Operimit te Rrjetit).
5. Abissnet ka te drejten qe te auditoje rrjetet dhe sistemet ne menyre periodike ne menyre qe te siguroje perputhshmeri te plote me politikat e permendura me lart.

4.2 Informacioni i Sigurise dhe i Pronesise

1. Informacionin i cili mbahet ne sistemet Internet, Intranet apo Extranet duhet te klasifikohet si konfidencial apo jo konfidencial. Punonjesit e kompanise ndermarin hapat e nevojshem ne menyre qe te ndalohet aksesi i pa autorizuar drejt ketyre informacioneve.
2. Password-et mbahen te sigurte dhe nuk ndahen me punonjesit e tjere te kompanise dhe aq me teper me te trete jashte kompanise. Perdoruesit e autorizuar jane totalisht pergjegjes per sigurine e password-eve apo llogarive te tyre. Cdo kater muaj ndryshohen password-et nga i gjithe staffi i Abissnet ne menyre qe te rritet siguria, gjithashtu cdo tre muaj ndryshohen password-et e paisjeve sistemeve apo paisjeve kryesore ne rrjetin Abissnet.
3. Te gjithe kompjuterat, laptopet dhe workstations jane te siguruar me password me nje kohe aktivizimi prej 10 minutash nese ne kete paisje nuk po punohet, ose duke bere log-out menjehere nga perdoruesi i cili do te largohet nga vendi i punes,

4. Punonjesit e kompanise Abissnet perdorin enkriptim ne informacionin qe behet share apo transferohet.
5. Per shkak se informacioni qe mbahet ne komjuterat e levizshem eshte shum i cenueshem, kur transferohet informacion tregohet nje kujdes i vecante.
6. Nese nje punonjes i Abissnet, perdor email me domain Abissnet.al per pastime ne grupe te ndryshme e ka me detyrim te citoje qe ky eshte nje opinion totalisht personal dhe nuk ka lidhje me politikat qe ndjek Abissnet, pervec rasteve kur postimet jane rrjedhoje e mardhenieve biznesi dhe personi ne fjale eshte i autorizuar te flase ne emer te kompanise.
7. Te gjithe hostet te cilat jane te lidhura ne rrjetin e brendshem te kompanise Abissnet, qofshin keto ne pronesi individuale apo te Abissnet bejne skanime te vazhdueshme per viruse.
8. Punonjesit tregojne nje kujdes te vecante kur hapin emaile nga dergues te panjohur, duke u kujdesur te mos hapin te dhenat te cilat I jane bashkangjitur atij email duke qene se mund te jene viruse te ndryshme.

4.3 Perdorimi i papranueshem

Aktivitete qe do te permenden me poshte jane ne pergjithesi te ndaluara.

Aktivitetet e Rrjetit dhe Sistemeve

Aktivitetet e meposhtme jane te ndaluara ne menyre strikte dhe pa perjashtime:

1. Shkelja e te drejtave te cdo personi ose te kompanise te cilat kane te bejne me patentat, te drejten e autorit, shkembimet secrete apo te dhena te tjera si instalimi ose shperndarja e software-ve te vjedhura te cilat nuk jane ne pronesi per tu perdorur nga Abissnet.
2. Kopjim I pa autorizuar I materialeve, duke perfshire por jo vetem, instalimin e programeve te ndryshme per te cilat Abissnet apo perdoruesi fundor nuk ka nje license.
3. Eksportimi I programeve, informacioneve teknike apo programeve te enkriptuara ne shkelje te ligjeve te kontrollit te exportit rajonal klasifikohet si shkelje dhe jo e ligjshme. Strukturat perkatese duhet te konsultohen me pare se te ndermarrin vendime te tilla.
4. Instalimi I programeve demtuese ne rrjet ose ne server.
5. Tregimi I password-it te tjereve apo lejimi I perdorimit te passwordit nga te tjere.
6. Berja e deklaratave ne lidhje me garancine ne menyre te drejtperdrejte apo te nenkuptuar, me perjashtim te rasteve kur eshte pjese e punes se perditshme.

7. Skanimi I portave apo skanime sigurie jane te ndaluara me perjashtim te rasteve kur jepet leje nga Pergjegjesi I Sigurise se Rrjetit.
8. Ekzekutimi I cdo forme monitorimi rrjeti gje e cila mund te implikoje personin ne fjale ne marje te informacionit eshte e ndaluar me perjashtim te rasteve kur eshte pjese e punes se perditshme.
9. Shmangja e autentikimit te perdoruesave ose sigurise ne ndonje host, rrjet apo llogari.
10. Pengimi ose bllokimi I sherbimit te cdo perdoruesi tjeter pervec hostit te punonjesit.
11. Perdorimi I skripteve, ose dergimi I mesazheve te cdo lloji me qellim bllokimin apo nderhyrjen ne nje session terminal te nje perdoruesi ne menyre lokale apo nepermjet internetit.
12. Nxjerrja e informacionit rreth punonjesve te Abissnet jashte Abissnet.

Aktivitetet e Komunikimit dhe Email-et

1. Dergimi I email-eve te pa kerkuara, duke perfshire dergimin e email-eve junk ose email-eve te tjere me qellim reklamimi drejt perdoruesave te cilet nuk e kane kerkuar nje informacion te tille(email-e spam).
2. Cdo forme kercenimi nepermjet email apo telefonit
3. Perdorim I pa autorizuar I informacionit ne email.
4. Shperndarja e email drejt adresave te tjera pervec atij I cili e ka sjelle ate email.
5. Krijimi dhe dergimi I skemave “piramide” te cdo tipi me ane te email.
6. Perdorimi I pa kerkuar I email-eve te gjeneruara nga rrjeti I Abissnet apo cdo kompanie tjeter, apo shperndarja e sherbimeve te hostuara ne Abissnet apo te lidhura ne rrjetin e Abissnet.
7. Postimi I te njejtit mesazh apo mesazheve te cilat nuk kane lidhje me biznesin drejt nje numri te madh njerezish.

5.0 Zbatimet

Cdo punonjes I cili thyen politikat e permendura me lart do te jete pjese e ndeshkimeve disiplinore duke shkuar deri ne shkeputje te mardhenies se punes.

- **Politikat e Sigurise se Server-ave**

1.0 Qellimi

Qellimi I ketyre politikave eshte vendosja e standarteve per konfigurimet baze te serverave te brendshem te cilet jane ne pronesi te Abissnet. Implementimet

sa me efektive te ketyre politikave do te minimizojne aksesin e pa autorizuar ne informacionet dhe teknologjine e cila eshte ne pronesi te Abissnet.

2.0 Mbulimi

Keto politika aplikohen ne paisjet te cilat zoterohen nga Abissnet dhe tek serverat te cilet jane te regjistruar ne pronesi te Abissnet. Keto politika jane specifikishte per paisjet te cilat ndodhen ne rrjetin e brendshem te Abissnet.

3.0 Politikat

3.1 Pergjegjesite dhe pronesia

Te gjithe serverat e brendshem ne Abissnet jane ne pronesi te nje grupi operacional I cili eshte pergjegjes per administrimin e sistemit. Grupet operacionale monitorojne perputhshmerine e konfigurimeve ne cdo server. Grupi operacional krijon nje guide per ndryshimin e konfigurimeve, gje e cila pefshin rishikimin dhe miratimin nga Pergjegjesi I Sigurise se Informacionit.

- Serverat regjistrohen ne sistemin e menaxhimit te korporates. Minimalisht kerkohet informacioni I meposhtem ne menyre qe te identifikohet ne menyre te sakte pika e kontaktit.
    - Vendodhja dhe nje kontakt I serverit dhe nje kontakt reserve.
    - Version I Sistemit te Operimit dhe atij Fizik.
    - Funksionet dhe aplikacionet kryesore.
- Informacioni ne sistemin e menaxhimit te korporates mbahet I perditesuar.
- Ndryshimet ne konfigurimin e serverave duhet te ndjekin procedurat perkatese te ndryshimeve perkatese.

3.2 Udhezimet per konfigurimet e pergjithshme

- Konfigurimet e sistemeve te operimit duhet te jene ne perputhshmeri me ushezimet e miratuara nga Pergjegjesi I Sigurise se Informacionit.
- Sherbimet dhe aplikacionet qe nuk perdoren caktivizohen.
- Aksesi ne sherbime regjistrohet dhe mbrohet me ane te metodave te kontrollit te aksesit.
- Instalohen patch-et e sigurise me te fundit.
- Serverat jane fizikisht te vendosur ne nje ambient te kontrolluar.
- Serverat nuk duhet te jene te vendosura ne dhoma te vogla, por ne Abissnet jane te vendosur ne dhoma me hapesire te madhe dhe me ajer te kondicionuar dhe me lidhje redundante.

3.3 Monitorimi

- Te gjitha eventet qe kane lidhje me sigurine e sistemeve duhet te regjistrohen si me poshte:
    - Te gjitha regjistrimet te cilat kane lidhje me sigurine mbahen online per te pakten nje jave.
    - Backup I konfigurimeve I perditshem duhet ruhet deri te pakten 1 muaj.
    - Nje backup I plote I te gjitha regjistrimeve te sistemeve te nje jave mbahet te pakten per nje muaj.
    - Backup-e te plota te nje muaji ruhen per te pakten 2 vite.
- Eventet qe kane lidhje me sigurine raportohen tek Pergjegjesi I Sigurise se Informacionit, I cili me pas rishikon regjistrimet qe ka sistemi dhe raporton me pas tek menaxheri I IT. Eventet qe kane lidhje me sigurine perfshine:
    - Sulmet nga skanimi I portave
    - Akses I padeshiruar tek llogarite e privilegjuara.
    - Ndodhi jo normale ne lidhje me aplikacionet ne nje host te caktuar.

4.0 Zbatimi

Cdo punonjes I cili thyen politikat e permendura me lart do te jete pjese e ndeshkimeve disiplinore duke shkuar deri ne shkeputje te mardhenies se punes.

- **Politikat e Perdorimit te Email-eve**

1.0 Qellimi

Me qellim parandalimin e prishjes se imazhit te kompanise Abissnet nga email-et qe dalin nga Abissnet, publiku I gjere tenton ti shikoje keto mesazhe si nje deklarate zyrtare nga ana e Abissnet.

2.0 Mbulimi

Kjo politike meret me perdorimin e duhur te cdo email qe dergohet nga adresat email Abissnet dhe aplikohet mbi te gjithe punonjesit e Abissnet.

3.0 Politikat

3.1 Perdorimi I ndaluar

Sistemi I email-eve ne Abissnet nuk perdoret per krijimin apo shperndarjen e mesazheve me permbajtje ofenduese mbi rracen, gjinine, ngjyren, moshen, orientimet seksuale, pornografi, besimet fetare, besimet politike apo mbi

origjinen kombetare. Punonjesit te cilet marin ndonje email I cili ka permbajtje te ngjashme me rastet e permendura me lart raportojne menjehere tek supervizori.

3.2 Perdorimi personal

Perdorimi I nje sasie te arsyeshme te burimeve te Abissnet per email-e personale eshte e pranueshme, por keto emaile qe nuk kane lidhje me punen duhet te ruhen ne nje folder te vecante. Dergimi I email-eve jo serioz nga llogaria Abissnet eshte e ndaluar. Sa here qe dergohet nje email I ri, fillimisht duhet te kaloje kontrollin e antivirus-it, me pas eshte I sigurt per tu derguar nga llogaria Abissnet drejte llogarive te tjera. Keto kufizime jane te aplikueshme dhe per email-et te cilat I jane derguar nje punonjesi Abissnet dhe I cili do ta ridergoje kete email ne nje llogari tjeter brenda apo jashte Abissnet.

3.3 Monitorimi

Punonjesit e Abissnet nuk presin privatesi ne informacionin qe ato ruajne, dergojne apo marin ne sistemin e email te kompanise. Abissnet monitoron mesazhet pa patur nevoje te njoftoje punonjesit per kete gje. Abissnet nuk eshte I detyruar te monitoroje mesazhet e derguara me email.

4.0 Zbatimi

Cdo punonjes I cili thyen politikat e permendura me lart do te jete pjese e ndeshkimeve disiplinore duke shkuar deri ne shkeputje te mardhenies se punes.

- **Politikat e medias se levizshme**

1.0 Rishikim I pergjithshem

Media e levizshme eshte nje burim I njohur I infektimeve me viruse dhe lidhet direct me humbje te informacionit ne shume organizata.

2.0 Qellimi

Per te minimizuar riskun e humbjeve apo te ekspozimit te informacionit qe mbahet nga Abissnet gjithashtu dhe reduktimi I riskut te marjes se viruseve ne kompjuterat te cilat operojne ne Abissnet.

3.0 Mbulimi

Kjo politike mbulon te gjithe kompjuterat dhe serverat te cilet operojne ne Abissnet.

4.0 Politikat

Stafi I Abissnet mund te perdore median e levizshme vetem ne kompjuterat e tyre te punes. Media e levizshme e Abissnet nuk duhet te lidhet apo te perdoret ne kompjutera te cilet nuk zoterohen nga Abissnet apo pa lejen e Abissnet. Informacioni sensitivduhet te ruhet ne media te levizshme vetem kur eshte I specifikuar ne detyrat e punes, ose ne ato raste kur kerkohet informacion nga organizatat qeverisese. Perjashtime nga keto rregulla behen vetem ne rastet kur behen me kerkese te vecante dhe vetem per ceshtje specifike.

5.0 Zbatimi

Cdo punonjes I cili thyen politikat e permendura me lart do te jete pjese e ndeshkimeve disiplinore duke shkuar deri ne shkeputje te mardhenies se punes.

- **Politikat e password-eve te DB(Data Base)**

1.0 Qellimi

Keto politika vendosin kerkesat per ruajtjen dhe marjen e username nga databaza ne menyre te sigurte, keto username do te perdoren per te aksesuar nje nga paisjet te cilat ndodhen ne rrjetin Abissnet. Programet kompjuterike te cilat operojne ne rrjetin Abissnet shpesh qe te operojne ne menyre te plote kane nevoje per nje nga databazat e brendshme te rrjetit Abissnet. Ne menyre qe te aksesoje keto databaza , nje program duhet te autentikohet ne database duke paraqitur kredenciale te vlefshme.

2.0 Mbulimi

Kjo politike aplikohet tek te gjitha programet te cilat do te aksesojne databazen e perdoruesave.

3.0 Politikat

3.1 Te pergjithshme

Me qellim mirembajtjen e sigurise se databazes se brendshme te Abissnet, aksesi I programeve soft do te lejohet vetem pas autentikimit te suksesshem me kredencialet perkatese. Kredencialet te cilat do te perdoren per autentikim ne kete database nuk duhet te jene te ruajtura ne tekst ne kodin e programit por te enkriptuara. Kredencialet e databazes nuk duhet te ruhen ne nje vendodhje e cila eshte e aksesueshme nga web.

3.2 Kerkesa Specifike

3.2.1 Ruajtja e username dhe password te databazes

- Username dhe password te databazes ruhen ne nje dokument te vecante nga pjesa e kodit te ekzekutimit te programit. Ky document nuk eshte I lexueshem jasht rrjetit te Abissnet.
- Kredencialet e databazes jane te ruajtura ne serverin e databazes.

3.2.2 Marja e username dhe password nga databaza

- Nese username dhe password jane te ruajtura ne nje document qe nuk eshte kodi kryesor, atehere keto te dhena lexohen nga nje file tjeter qe eshte I ruajtur ne kete database.
- Hapesira ku do te ruhen keto user dhe password eshte e ndare fizikisht nga pjesa tjeter e programit.

3.2.3 Aksesi ne databazen e username dhe password-eve

- Cdo program apo cdo koleksion programesh ka kredencialet e tij unike ne database. Ndarja e kredencialeve ndermjet programeve te ndryshme nuk lejohet.
- Password-et e databazes te cilet perdoren nga programet kane nivele te ndryshme.

4.0 Zbatimi

Cdo punonjes I cili thyen politikat e permendura me lart do te jete pjese e ndeshkimeve disiplinore duke shkuar deri ne shkeputje te mardhenies se punes.

- **Politikat e Paisjeve DMZ**

1.0 Qellimi

Qellimi I kesaj politike eshte qe te percaktoje standartet te cilat te plotesohen nga te gjitha paisjet te cilat zoterohen nga Abissnet dhe jane te vendosura jashte firewall te kompanise. Keto standarte jane krijuar per te minimizuar mundesine e humbjes se informacioneve te rendesishme te Abissnet. Paisjet te cilat ndodhen jashte murit mbrojtes(firewall) te Abissnet konsiderohen si pjese e DMZ(De-militarized zone). Keto paisje jane me shume te prirura per tu sulmuar nga jashte duke qene se nuk jane ne pjesen e brendshme te mbrojtur te rrjetit Abissnet.

Kjo politike percakton standartet e meposhtme:

- Pergjegjesi pronesie
- Kerkesa per konfigurime te sigurta
- Kerkesa operacionale
- Kerkesa per kontrolle te vazhdueshme

2.0 Mbulimi

Te gjitha paisjet e vendosura ne nje DMZ dhe qe zoterohen nga Abissnet duhet te ndjekin keto politika. Te gjitha paisjet ekzistuese apo ato qe do te vendosen me tej ne te ardhmen ne zonen DMZ duhet te plotesojne kushtet e percaktuara me lart.

3.0 Politikat

3.1 Pergjegjesite dhe pronesia

Pergjegjesi I rrjetit eshte pergjegjes per:

- Paisjet duhet te jene te dokumentuara ne sistemin e menaxhimit te kompanise
    - Vendodhja dhe kontakti per hostet remote
    - Versioni hardware dhe ai I operimit
    - Funskionet dhe aplikacionet kryesore
    - Password-et e privilegjuara
- Akses I menjehershem te paisjet dhe tek regjistrimet e sistemit sa here te jete e nevojshme.
- Sipas kerkesave apo nevojave duhet te mundesohet nderrim I paisjeve.

Per te verifikuar perputhshmerine e plote me keto politika, pergjegjesi I sigurise se informacionit auditon ne menyre periodike paisjet DMZ.

3.2 Politikat e pergjithshme te konfigurimit

- Paisjet hardware, sistemet e operimit, sherbimet dhe aplikacionet duhet te miratohen nga Pergjegjesi I sigurise se informacionit si pjese e fazes se para aplikimit.
- Sherbimet dhe aplikacionet te cilat nuk I sherbejne klienteve aktiv behen inactive.
- Sherbimet dhe aplikacionet duhet te mbrohen me access-lista.
- Te gjitha update-et e hosteve duhet te behen nepermjet kanaleve te sigurta.
- Evente te cilat kane te bejne me sigurine e paisjeve duhet te regjistrohen dhe me pas te auditohen nga pergjegjesi I sigurise se informacionit ku perfshihen:
    - Tentativat e deshtuara per te aksesuar paisjet
    - Deshtimet per te kerkuar akses te privilegjuar
    - Dhunime te politikave te aksesit

3.3 Procedurat e menaxhimit te instalimeve te reja

- Instalimet e reja behen nepermjet procesit te vendosjes se paisjeve DMZ.

- Ndryshimet ne konfigurime duhet te ndjekin procedurat e menaxhimit te ndryshimeve.
- Pergjegjesi I sigurise se informacionit duhet te ndjeke hap pas hapi te gjitha procedurat ne menyre qe te aprovoje ose jo te gjitha konfigurimet e reja apo ndryshimet perkatese.

3.4 Ofruesit e sherbimeve te jashtme

- Pergjegjesia e sigurise se ketyre pasijeve te cilat jane te vendosura ne rrjetin e jashtem te Abissnet eshte qaresuar me ofruesin e ketij sherbimi ne menyre te qarte ne kontrate sipas kushteve te lart permendura.

4.0 Zbatimi

Cdo punonjes I cili thyen politikat e permendura me lart do te jete pjese e ndeshkimeve disiplinore duke shkuar deri ne shkeputje te mardhenies se punes.

- **Politikat e extranet**

1.0 Qellimi

Ky document pershkruan politikat nepermjet te cilave palet te treta lidhen me ane te rrjetit Abissnet me qellim nderlidhjeje ndermjet bizneseve.

2.0 Mbulimi

Ne kete politike perfshihen pale te treta te cilat kerkojne akses ne burimet jo publike te Abissnet pavaresisht menyres se perdorur per te bere lidhjen qofte ajo me VPN apo me qark te thjeshte si psh ISDN apo frame relay. Lidhja me pale te treta sic jane kompanite e ofrimit te sherbimit te internetit te cilat ofrojne akses ne internet per kompanine Abissnet nuk jane pjese e ketyre politikave.

3.0 Politikat

Kerkesat paraprake

- Te gjitha lidhjet e reja extranet kalojne ne nje faze rishikimi ne bashkepunim me departamentin e sigurise se informacionit, ku

rishikimet kane te bejne me permbushjen e plote te kerkesave te biznesit per te patur nje siguri sa me te larte.

- Per cdo lidhje te re qe behet firmoset nje marreveshje ndermjet Abissnet dhe paleve te treta te interesuara per te mare sherbime nga Abissnet. Kjo marreveshje firmoset nga zevendes presidenti I kompanise Abissnet dhe nga perfaqesues te paleve te treta.
- Nga kompania Abissnet vendoset nje pike kontakti per palet e treta te cilet kerkojne keto sherbime nga Abissnet dhe te gjitha ceshtjet ne lidhje me kete klient ndiqen nga kontakti I vendosur

4.0 Zbatimet

Cdo punonjes I cili thyen politikat e permendura me lart do te jete pjese e ndeshkimeve disiplinore duke shkuar deri ne shkeputje te mardhenies se punes.

- **Politikat e aksesit remote**

1.0 Qellimi

Qellimi I kesaj politike eshte qe te percaktoje standartet per lidhjen e hosteve nga rrjeti I jashtem drejt rrjetit Abissnet. Keto standarte jane dizenjuar ne menyre te tille qe te minimizojne ekspozimin e Abissnet nga demet e jashtme te cilat vijne si pasoje e perdorimit te pa autorizuar te burimeve te Abissnet.

2.0 Mbulimi

Kjo politike aplikohet tek te gjithe punonjesit Abissnet si dhe te paleve te treta te lidhura ne rrjetin Abissnet. Implementimet qe jane te mbuluara ne kete politike perfshijne: ISDN, dial-in modems, DSL, VPN, SSH etj.

3.0 Politikat

- Eshte pergjegjesi e punonjesve te Abissnet ose te tjereve te cilet kane akses remote ne rrjetin Abissnet qe te sigurohen qe ti jepet e njejta konsiderate njelloj sikur te jene te lidhur onsite, te kene parasysh te gjithe politikat e sigurise ne menyre te njejte.
- Aksesi remote duhet te kontrollohet ne menyre strikte, dhe password-et duhet te jene te veshtire per tu thyer.
- Password-et nuk ndahen me asnje person, qofshin ato dhe pjestare te familjes.

4.0 **Zbatimet**

Cdo punonjes I cili thyen politikat e permendura me lart do te jete pjese e ndeshkimeve disiplinore duke shkuar deri ne shkeputje te mardhenies se punes.

- **Politikat e sigurimit te router-ave**

1.0 Qellimi

Ky document pershkruan konfigurimet minimalete sigurise per te gjithe router-at dhe switch-et te cilet lidhen ne rrjetin e Abissnet.

2.0 Mbulimi

Ndikon tek te gjithe router-at dhe switch-et ne rrjetin Abissnet.

3.0 Politikat

Cdo router ploteson kerkesat minimale te konfidurimit si me poshte:

- Password qe te kalon ne priviledge-ed mode ruhet I enkriptuar.
- Ndalohen:
  - Broadcast-et e pa nevojshme ne rrjet.
  - Paketat qe vijne ne hyrje te router me adrese IP te pa vlefshme.
- Perdoren string-e standarte te kompanise per SNMP
- Rregulla aksesi drejt paisjeve.
- Router-at jane te perfshire ne sistemin e menaxhimit dhe te monitorimit.
- Cdo router apo switch eshte I pajisur me banner ku shkruhet: “Akses I Pa Autorizuar”.
- telnet nuk lejohet jashte rrjetit te Abissnet, pervec ne rastet kur nje punonjes I abissnet eshte I lidhur me vpn me rrjetin Abissnet.

4.0 Zbatimet

Cdo punonjes I cili thyen politikat e permendura me lart do te jete pjese e ndeshkimeve disiplinore duke shkuar deri ne shkeputje te mardhenies se punes.

- **Rrjetet Virtuale Private (VPN)**

1.0 Qellimi

Qellimi I ketyre politikave eshte qe te siguroje udhezime per aksesin remote ose lidhej virtuale private drejt rrjetit Abissnet.

2.0 Mbulimi

Kjo politike zbatohet mbi te gjithe punonjesit e Abissnet duke perfshire dhe personelin qe ka lidhje me pale te treta te cilat perdorin VPN per te aksesuar rrjetin e brendshem te Abissnet.

3.0 Politikat

- Punonjesit e Abissnet mund te perdorin VPN per te punuar nga shtepite e tyre ne raste emergjente, kur duhet te behet nje nderhyrje e shpejte ne rrjet apo kur duhet te modifikohen dokumenta te ndryshem.
- VPN perdoret nga punonjesit Abissnet duke perdorur kredencialet e tyre unike ku perfshihet nje username dhe nje password I forte ne menyre qe te realizojne lidhjen me Abissnet. Nuk duhet ne asnje rrethane keto te dhena te ndahen apo te perdoren nga te tjere pasi te gjitha masat ndeshkuese do te bien mbi username perkates dhe jo mbi personin I cili ka shkaktuar demet perkatese nga nje nderhyrje e pa deshiruar.
- Punonjesit te cilet mund te perdorin VPN marin aprovimin me pare nga pergjegjesi I sigurise se informacionit.
- Te gjithe kompjuterat qe perdoren per te bere lidhjen VPN duhet te jene te update-uar me antiviruset me te fundit.
- Te gjitha te dhenat e VPN dhe gateway konfigurohen nga administrator I rrjetit.

4.0 Zbatimet

Cdo punonjes I cili thyen politikat e permendura me lart do te jete pjese e ndeshkimeve disiplinore duke shkuar deri ne shkeputje te mardhenies se punes.