NISATEL OPERATOR PUBLIK I TELEKOMUNIKACIONEVE
Pavaresia 1200, Vlore, Albania
E-mail: info@nisatel.al;

LENDA: Informacion per sigurine e rrjetit dhe informacionit sipas rregullores se AKEP (Aneksi 3)

Ky informacion perfshin te gjitha pikat e Aneksit 3 te rregullores se AKEP.

Pika D1: Qeverisja dhe Menaxhimi i Riskut

Pergjegjesi i rrjetit kujdeset ne cdo moment per menaxhimin e riskut duke bere te mundur ne rast risku identifikimin , percaktimin , prioritizimin e riskut duke perdorur mjete sa me ekonomike dhe te koordinuara per te minimizuar , monitoruar apo per te zvogeluar probabilitetin qe nje risk te ndodh .

Te gjithe punonjesite e Nisatel vihen ne dijeni per sigurine dhe jane subjekt i nje kontrolli vjetor nese a jane konform zbatimit te rregullave dhe standardeve te sigurise

Te gjithe punonjesite e Nisatel jane ne dijeni per punen qe duhet te kryejne dhe cfare lidhet me ta duke mos cenuar as privatesine e te tjereve si dhe as sigurine e sistemeve duke u pajisur secili me account te dallueshem nga tjetri .

Politikat e sigurise rishikohen ne menyre periodike nga pergjegjesi i rrjetit duke bere te mundur shmangien e incidenteve , shkeljet ,qe mund te kene ndodhur me pare ofruesve te tjere .

Ne menyre periodike behen kontrolle apo skanime te sistemeve dhe programeve te implementuara per pune ne menyre qe te identifikohet apo ndalohet sulmi nga ndonje virus, malware, apo sulm pirat.

Punonjesit janë pergjegjes per mbrojtjen dhe trajtimin me kujdes te pasurive te kompanise. Te gjitha llojet e informacioneve mbrohen me sisteme, me standart te larta te sigurise si nga prodhuesit edhe nga instalimet e implementuara prej kompanisë tonë.

Ne rast te incidenteve me palet e treta mbahen rekorde per keto incidente duke bere te mundur rishikimin e rregullores per sa i perket sigurise per palet e treta .

Personi pergjegjës për risqet ka per detyre zbulimin dhe identifikimin e kërcenimeve perpara se ato te ndodhin duke bere te mundur planifikimin dhe veprimtarine parandaluese gjate kohes kur nje proces, aktivitet apo sherbim eshte duke u ekzekutuar.

Personi pergjegjes per risqet zbaton nje procedure standarte per identifikimine e kercenimeve dhe raportimit menjehere te Pergjegjesi i Departamentit dhe Administratori.

NISATEL OPERATOR PUBLIK I TELEKOMUNIKACIONEVE
Pavaresia 1200, Vlore, Albania
E-mail: info@nisatel.al;

Pika D2: Siguria e Burimeve Njerëzore

- ∑ Te gjithe punonjesit ndjekin trajnime te herepashershme per sa i perket sigurise teknike te tyre apo dhe sigurise se sistemeve qe jane duke perdorur .

- ∑ Te gjithe punonjesit jane te detyruar te zbatojne kerkesat e rregullores se sigurimit teknik per mbrojtjen ne pune.Shkelja ose mos-zbatimi i ketyre rregullave dhe udhezimeve ,perben shkelje te disiplines ne pune dhe sipas shkalles se shkeljes ngarkon me pergjegjesi punonjesin, i cili ka kryer kete shkelje, (shkeljet trajtohen ne baze te rregullores se brendeshme te kompanise).

- ∑ Punonjesve, mbi bazen e udhezimeve te Kodit te Punes,u eshte vendosur ne dispozicion, prane qendres se punes , kutia e ndihmes se shpejte.

- ∑ 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 .

- ∑ Cdo punonjes i ri nenshkruan deklaraten e pergjegjesive Civile dhe Penale, e cila ngarkon me pergjegjesi direkte, personin qe nxjerr/perdor apo shperndan informacion te

brendeshem te ndermarrjes. Ne fund te ketij dokumenti kerkohet nenshkrimi pasi eshte kuptuar dhe eshte pranuar permbajtja e deklarates.

- 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.

Nder politikat kryesore, perfshihen referencat tek logset e sistemeve/software-ve, apo burimeve te tjera te kompanise.

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.

NISATEL OPERATOR PUBLIK I TELEKOMUNIKACIONEVE
Pavaresia 1200, Vlore, Albania
E-mail: info@nisatel.al;

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 sebashku 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
Pergjegjes Koordinimi	Klodjan Gocllari

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.

Meposhte disa nga trajnimete zhvilluara, shkeputur si fragment nga regjistrat e kompanise per trajnimin dhe hyrjet e reja te punonjesve:

Shkurt 2019 - Mars 2019 - Trajnim per rrjetin fiber, problematikat aktuale,krijimi i konektoreve fundor.

Maj 2019 – Prill 2019 – Trajnim per teknologjite e perdorura ne Nisatel

Shtator 2019 – Tetor 2019 – Trajnim per teknologjine VOIP

Dhjetor 2019- Mediat e Transmetimit, fiber, baker.

NISATEL OPERATOR PUBLIK I TELEKOMUNIKACIONEVE
Pavaresia 1200, Vlore, Albania
E-mail: info@nisatel.al;

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 brendesheme 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 password,(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-Network, te skeduluara dhe te kryera ne orare te pershtetshme per nderhyrje. Me tutje procedurat menaxhuese perfshijne Edge-Network, 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.

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 firewall 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

NISATEL OPERATOR PUBLIK I TELEKOMUNIKACIONEVE
Pavaresia 1200, Vlore, Albania
E-mail: info@nisatel.al;

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 qytetit, jane te lidhura me sallen qendrore te pajisjeve , me minimalisht 2 rruge fizike, kjo per efekt redundance.
3) 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 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)
4) 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, switchet 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:

NISATEL OPERATOR PUBLIK I TELEKOMUNIKACIONEVE
Pavaresia 1200, Vlore, Albania
E-mail: info@nisatel.al;

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.

NISATEL OPERATOR PUBLIK I TELEKOMUNIKACIONEVE
Pavaresia 1200, Vlore, Albania
E-mail: info@nisatel.al;

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 totalteperdoruesveteofru	260	260
>1000ose>5%	*Mesatar*	*Ilarte*
Nerasttenjenumritepanjo hurteperdoruesveteprekur ngaincidentiisigurise,zon agjeografikeeshtrirjessein cidentittesigurise	-	-
>20km²	*Mesatar*	*Ilarte*
Vleresimi Perfundimtari Impaktit:	*Mesatar*	*ILarte*

NISATEL OPERATOR PUBLIK I TELEKOMUNIKACIONEVE
Pavaresia 1200, Vlore, Albania
E-mail: info@nisatel.al;

Deklarata e Aplikimit

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 mesiper.
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		

NISATEL OPERATOR PUBLIK I TELEKOMUNIKACIONEVE
Pavaresia 1200, Vlore, Albania
E-mail: info@nisatel.al;

	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 per palet, 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.	

		ne datacenter. Monitorim 24x7. Alarm automatik me SMS,senore per tymin, lageshtine dhe zhurmat.
	c) Implementim i standarteve të industrisë mbi kontrollet fizike dhe të mjedisit.	I referohemi Manualit mbi Rregullat e Sigurimit Teknik dhe Manuali per parandalimin dhe mbrojtjen nga zjarri
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.	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 Power dhe Gamatronic Power. 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 password vete. Passwordet jane te enkriptuara MD5 ne sistem. Ne sisteme jane gjurmet e nderrimit te passw. 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
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.	pozicionit te punes te cdo punonjesi te kompanise.
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 firewall-et. b) Siguro që të dhënat kritike të sigurisë si password-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 firewall 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
SO 13.3	c) Rishiko dhe përditëso politikën/procedurat për funksionimin e sistemeve kritike, duke marrë në konsideratë incidentet dhe/ose ndryshimet.	Takime me drejtuesit e departamenteve ne baza te pakten 3 mujore per modifikimin rishikimin moduleve te ndryshme te sistemit
SO 14: Ndryshimi i Menaxhimit		
SO 14.	a) Ndiqni procedurat e paracaktuara, kur bën ndryshime në sistemet kritike.	Ndryshimet e procedurave te sistemeve kritike behen sipas vendimeve te posacme.

1		
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.	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	d) procedurat e menaxhimit të rishikimit dhe 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. 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 15.2	Implementimi i politikave / procedurave per menaxhimin e burimeve dhe kontrollin e konfigurimit.	
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	
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.	Guide permbledhese per problematikat kryesore ne rrjet perfshin dhe incidentet e cila behet update vazhdimisht.
SO 17: Procesi i zbulimit te incidenteve		
SO 17.	a) Ngritja e proceseve apo sistemeve për zbulimin e incidentit.	Jane implementuar zgjidhje software qe bejne kontrolle rutine.

NISATEL OPERATOR PUBLIK I TELEKOMUNIKACIONEVE
Pavaresia 1200, Vlore, Albania
E-mail: info@nisatel.al;

1		
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 software/scripte qe monitorojne automatikisht portat e ndryshme te rrjetit dhe raportojne anomali te ndryshme. Vazhdimisht behen kerkime per sisteme/software/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. Datacenter sekondar dyte prane Kinostudio qe mundeson te gjitha sherbimet ne rast shkeputje totale te datacenterit primar
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.	
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	

2	sa me te larte te kapaciteteve per rimekembjene e situates c) Implementimi I kapaciteteve te industrive standarte te rimekembjes se katastrofave ose te perdorin pale te treta (siç jane rrjetet emergjente nacionale)	
SO 20.3	d) Vendosja e nje mekanizmi per mitigimin kapaciteteve per rregullimin e situates e) Kontrollimi dhe updatimi I kapacatiteve en menyre te vazhdueshme te regullt, duek amrre parasysh ndryshimet qe ndodhin, incidentet e meparshme, rezultatet e testeve.	
D7: Monitorimi, Auditimi dhe Testimi		
SO 21: Politikat e Logi dhe Monitorimit		
SO 21.1	a)Imlementimin e monitorimit dhe logeve e sistemeve kritike	Te gjitha sistemet kritike dhe jo kritike ruajne syslog per nje periudhe te pakten 3 mujore. Sistemet kritike te informacionit kane te dhenat te loguara per nje periudhe 2 vjecare dhe me teper.
SO 21.2	b) Implementon politikën e ngjarjeve dhe monitorimin e sistemeve kritike. c) Vendos mjete për monitorimin e sistemeve kritike d) Vendos mjetet për të mbledhur dhe ruajtur shkrimet e sistemeve kritike.	
SO 21.3	e) Vendos mjetet për mbledhjen dhe analizën e të dhënave të monitorimit dhe logot. f) Rishikimi dhe perditesimin i ndodhive dhe monitorimin e politikave / procedurave, duke marrë parasysh ndryshimet dhe incidenteve te shkuara.	
SO 22: Qeverisja dhe Menaxhimi i Riskut		
SO 22.1	a) Veprime dhe backup provë dhe planet emergjente për t'u siguruar që sistemet dhe proceset e punës dhe personeli është i përgatitur për dështimet e mëdha dhe të paparashikuara.	Cdo muaj realiziohen testime duke fikur sistemin/pajisjen primare per tu siguruar qe sistemi/pajisja backup vijon punen automatikisht.
SO 22.2	b) Implementimi i programit për ushtrimin backup dhe planeve emergjente rregullisht, duke përdorur skenare realiste që mbulojnë një gamë të skenarëve të ndryshëm gjatë kohës. c) Sigurohuni që çështjet dhe mësimet e nxjerra nga ushtrimet janë adresuar nga njerëzit përgjegjës dhe se proceset dhe sistemet përkatëse janë përditësuar në përputhje me rrethanat.	

SO 22.3	d) Rishikimi dhe përditësimin e planeve te ushtrimit, duke marrë parasysh ndryshimet dhe incidentet e shkuara dhe të paparashikuara të cilat nuk janë të mbuluara nga programi i veprimit. d) Përfshirja furnizuesit, si dhe palët e tjera të treta, si partnerët e biznesit ose konsumatorët në veprim.	Planet dhe teknikat e emergjences se sistemeve dhe pajisjeve primare/ backup jane ne permiresim te vazhdueshem.
SO 23: Rrjeti dhe testimi i sistemit te informacionit		
SO 23.1	a)Testo rrjetet dhe sistemet e informacionit perpara se ti perdorni ato ose ti lidhni me sistemet egzistuese.	Te gjitha sistemet, pajisjet dhe zgjidhjet software testohen per nje per nje periudhe jo me pak se nje mujore. Pajisjet fundore te klienteve testohen ne kapacitet te plote per nje periudhe jo me pak se 1 javore.
SO 23.2	b) Implemento rregulla dhe procedura per te testuar rrjetin dhe sitemet e informacionit c) Implemento vegla per testime automatike	
SO 23.3	d)Rishikimi dhe azhurnimi i rregullave/procedurat për testim, duke marrë parasysh ndryshimet dhe incidentet e fundit.	
SO 24: Vleresimi i Sigurise		
SO 24.1	a) Siguro qe sistemet kritike tu nënshtrohen sigurisë se canimeve dhe testimin e sigurisë rregullisht, sidomos kur sistemet e reja janë futur dhe ndiqen ndryshimet.	Mbledhje cdo 3 muaj e keshillit teknik te kompanise mbi aspektet e sigurise ne rrjet, ndryshimet dhe objektivat mbi politikat e sigurise. Vendimet jane te detyrueshme per te gjithe departamentet dhe jane objekt auditimi.
SO 24.2	b) Implemento rregulla/procedura për vlerësimin e sigurisë dhe testimin e sigurisë.	
SO 24.3	c) Vlereso efektivitetin e politikave/procedurave për vlerësimin dhe testimin e sigurisë d) Shqyrto dhe korrigjo politikat/procedurat për vlerësimin dhe testimin e sigurisë, duke marrë parasysh ndryshimet dhe incidenteve të shkuara.	
SO 25: Monitorimi i pajtueshmerise – Monitorimi i rregullt sipas ligjit		
SO 25.1	a) Monitoro zbatimin brenda standardeve dhe kërkesave ligjore	Ne organigramen e kompanise eshte percaktuar pozicioni i Auditit te Brendshem, i cili periodikisht monitoron dhe kontrollon zbatimin e procedurave dhe vendimeve te percaktuara dhe te miratuara nga kompania. Auditi ka objektiva te miratuara tremujore ku perfshihet kontrolli i detajuar i cdo departamenti. Sipas rastit, ne fund te kontrollit, Auditi jep vleresimin per permiresim dhe ben njoftimet per rregullim, ose percakton nese duhet bere rishikim dhe ndryshim i procedures. Raporti i Auditmit aprovohet dhe miratohet nga Administratori dhe arkivohet.
SO 25.2	b) Implemento rregulla dhe procedura per monitorimin e rregullt dhe auditimin	
SO 25.3	c)Vlerësoni politikat / procedurat sipas standarteve dhe auditim d) Rishikimi dhe perditesimi i politikave/ procedurat për pajtim dhe të auditimit, duke marrë parasysh ndryshimet dhe incidenteve të fundit	

NISATEL OPERATOR PUBLIK I TELEKOMUNIKACIONEVE
Pavaresia 1200, Vlore, Albania
E-mail: info@nisatel.al;

Kodi i Mbrojtjes, Përpunimit, Ruajtjes dhe Sigurisë së të Dhënave Personale

NISATEL OPERATOR PUBLIK I TELEKOMUNIKACIONEVE
Pavaresia 1200, Vlore, Albania
E-mail: info@nisatel.al;

Kodi i Mbrojtjes, Përpunimit, Ruajtjes dhe Sigurisë të të dhënave Personale të Nisatel sh.p.k

Nisatel Sh.p.k
L. Pavaresia , Rr.Nermin Vlora , Pall 1200
Vlorë, Albania.

Përmbledhje

NISATEL OPERATOR PUBLIK I TELEKOMUNIKACIONEVE
Pavaresia 1200, Vlore, Albania
E-mail: info@nisatel.al;

1.Hyrje

Mbi administrimin, përdorimin dhe shfrytëzimin sa më efektiv të të dhënave personale , si dhe për sigurimin e tyre nga vjedhjet, dëmtimet apo veprime të tjera, për udhëzimin e punonjësve dhe për përcaktimin e përgjegjësive të tij/saj hartohet ky Kod, me përmbajtjen e mëposhtme:

Përkufizime

Departamenti i Burimeve Njerëzore - përcakton , njësinë e ngritur / formuar pranë kompanisë e cila administron procesin e njohjes , pranimit të këtij kodi nga departamentet të cilat kanë lidhje të drejtëpërdrejte me manaxhimin, rruajtjen , ekspozimin e të dhënave personale në bazën e të dhënave të kompanisë.

Punonjësit e perfshirë në informacione konfidenciale / Strukturat e shoqerisë Nisatel – I referohet personave të cilët janë punësuar pranë kompanisë Nisatel, dhe kanë akses në bazën e te dhënave konfidenciale qe i nënshtrohen kushtëve të këtij Kodi.

"Kontrollues" – u referohet strukturave Audituese, Zyra e Standarteve dhe Procedurave , Burimet Njerëzore, të cilët angazhohen në mënyrë të drejtëpërdrejtë në kontrollin e zbatueshmërisë së këtij kodi , si dhe trajnimin për qëllimin dhe mënyrën e përpunimit të të dhënave personale , në përputhje me ligjet dhe aktet nënligjore, si dhe për përmbushjen e detyrimeve të përcaktuara në këtë ligj.

"Perpunues" – Për efekt të këtij Kodi janë departamenti si Support, Teknika, Dyqanet, Network Operations Center, Autoriteti i Administrimit te Rrjetit përvec punonjësve të kontrolluesit, që përpunojnë të dhëna për vetë kontrolluesin.

"Marrës" është cdo person fizik ose juridik, autoriteti publik, agjenci apo ndonjë organ tjetër të cilit i janë dhënë të dhënat e një pale të tretë ose jo.
Termat e tjerë të përdorur në zbatimin e këtij Kodi do të kenë të njëjtin kuptim si në ligjin nr. 9887, dt.10.03.2008 "Për mbrojtjen e të dhënave personale", [1] i ndryshuar.

Nisatel Sh.p.k i trajton me seriozitet cdo shkelje të këtij Kodi.

[1] Aneksi 1: Bashkëngjitet këtij Kodi

1.1Qëllimi i Kodit

Ky Kod është i zbatueshëm për njësitë , divizionet, filialet , e Nisatel sh.p.k, përfshirë dhe drejtorët , menaxherët dhe punonjësit e tyre, të cilët menaxhojnë në mënyrë të drejtëpërdrejtë të dhënat personale të klientëve Nisatel sh.p.k.

Referimet si "punonjës" ose punonjësit përfshijnë të gjithë drejtorët, manaxheret dhe punonjësit e Nisatel, përfshirë agjentët e jashtëm të cilët kanë lidhje të drejtëpërdrejtë me këto të dhëna të shoqërisë. Ky Kod ka për qëllim të përcaktojë parimet e përgjithshme dhe masat organizative dhe tekniike për mbrojtjen , ruajtjen sigurinë dhe administrimin e të dhënave personale. Ajo Zbatohet për të gjitha të dhënat e perpunuara nga Nisatel në përputhje me "Ligjin për mbrojtjen e të dhënave personale".
Përpunimi i të dhënave bëhet në përputhje me Kushtetutën, Ligjin per Mbrojtjen e të Dhënave Personale, si dhe me Misionin e Nisatel, duke respektuar të drejtat dhe liritë e njeriut.

1.2. Objekti i Kodit

Objekti i këtij Kodit është përcaktimi i procedurave organizative e teknike, masave për mbrojtjen e të dhënave personale dhe sigurisë, ruajtjes dhe administrimit të të dhënave personale nga strukturat e Nisatel Sh.p.k

1.3 Përputhshmeria me Kodin

Cdo punonjës i perfshirë në informacionin konfidencial vepron në përputhje me përcaktimet e këtij kodi në cdo rast të verifikimit të ngjarjeve të përshkruara dhe të rregulluara me këtë Kod.

1.4. Administrimi i Kodit

Kodi i Mbrojtjes, Përpunimit, Ruajrjes dhe Sigurisë së të Dhënave Personale" administrohet nga Departanenti i Burimeve Njerëzore. Kjo njësi ka përgjegjësi për trajtimin e këtij Kodi me punonjësit e shoqërisë si dhe administrojnë procedurën e njohjes me kodin për punonjës e rinj, si dhe nënshkrimin e deklaratës së pranimit të këtij Kodi nga punonjësit.

Nëse punonjësit kanë paqartësi në lidhje me zbatimin e këtij Kodi ose me kuptimin e përcaktimeve në këtë Kodit të Mbrojtjes, Perpunimit, Ruajtjes dhe Sigurise së të Dhënave Personale, ata janë të detyruar të kërkojnë shpjegime pranë Departamentit të Burimeve Njerëzore.

Asnjë veprim i kryer në shkelje të këtij Kodi, nga ndonjë punonjës, nuk është i justifikuar për shkak se punonjësi mund të ketë patur paqartësi në zbatimin e përcaktimeve këtu në këtë Kod.

Raportimi dhe njoftimi i shkeljeve, administrohet nga Audit, Departamenti të Burimeve Njerezore në bashkëpunim me Departamentin Juridik.

1.5 Fusha e zbatimit

Ky Kod zbatohet për përpunimin e të dhënave personale plotësisht ose pjesërisht, nëpërmjet mjeteve automatike, dhe me mjete të tjera që mbahen në një sistem arkivimi apo kanë për qëllim të formojnë pjesë të sistemit të arkivimit pranë shoqerise Nisatel Sh.p.k.

2 PERPUNIMI 1 TE DHENAVE PERSONALE

2.1 Mbrojtja e të dhënave personale

Cdo punonjës i strukturave të Nisatel, që merret me përpunimin e të dhënave personale te subjekteve, detyrohet të zbatojë kërkesat e neneve 2 dhe 5 të ligjit"Per mbrojtjen e të dhënave personale", i ndryshuar, si më poshtë:

- ∑ Respektimin e parimit për përpunimin e ligjshëm të të dhënave personale, duke respektuar dhe garantuar të drejtat dhe lirite themelore të njeriut dhe, në vecanti, të drejtën e ruajtjes së jetës private;
- ∑ Kryerjen e përpunimit ne mënyrë të drejtë dhe të ligjshme;
- ∑ Grumbullimin e të dhënave personale per qëllime specifike, të përcaktuara qartë, e legjtime dhe kryerjen e përpunimit të tyre në përputhje me këto qëllme;
- ∑ Të dhënat qe përpunohen janë të mjaftueshme, të lidhen me qëllimin e përpunimit dhe të mos e tejkalojnë këtë qëllim;
- ∑ Të dhënat janë të sakta nga ana faktike, dhe kur është e nevojshme, të bëhet përditësimi e kryerja e cdo veprimi për të siguruar që të dhënat e pasakta e të parregullta të fshihen apo të ndryshohen;
- ∑ Te dhënat mbahen në atë formë, që të lejojnë identifikimin e subjekteve të të dhënave për një kohë, por jo më tepër sesa është e nevojshme për qellimin, për të cilin ato janë grumbulluar ose përpunuar me tej.

2.2 Qellimi i Përpunimit

Cdo punonjës i Nisatel mund t'i përdorë të dhënat personale vetëm për kryerjen e detyrave të parashikuara nga ligji dhe në përputhje me aktet ligjore e nënligjore që rregullojnë mënyrën e përpunimit të të dhënave personale, jashtë këtyre kushteve, përben shkelje.

2.3. Kriteret e perpunimit të të dhenave personale

Punonjesit e cdo strukture të Nisatel që përpunojnë të dhëna personale të subjekteve, bazohen në kriteret e përcaktuara në nenin 6 të ligjit"Per mbrojtjen e të dhënave personale".

Te dhënat personale përpunohen vetëm:

- ∑ për të mbrojtur interesat jetikë të subjektit të të dhënave;
- ∑ per përmbushjen e një detyrimi ligjor;
- ∑ për kryerjen e një detyre ligjore me interes publik ose ushtrimin e një kompetence të kontrolluesit ose të një pale të tretë.
- ∑ për ndjekjen e interesave legjitimë ose të një pale të tretë, së cilës i janë përhapur të dhënat, përvec kur këta interesa mbizotërojnë mbi interesat për mbrojtjen e të drejtave dhe të lirive themelore të subjektit të të dhënave.

Sa më siper keto te dhena perpunohen me urdher te Administratorit te shoqerise Nisatel,

2.4 Përpunim i të dhenave sensitive

Përpunimi i të dhënave sensitive nga cdo punonjës kryhet në përputhje me kriteret e përcaktuara në nenin 7 të ligjit "Për mbrojtjen e të dhënave personale", i ndryshuar.

2.5 Transferimi nderkombetar i te dhenave

Në rast të kryerjes së transferimit ndërkombëtar të të dhënave personale cdo punonjës i shoqerisë Nisatel, zbaton parashikimet e nenit 8 dhe 9 të ligjit "Për mbrojtjen e të dhënave personale" dhe aktet nënligjore te dala në zbatim të tij.

1. Të dhënat dhe informacionet, mund t'u komunikohen institucioneve homologe të shteteve të tjera në bazë të marrëveshjes së bashkëpunimit, me kusht që në shtetin kërkues këto të dhëna dhe informacione të trajtohen dhe të ruhen, në përputhje me legjislacioriin për mbrojtjen. e të dhënave.
2. Të dhënat dhe informacionet e përmendura në paragrafin e mësipërm trajtohen vetëm nga autoritetet përkatëse të shtetit marrës.
3. Transferimi i të dhënave të cilat janë "shumë sekrete" nuk realizohet nëpërmjet linjave të komunikimit elektronik.
4. Transferimi i të dhënave të cilat janë"sekrete"realizohet nëpërmjet linjave të komunikimit elektronik, te sigurta dhe rregullohen nga marrveshe te veganta, (NDA, Marrveshje lnterkoneksioni).

3. TE DREJTAT E SUBIEKTIT TE TE DHENAVE

3.1. Zbatimi i të drejtave të subjekteve të të dhënave personale

1. Përhapja ose komunikimi i të dhënave personale kryhet në përputhje me qëllimin për të cilin janë grumbulluar këto të dhëna.
2. Cdo person ka të drejtë që të njihet me të dhënat personale të përpunuara nëpërmjet një kërkese me shkrim.
3. Cdo institucion që përpunon të dhëna personale është i detyruar që në bazë të ligjit nr. 9887, datë 10 03.2008 "Për mbrojtjen e të dhënave personale", të zbatojë këto të drejta të subjekteve të të dhënave personale:

    a) të drejtën për akses;
    b) të drejtën për të kërkuar korrigjimin ose fshirjen;
    c) vendimmarrjen automatike;
    d) të drejtën për të kundërshtuar;
    e) të drejtën për tu ankuar;
    f) të drejtën për kompensimin e demit.

4. Kërkesat permbajnë të dhëna të mjaftueshme për të vërtetuar identitetin e kërkuesit. Kontrolluesi, brenda 30 ditëve nga data e marrjes së kërkesës, informon subjektin e të dhënave ose i shpjegon atij arsyet e mosdhënies së informacionit.

3.2. Kerkesat per informacion

Kërkcsën për informacion mund ta bëjë:

- ∑ Vetë personi ,
- ∑ Përfaqësuesi ligjor i pajisur me autorizimin përkatës;

- ∑ Persona të tjerë të cilët megjithëse nuk kanë interes të drejtpërdrejtë, provojnë se kanë një interes të ligjshëm për të marrë dijeni në lidhje me këto të dhëna dhe që përputhet me qëllimin e grumbullimit të këtyre të dhënave;
- ∑ Prindi ose kujdestari kur :

    a) Fëmija nuk ka zotësi të plotë për të vepruar,
    b) Prindi është duke vepruar në interes të fëmijës.

Përgjigja në cdo rast dërgohet në adresën e kërkuar nga vetë kërkuesi.

4. SIGURIA E TE DHENAVE PERSONALE

4.1Masat për Sigurinë e të dhënavë

Shoqëria Nisatel merr masa organizative dhe teknike të përshtatshme për të mbrojtur të dhënat personale nga shkatërrime të paligjshme, aksidentale, humbje aksidentale, për të mbrojtur aksesin ose përhapjen nga persona të paautorizuar, vecanërisht kur përpunimi i të dhënave bëhet në rrjet, si dhe nga cdo formë tjetër e paligjshme përpunimi.

Masat e vecanta të sigurisë:

- Përcaktohen funksionet ndërmjet njësive organizative dhe perpunuesve për përdorimin e të dhënave;
- Përdorim te dhënat vetem me urdhër të njësive organizative të autorizuar;
- Udhëzojme perpunuesit, pa përjashtim,për detyrimet që kanë, në përputhje me ligjin për mbrojtjen e të dhënave personale dhe rregulloret e brendshme për mbrojtjen e të dhënave, përfshirë edhe rregulloret për sigurinë e të dhënave;
- Ndalojmë hyrjen e personave të paautorizuar në mjediset e kontrolluesit ose përpunuesit të të dhënave.
- Aksesi në, të dhënat dhe programet, bëhet vetëm nga personat e autorizuar, ndalohet përdorimi nga persona të paautorizuar;
- Vënia në punë e pajisjeve të përpunimit të të dhënave bëhet vetem me autorizim të Administratorit te shoqerise dhe cdo mjet sigurohet me masa parandaluese ndaj venies së autorizuar në punë;
- Regjistrohet dhe dokumentohen modifikimet, korrigjimet, fshirjet, transmetimet, përditësimet, etj.
- Sa herë që punonjësit e shoqerisë largohen nga vendi i tyre i punës, ata mbyllin kompjuterat e tyre, dollapët, kasafortat dhe zyrën, ne të cilat janë ruajtur të dhënat personale ;
- Nuk leiojme largimi nga mjediset e punes kur ka të dhëna të pambrojtura në tavoiinë, dhe ndodhet në prani të personave të cilët nuk janë të punësuar ne shoqerinë Nisatel;
- Nuk mbajme në monitorim të dhëna personale, kur është i pranishem një person i pautorizuar dhe sidomos në vende jo publike;
- Nuk nxjerrim jashtë zyrës, në asnjë rast, kompjutera, laptop, flash/USB apo pajisje të tjera që përmbajne të dhëna personale dhe nuk lihen ato ne vende të pasigurta, pa u siguruar për fshirjen apo shkaterrimin e të dhënave më parë;

- Të dhenat i mbrojmë duke verifikuar identitetin e përdoruesit dhe duke i lejuar akses vetëm individëve të autorizuar.
- Udhëzimet.për përdorimin e kompjuterit, ruhen në mënyrë të tillë qe ato të mos jenë të aksesueshme nga persona te paautorizuar;
- Kryejme hyrjet dhe daljet duke përdorur fjalekalime personale në fillim të aksesit të tyre në të dhënat e mbrojtura, të ruajtura në bazat e të dhenave;
- Regjistrimi i Kontrolluesve dhe i përdoruesve kryhet me funksionalitet e fjalëkalimeve për hyrjen e të dhënave.
- Fjalekalimet ciiësohen sekrete dhe janë vetjake;
- Ne dokumente që përmbajnë të dhëna të mbrojtura, sigurojme shkatërrimin e materialeve ndihmëse, (p.sh. provat apo shkresat, matricat, llogaritjet, diagrame dhe skica) të përdorura ose të prodhuara per krijimin e dokumentit;
- Të dhënat e dokumentuara nuk përdoren per qëllime të tjera, që nuk janë në përputhje me qëllimin e grumbullimit.
- Ndalojme cdo përpunim të të dhenave të regjistruara në dosje per një qëllim të ndryshëm nga e drejta per të hedhur të dhëna. Përjashtohet nga ky rregull rasti kur të dhenat përdoren per parandalimin ose ndjekjen e një vepre penale.
- Ruajme dokumentacionin e të dhënaive per aq kohë sa është i nevojshëm për qëllimin, për të cilin është grumbulluar.
- Niveli i sigurisë eshte i sigurt me natyren e përpunimit të të dhënave personale.

4.2. Mbrojtja e ambjenteve

> Ambientet në të cilat do të përpunohen të dhënat personale mbrohen nga masa organizative, fizike dhe teknike që të parandalojnë aksesin e personave të paautorizuar në mjediset dhe aparaturat me të cilat do të përpunohen të dhënat personale.

Zbatimi i masave të sigurimit bëhet në përputhje me nivelin e sigurisë së të dhënave dhe informacionit të administruar, si dhe treguesit e nivelit të rrezikut që mund të vijë nga ekspozimi i paautorizuar i informacionit të ruajtur.

Në ambientet ku përpunohen të dhëna personale zbatohen këto masa sigurie:

- Ndalojme hyrjen e personave të paautorizuar.
- Personat që futen në këto ambjete pajisen me autorizimin përkatës.
- Ambientet e hyrjes, survejohen me kamera gjatë 24 orëve.
- Vec masave dhe sistemeve të tjera të mbrojtjes, vendosen pajisje dhe sisteme të sigurimit elektronik (sisteme sinjalizimi, telekamera, etj).

- Ambientet pajisen me dollap hekuri, të sigurta për mbrojtjen e dosjeve nga dëmtimi i tyre, me kasaforta e brava automatike me celësa dhe drynë të vecantë nga ata të përdorimit të zakonshëm dhe vulosen me dyllë/parafinë ose plastelinë.
- Dyert të jenë të blinduara dhe dritaret të sigurta.
- Sigurohet mbikëqyrje e vazhdueshme, ditën dhe natën me roje fizike.

4.3. Drejtoritë Teknike

Drejtoritë Teknike disponojnë kopje dhe një dublikatë të të gjitha të dhënave dhe software që mbahen ose ruhen në server qëndror. Një kopje dublikatë mbahet në një vend ose ambient të ndryshëm nga godina në të cilën ndodhet shoqeria. Numri dhe forma e kopjeve shtesë të dokumcnteve, mjeteve të tjera të komunikimit në të cilat ruhen përcaktohen nga departamenti përkatës për cdo dokument.

4.4. Mbrojtja e të dhënave elektronike

Pajisjet elektronike për përpunimin e të dhënave dhe informacioneve përdoren vetëm për kryerjen e detyrave të përcaktuara në Kod. Këto pajisje përdoren vetëm nga punonjës të

autorizuar, të trajnuar më parë për përdorimin e tyre. Trajnimi i personelit që merret me përpunimin automatik të të dhënave bëhet nga Drejtoritë Teknike.

Për cdo gabim apo defekt në sistemet/databaset njoftohet administratori i sistemit, i cili mbi bazën e kërkesës bën rregullimin përkatës.

4.5. Mbrojtja software

Për secilin program Departamenti/Drejtoritë Teknike mund të përcaktojë:

1. Kush do të ketë akses per fshirje, kopjojë ose ta ndryshojë atë;
2. Ku ruhet kopja e programit dhe kush është përgjegjës për mbajtjen e përditësuar.

4.6. Fjalëkalimet

Shumë nga aplikimet dhe sistemet kompjuterike jane të mbrojtura me fjalëkalim. Për arsye sigurie, këto fjalekalime herë pas here dryshohen (*cdo 3 muaj ose cdo 6 muaj*). Disa rregulla që aplikojmë mbi perdorimin dhe vendosjen e fjalëkalimeve:

- ∑ Fjalëkalimi nuk ndahet me persona të tjerë brenda apo jashtë shoqerise. Punonjësit janë përgjegjes per ruajtjen dhe mos shpërndarjen e këtij informacioni.

- ∑ Gjatë vendosjes se fjalëkalimit, vendoset nje fjalë apo frazë që mund të mbahet mend lehtesisht, por jo dicka që identifikon lehtësisht, si psh: emri apo adresa.
  Ne perdorim fjalkalime të forte. Një fjalëkalim i forte konsiderohet ai që përmban shkronja të mëdha dhe të vogla, numra dhe karaktere pikësimi.

4.7. Monitorimi dhe regjistrimi i aksesit per te dhenët personale

Hyrja tek të dhënat dhe informacionet u nenshtrohet normave të vecanta të sigurisë për ruajtjen e paprelfshmërisë dhe per përditësimin e tyre. Sistemi është i ndërtuar në mënyre të tillë qëvërteton identitëtin e përdoruesit. Kjo kërkon që serveri qendror të njohëcdo perdorues terminalist dhe cdo përdorues nëpërmjet programeve të vecanta. Ky sistem mundëson identifikimin e vazhdueshëm të përdoruesit nëcdo kohë, në një terminal te caktuar, vendin e punes ose pajisje të tjera për periudhën per të cilën të dhënat specifike jane ruajtur.

Perdoruesit njihen me llojin e të dhenave në regjistrimet e përditshme dhe kohën e ruajtjes se këtyre regjistrimeve.

Regjistrimet e perditshme administrohen nga Departamenti Netëork Operation Centers, i cili eshte përgjegjës per mbrojtjen e të dhenave, përcakton përmbajtjen e te dhenave të regjistrimeve ditore dhe kohën e ruajtjes së te dhënave personale. Periudha e ruajtjes së regjistrimit të të dhenës ose

informacionitështë e barabartë me periudhën e ruajtjes së dokumentit shkresor që përmban këtë dhëne ose informacion. Me kalimin e këtij afati këto të dhena arkivohen ose asgjësohen. Njohja dhe regjistrimi i përpunuesve terminalistë dhe i përdoruesve kryhet me përdorimin e fjalëkalimeve per hyrjen në bazën e të dhënave. Fjalëkalimet cilësohen sekrete dhe janë vetjake.

Hyrja në të dhenat dhe informacionet lejohet ose pengohet me programe të vecanta elektronike. Kontrolli dhe dokumentimi i aksesit në të dhëna dhe informacione realizohet nga personat përgjegjës për mbrojtjen e të dhënave.

4.8. Mbrojtja e dokumunteve

Dokumentat e klasifikuar dhe mjetet e tjera të komunikimit në të cilat mbahen të dhëna personale shënohen me një lloj sekretimi dhe një nivel i caktuar kofidencialiteti.

4.9. Dokumente sekrete

Kur krijohen dokumente që përmbajnë të dhëna që kosiderohen “shumë sekrete" ose “sekrete”, në dokumentin origjinal përcaktohen të dhëna lidhur me numrin e kopjeve që i janë bërë dokumentit (të shkruar, printuara, vizatuara, duplikuara) dhe kujt i janë dhënë. Cdo kopje ka numrin e vet të regjistrimit.

Nëqoftëse materiali i përmendur në paragrafin e mësipërm përbëhet nga disa faqe ose lidhet me dokumente të tjera ose ka pjesë të tjera përbërëse atëherë cdo faqe sigurohet nga një nivel i caktuar kofidencialiteti ose të sigurohet që faqet dhe lidhjet të mos hiqen ose grisen pa një paralajmërim të mëparshëm.

Kur të dhënat konfidenciale prezantohen në një ekran ose në sisteme të tjera mediatike, niveli i fshehtësisë ose konfidencialitetit tregohet në cdo pjesë (ilustrime, piktura, vrojtime, parashikime) të prezantimit (paraqitjes).

4.10. Rruajtja e dokumentave sekretet

Dokumentet që mbajnë të dhëna që janë “shumë sekrete” ose “sekrete" kycen në njësi prej hekuri teknikisht të sigurta, ose të mblidhen në një pllakë hekuri të kycur dhe e siguruar nga një kod, megjithëse ato janë drejtpërdrejtë të kontrolluara nga një punonjës që i nevojiten dokumente përkatëse (të caktuara) për punën e tij.

Celësat e këtyre njësive mbrohen nga nëpunësit në kontakt të ngushtë fizik, në vendet e tyre ose në zarfe të vulosura nga zyra kryesore. Celësa të tjerë mbahen nga zyra kryesore e drejtuesit të njësisë organizative përkatëse. Në qoftë se një celës humbet, kyci ndryshohet, ndryshimi i këtij të fundit, shoqërohet me proces-verbal përkatës.

Në vendet ku mbrohen dokumentet e përmendura në paragrafin e mësipërm hyjnë vetëm punonjës që krijojnë, përdorin, mbrojnë ose sigurojnë këto dokumente.

Materialet përgatitore të përdorura për krijimin e dokumenteve që përmbajnë të dhëna “shume sekrete" ose “sekrete" (matrica, llogaritje, diagrama, skica, cështje ose printime skarco) shkatërrohen nga një komision dëshmitarësh ose vëzhguesish. Mënyra që përdoret për shkatërrimin e tyre eshte që të sigurojë pa lexueshmërinë dhe të pëngojë riprodhimin e përmbajtjes.

Komisioni i vëzhguesve mban një raport për shkatërrimin e materialit të përmendur në paragrafin e mësipërm i cili firmoset nga të gjithë anëtarët e komisionit. Komisioni i vëzhguesve përbëhet nga tre anëtarë të caktuar nga eprori i njësisë përkatëse. Procedura që përdoret per shkatërrimin e dokumenteve që përmbajnë të dhëna personale përcaktohet nga eprori përkatës.

E njëjta procedure perdoret edhe për shkatërrimin e të dhënave dhe dokumenteve dhe mjeteve të tjera të komunikimit koha e përdorimit të të cilave ka mbaruar.

4.11. Dublikata e programeve

Dublikata e programeve me të dhëna që përdoren në rastin e fatkeqësive natyrore ose në raste të gjendjes së jashtëzakonshme ose gjendje lufte ruhen në vende që ndodhen jashtë zyrës kryesore të njësisë organizative perkatëse. Mënyra e krijimit, shumëfishimit dhe ruajtjes së

këtyre dublikatave përcaktohet në mënyrë të vecantë për cdo dokument, në përputhje me rregullat e ruajtjes dhe garantimit të tyre, të vendosura nga njësia organizative përkatëse dhe me rregullat e zbatueshme në rastin e fatkeqësive natyrore.

Në qoftë se një dokument me të dhëna konfidenciale humbet ose zhduket, nëpunësi kompetent ka per detyrë të informojë menjëherë eprorin e tij dhe te marrë cdo masë që vlerësohet e domosdoshme për të përcaktuar rrethanat në të cilat ka humbur dokumenti si dhe për eliminim e pasojave të dëmshme.

5. DISPOZITA PERFUNDIMTARE

5.1. Masat administrative

Punonjës i cili shkel detyrën per të mbrojtur të dhënat personale është përgjegjës per thyerje të disiplinës, rregullave, dhe detyrimeve në veprimtarinë e punës së tij. Në qoftë se veprimet e tyre nuk përbëjnë vepër penale ndaj tyre merren masa administrative dhe disiplinore.

5.2. Mbikeqyrja e masave dhe procdeurave mbrojtëse

Mbikëqyrja e implementimit të rregullave për mbrojtjen e të dhenave personale per respektimin normave të sigurisë, për mbrojtjen e të dhënave të automatizuara kunder prishjes së tyre aksidentale ose të paautorizuar, si dhe kundër hyrjes, ndryshimit dhe përhapjes së paautorizuar të tyre realizohet nga Audit i cili mbikëqyr mbrojtjen e të dhënave respektive.

5.3. Konfidencialiteti për përpunimin e të dhënave

Cdo punonjës që përpunon të dhëna apo vihet në dijeni me të dhënat e përpunuara nuk mund ti bëjë të njohur përmbajtjen e këtyre të dhënave personave të tjerë. Ai detyrohet të ruajë konfidencialitetin dhe besueshmërinë edhe pas përfundimit të funksionit.

Cdo person që vepron nën autoritetin e kontrolluesit, nuk duhet t'i përpunojë të dhënat personale, tek të cilat ka akses, pa autorizimin e kontrolluesit, përvecse kur detyrohet me ligj.

5.4. Detyrimi per bashkepunim

Strukturat teknike janë të ndërgjegjshëm për detyrimin që kanë për të bashkëpunuar me kontrolluesit dhe për ti siguruar të gjithë informacionin që ai kërkon për përmbushjen e detyrave, pasi Kontrolluese ka akses në sistemin e kompjuterave, në sistemet e arkivimit, që kryejnë përpunimin e të dhënave personale dhe në të gjithë dokumentacionin, që lidhet me përpunimin dhe transferimin e tyre, për ushtrimin e të drejtave dhe të detyrave që i janë ngarkuar me ligj.

5.5. Detyrimi per zbatim

Të gjithë aktet ligjore të Kontrolluesit janë të detyrueshme për zbatim nga strukturat e shoqerise Nisatel sh.p.k.

Cdo punonjës që merret me përpunimin e të dhënave personale është i ndërgjegjshëm se përpunimi i të dhënave personale në kundërshtim me kërkesat e ligjit "Për mbrojtjen e të dhënave personale" përbën kundërvajtje administrative dhe dënohet me gjobë.

5.6. Sanksione

Ky Kod është pjesë e rregullores së brendshme dhe mosrespektimi i kërkesave të saj përbën shkelje të disiplinës në punë dhe ndëshkohen sipas legjislacionit në fuqi.

5.7. Përvctësimi i Përmbajtjes se Kodit

Cdo punonjes ka detyrimin të lexojë me kujdes të gjithë përmbajtjen e këtij Kodi dhe të kuptojë qartësisht përgjegjësitë që ai mban në rastin e mosrespektimit të përcaktimeve të këtij Kodi.

Nënshkrimi i këtij Kodi nga ana punonjesit tregon se ai i kupton dhe se i ka të qarta të gjitha përgjegjësitë financiare, civile dhe penale që rrjedhin prej zbatimit të kushteve të përcaktuara në këtë Kod.

5.8. Raportimi i Shkeljeve

Raportimi i shkeljeve është një veprim që nxitet dhe mirëpritet gjatë zbatimit të këtij Kodi. Cdo punonjës i shoqërisë është i detyruar të njoftojë dhe raportojë menjëherë verifikimin e ndonjë ngjarje që bie ndesh me përcaktimet e këtij Kodi.

Nëse një punonjës është i pranishëm gjatë ndodhisë s ngjarjes që bie ndesh me përcaktimet c këtij Kodi, dhe nuk vepron Sig përshkruhet këtu në këtë Kod, është njësoj përgjegjës për veprimet e kryera nga shkelësi përkatës. ’

Shkeljet e këtij Kodi mund të raportohen në mënyrë të fshehtë ose të hapur në adresat e kontaktit si më poshtë:

- Audit i Brendshëm
- Burimet Njerëzore
- Drejtori i Departamentit
- Zv. Dr. Ekzekutiv i shoqreisë Dr. Ekzekutiv i shoqerisë

Punonjësi ka të drejtën e ruajtjes së fshehtësisë së raportimit të kryer prej tij.

6. Veprimet Disiplinore

Veprimet disiplinore të përcaktuara në këtë Kod janë në përputhje me parimet bazë të funksionimit të shoqërisë tonë, dhe ato garantojnë zbatimin e këtij Kodi.

6.1. Procedurat e Trajtimit të Shkeljeve

Veprimet disiplinore ndërmerren në përputhje me procedurën e trajtimit të shkeljeve, e cila administrohet nga Auditi i Brendshëm.

6.2. Pranimi i Veprimeve Disiplinore

Veprimet disiplinore ndërmerren kur punonjësi shkel përcaktimet e këtij Kodi. Shkeljel e kryera nga punonjësi verifikohen nga manaxherët e tyre, nga Audit i Brendshëm, nga personeli i Drejtorisë së Kontrollit, ose nga personeli i Departamentit të Burimeve Njerëzore. Shkeljet e verifikuara i paraqiten punonjësit, i cili duhet të pranojë procedurën dhe dokumentet e rezultuara nga veprimet disiplinore të ndërmarra ndaj tij. Nëse punonjësi ka kundërshtime në lidhje me masat e marra ndaj tij, si rrjedhim i veprimeve disiplinore, atëherë ai duhet të paraqesë një kërkesë apelimi pranë Departamentit të Burimeve Njerëzore. Kërkesa e apelimit mund të paraqitet brenda 30 ditësh nga data e marrjes së vendimit disiplinor.

Aneksi 1: Ligjin nr. 9887, datë 10.03.2008 “Per mbrojtjen e të dhënave personale”

Aneksi 2: Deklarata e Konfidencialitetit të Mbrojtjes, Perpunimit, Ruajtjes dhe Sigurise së të Dhënave Personale.

Aneksi 3: Inventari i Shkeljeve te te dhenave Personale

Aneksi 4: Certifikata ISO 27001:2013

NISATEL OPERATOR PUBLIK I TELEKOMUNIKACIONEVE
Pavaresia 1200, Vlore, Albania
E-mail: info@nisatel.al;

Aneks 1 : Ligjin nr. 9887, datë 10.03.2008 "Per mbrojtjen e të dhënave personale"

LIGJ
Nr. 9887, datë 10.03.2008, ndryshuar me ligjin Nr. 48/2012

"PËR MBROJTJEN E TË DHËNAVE PERSONALE"

Në mbështetje të neneve 78 dhe 83 pika 1 të Kushtetutës, me propozimin e Këshillit të Ministrave,

KUVENDI I REPUBLIKËS SË SHQIPËRISË
VENDOSI:

KREU I
DISPOZITA TË PËRGJITHSHME

Neni 1
Objekti

Ky ligj ka për objekt përcaktimin e rregullave për mbrojtjen dhe përpunimin e ligjshëm të të dhënave personale.

Neni 2
Parim i përgjithshëm

Përpunimi i ligjshëm i të dhënave personale bëhet duke respektuar dhe garantuar të drejtat dhe liritë themelore të njeriut dhe, në veçanti, të drejtën e ruajtjes së jetës private.

Neni 3
Përkufizime

Në këtë ligj termat e mëposhtëm kanë këto kuptime:

1. "Të dhëna personale" është çdo informacion në lidhje me një person fizik, të identifikuar ose të identifikueshëm, direkt ose indirekt, në veçanti duke iu referuar një numri identifikimi ose një

a më shumë faktorëve të veçantë për identitetin e tij fizik, fiziologjik, mendor, ekonomik, kulturor apo social.

2. "E dhënë gjyqësore" është çdo e dhënë lidhur me vendimet në fushën e gjykimeve penale, civile, administrative apo me dokumentimet në regjistrat penalë, civilë, ato të dënimeve administrative etj.

3. "E dhënë anonime" është çdo e dhënë, që në origjinë ose gjatë përpunimit, nuk mund t'i shoqërohet një individi, të identifikuar ose të identifikueshëm.

4. "Të dhëna sensitive" është çdo informacion për personin fizik, që ka të bëjë me origjinën e tij, racore ose etnike, mendimet politike, anëtarësimin në sindikata, besimin, fetar apo filozofik, dënimin penal, si dhe të dhëna për shëndetin dhe jetën seksuale.

5. "Kontrollues" është çdo person fizik ose juridik, autoritet publik, agjenci apo ndonjë organ tjetër që, vetëm apo së bashku me të tjerë, përcakton qëllimet dhe mënyrat e përpunimit të të dhënave personale, në përputhje me ligjet dhe aktet nënligjore të fushës, dhe përgjigjet për përmbushjen e detyrimeve të përcaktuara në këtë ligj.

6. "Subjekt i të dhënave personale" është çdo person fizik, të cilit i përpunohen të dhënat personale.

7. "Përpunues" është çdo person fizik ose juridik, autoritet publik, agjenci apo ndonjë organ tjetër që përpunon të dhëna personale në emër të kontrolluesit.

8. "Sistem arkivimi" është çdo grup i strukturuar i të dhënave personale, të cilat janë të aksesueshme në bazë të kritereve specifike, të centralizuara, të decentralizuara ose të shpërndara në një bazë, funksionale ose gjeografike.

9. "Mjete përpunimi" janë mjetet automatike, gjysmautomatike dhe mekanike që përpunojnë të dhëna personale.

10. "Instrumentet elektronike" janë kompjuteri, programet kompjuterike dhe çdo mjet, elektronik ose automatik, me të cilat bëhet përpunimi.

11. "Tregtim i drejtpërdrejtë" është komunikimi me çdo mjet dhe mënyrë i materialit reklamues, duke përdorur të dhënat personale të personave fizikë ose juridikë, të agjencive ose njësive të tjera, me ose pa ndërmjetësim.

12. "Përpunim i të dhënave personale" është çdo veprim ose grup veprimesh, të cilat janë kryer mbi të dhënat personale, me mjete automatike ose jo, të tilla si mbledhja, regjistrimi, organizimi, ruajtja, përshtatja ose ndryshimi, rikthimi, konsultimi, shfrytëzimi, transmetimi, shpërndarja ose ndryshe duke vënë në dispozicion, shtrirja ose kombinimi, fotografimi, pasqyrimi, hedhja, plotësimi, seleksionimi, bllokimi, asgjësimi ose shkatërrimi, edhe në qoftë se nuk janë të regjistruara në një bankë të dhënash.

13. "Marrës" është çdo person fizik ose juridik, autoritet publik, agjenci apo ndonjë organ tjetër të cilit i janë dhënë të dhënat e një palë të tretë ose jo. Autoritetet, të cilat mund të marrin të dhëna në kuadrin e një hetimi të veçantë, nuk konsiderohen si marrës.

14. "I ngarkuar" është personi që kryen përpunimin e të dhënave, me autorizim nga titullari ose personi përgjegjës.

15. "Palë e tretë" është çdo person fizik ose juridik, autoritet publik, agjenci apo ndonjë organ tjetër, përveç subjektit të të dhënave, kontrolluesit, përpunuesit dhe personave, të cilët, nën autoritetin e drejtpërdrejtë të kontrolluesit apo përpunuesit, janë të autorizuar të përpunojnë të dhëna.

16. “Transmetim” është transferimi i të dhënave personale te marrësit.

17. "Mbikëqyrje" është ndjekja me kujdes e përpunimit të të dhënave personale nga të gjithë kontrolluesit dhe përpunuesit, nëpërmjet bashkëpunimit, kontrollit, hetimit administrativ dhe inspektimit, për parandalimin e shkeljeve dhe, kur ka vend, edhe vendosja e sanksioneve administrative për të siguruar zbatimin e urdhrave, të udhëzimeve dhe rekomandimeve të Komisionerit, duke respektuar të drejtat dhe liritë themelore të njeriut.

18. "Monitorim i të dhënave personale" është puna e vazhdueshme, gjithëpërfshirëse, efikase dhe e planifikuar e institucionit në këto drejtime: udhëheqje, drejtim, organizim, ndihmë, bashkëpunim, takime sensibilizimi e njohjeje, orientim, raportim në Kuvend, publikim, shpjegime të ndryshme, dhënie përgjigjeje të ankimeve, veprimtari, seminare e leksione, aktivitete, dokumentim, hartim rregullash, marrëveshje, kontrata, udhëzime, vendime, rekomandime, kontroll i zbatimit të gjobave, krijim e hapje e regjistrave, si dhe për çështje të tjera që lidhen me ushtrimin e rregullt të veprimtarisë.

19. "Komunikim" është komunikimi i të dhënave personale një ose më shumë subjekteve të caktuara, të ndryshme nga i interesuari, nga përfaqësuesi i titullarit në territorin e vendit, nga përgjegjësit dhe të ngarkuarit, në çdo formë, edhe përmes vënies në dispozicion ose për konsultime.

20. "Përhapje" është komunikimi i informacionit për të dhënat personale palëve të papërcaktuara, në çfarëdo forme, edhe përmes vënies në dispozicion ose konsultimit.

21. "Bllokim" është ruajtja e të dhënave personale duke pezulluar përkohësisht çdo veprim tjetër përpunimi.

22. "Transferim ndërkombëtar" është dhënia e të dhënave personale marrësve në shtetet e huaja.

23. "Vendimmarrje automatike" është një lloj vlerësimi për individët, i kryer krejtësisht në mënyrë automatike, pa ndërhyrjen e individit.

24. "Pëlqim i subjekteve të të dhënave" është çdo deklaratë me shkrim, e dhënë shprehimisht me vullnet të plotë e të lirë dhe duke qenë në dijeni të plotë për arsyen pse të dhënat do të përpunohen, çka nënkupton që subjekti i të dhënave pranon që të përpunohen të dhënat e tij.

25. "Qëllimi historik" është qëllimi për studime, hulumtime, kërkime dhe dokumentim të figurave, fakteve dhe rrethanave të së kaluarës.

26. "Qëllimi statistikor" është qëllimi për hulumtime statistikore, prodhim të të dhënave statistikore edhe nëpërmjet sistemit informativ statistikor.

27. "Qëllimi shkencor" është qëllimi për studime dhe hulumtime sistematike, që finalizon zhvillimin e dijeve shkencore në një sektor të caktuar.

Neni 4
Fusha e zbatimit

1. Ky ligj zbatohet për përpunimin e të dhënave personale, plotësisht ose pjesërisht, nëpërmjet mjeteve automatike, si dhe për përpunimin me mjete të tjera të të dhënave personale, që mbahen në një sistem arkivimi apo kanë për qëllim të formojnë pjesë të sistemit të arkivimit. 2. Ky ligj

NISATEL OPERATOR PUBLIK I TELEKOMUNIKACIONEVE
Pavaresia 1200, Vlore, Albania
E-mail: info@nisatel.al;

zbatohet për përpunimin e të dhënave personale nga:

a) kontrollues të vendosur në Republikën e Shqipërisë;

b) misionet diplomatike ose zyrat konsullore të shtetit shqiptar;

c) kontrollues, të cilët nuk janë të vendosur në Republikën e Shqipërisë, por që e ushtrojnë

veprimtarinë nëpërmjet përdorimit të çdo mjeti, që ndodhet në Republikën e Shqipërisë. 3. Në rastet e parashikuara në shkronjën "c" të pikës 2 të këtij neni, kontrolluesi cakton një përfaqësues, i cili duhet të jetë i vendosur në Republikën e Shqipërisë. Parashikimet e këtij ligji, që zbatohen nga kontrolluesit, zbatohen edhe për përfaqësuesit e tyre.

3/1. Ky ligj zbatohet edhe për autoritetet zyrtare që përpunojnë të dhëna personale në fushat e parashikuara në pikën 2, të nenit 6, të këtij ligji**.**

4. Ky ligj nuk zbatohet për përpunimin e të dhënave:

a) për persona fizikë, për qëllime thjesht familjare ose personale;

b) vetëm për rastet kur jepet informacion për persona publikë zyrtarë ose punonjës të administratës publike (shtetërore), nëpërmjet të cilit pasqyrohet aktiviteti publik, administratativ ose çështje lidhur me detyrën e tyre.

KREU II
PËRPUNIMI I TË DHËNAVE PERSONALE

Neni 5
Mbrojtja e të dhënave personale

1. Mbrojtja e të dhënave personale bazohet:

a) në përpunimin në mënyrë të drejtë dhe të ligjshme;

b) në grumbullimin për qëllime specifike, të përcaktuara qartë, e legjitime dhe në përpunimin në përputhje me këto qëllime;

c) në mjaftueshmërinë e të dhënave, të cilat duhet të lidhen me qëllimin e përpunimit dhe të mos e tejkalojnë këtë qëllim;

ç) në saktësinë që të dhënat duhet të kenë dhe, kur është e nevojshme, duhet të përditësohen; duhet ndërmarrë çdo hap i arsyeshëm për të fshirë apo korrigjuar të dhëna të pasakta apo të paplota, në lidhje me qëllimin për të cilin janë mbledhur apo për të cilin përpunohen më tej;

d) në mbajtjen në atë formë, që të lejojë identifikimin e subjekteve të të dhënave për një kohë, por jo më tepër sesa është e nevojshme për qëllimin, për të cilin ato janë grumbulluar ose përpunuar më tej.

2. Kontrolluesi është përgjegjës për zbatimin e këtyre kërkesave në të gjitha përpunimet automatike ose me mjete të tjera të të dhënave.

Neni 6

Kriteret ligjore për përpunimin

1. Të dhënat personale përpunohen vetëm:

a) nëse subjekti i të dhënave personale ka dhënë pëlqimin;

b) nëse përpunimi është thelbësor për përmbushjen e një kontrate, për të cilën subjekti i të dhënave është palë kontraktuese, apo për diskutime ose ndryshime të një projekti/kontrate me propozimin e subjektit të të dhënave;

c) për të mbrojtur interesat jetikë të subjektit të të dhënave;

ç) për përmbushjen e një detyrimi ligjor të kontrolluesit;

d) për kryerjen e një detyre ligjore me interes publik ose ushtrimin e një kompetence të kontrolluesit ose të një pale të tretë, së cilës i janë përhapur të dhënat; dh) nëse është thelbësor për mbrojtjen e të drejtave dhe interesave legjitime të kontrolluesit, marrësit apo personave të tjerë të interesuar. Por, në çdo rast, përpunimi i të dhënave personale nuk mund të jetë në kundërshtim të hapur me të drejtën e subjektit të të dhënave për mbrojtjen e jetës personale dhe private.

2. Përpunimi i të dhënave personale, të përcaktuara në kuadër të veprimtarive të parandalimit dhe ndjekjes penale, për kryerjen e një vepre penale kundër rendit publik dhe të veprave të tjera në fushën e të drejtës penale, si dhe në fushën e mbrojtjes dhe sigurisë kombëtare, kryhet nga autoritetet zyrtare të përcaktuara në ligj.

3. Kontrolluesi apo përpunuesi, që merret me përpunimin e të dhënave personale, me qëllim ofrimin e mundësive për biznes apo të shërbimeve, mund të përdorë për këtë qëllim të dhëna personale të marra nga lista publike të dhënash. Kontrolluesi apo përpunuesi nuk mund të vazhdojë përpunimin më tej të të dhënave të specifikuara në këtë paragraf, nëse subjekti i të dhënave ka shprehur mospajtim ose ka kundërshtuar përpunimin e mëtejshëm të tyre. Asnjë e dhënë personale shtesë nuk mund t'i bashkëlidhet të dhënave të specifikuara më lart, pa pëlqimin e subjektit të të dhënave.

4. Kontrolluesit i lejohet të mbajë në sistemin e vet të arkivimit të dhënat personale edhe pasi subjekti ka kundërshtuar përpunimin, sipas pikës 3 të këtij neni. Këto të dhëna mund të përdoren përsëri vetëm nëse subjekti i të dhënave personale jep pëlqimin.

5. Mbledhja e të dhënave personale, që lidhen në mënyrë unike me një subjekt të dhënash, për arsye të tregtimit të drejtpërdrejtë, lejohet vetëm nëse subjekti i të dhënave ka dhënë pëlqimin e shprehur qartë.

Neni 7

Përpunimi i të dhënave sensitive

1. Me përjashtim të rasteve të parashikuara në pikat 2 dhe 3 të këtij neni, ndalohet përpunimi i të

dhënave, që zbulojnë origjinën racore ose etnike, mendimet politike, anëtarësinë në sindikata,

besimin fetar apo filozofik, dënimet penale, si dhe shëndetin dhe jetën seksuale. 2. Përpunimi i të dhënave sensitive bëhet vetëm nëse:

a) subjekti i të dhënave ka dhënë pëlqimin, që mund të revokohet në çdo çast dhe e bën të paligjshëm përpunimin e mëtejshëm të të dhënave;

b) është në interesin jetik të subjektit të të dhënave ose të një personi tjetër dhe subjekti i të dhënave është fizikisht ose mendërisht i paaftë për të dhënë pëlqimin e vet;

c) autorizohet nga autoriteti përgjegjës për një interes të rëndësishëm publik, nën masa të përshtatshme mbrojtëse;

ç) lidhet me të dhëna, që janë bërë haptazi publike nga subjekti i të dhënave ose është i nevojshëm për ushtrimin apo mbrojtjen e një të drejte ligjore;

d) të dhënat përpunohen për qëllime historike, shkencore ose statistikore, nën masa të përshtatshme mbrojtëse;

dh) të dhënat kërkohen për qëllime të mjekësisë parandaluese, diagnostikimit mjekësor, sigurimit të kujdesit shëndetësor, kurimit, menaxhimit të shërbimeve të kujdesit shëndetësor dhe përdorimi i tyre kryhet nga personeli mjekësor ose persona të tjerë, që kanë detyrimin për ruajtjen e fshehtësisë;

e) të dhënat përpunohen nga organizatat jofitimprurëse politike, filozofike, fetare ose sindikaliste, për qëllime të veprimtarisë të tyre të ligjshme, vetëm për anëtarët, sponsorizuesit ose personat e tjerë, që kanë lidhje me veprimtarinë e tyre. Këto të dhëna nuk u bëhen të ditura një pale të tretë, pa pëlqimin e subjektit të të dhënave, përveç kur parashikohet ndryshe në ligj;

ë) përpunimi është i nevojshëm për përmbushjen e detyrimit ligjor dhe të të drejtave specifike të kontrolluesit në fushën e punësimit, në përputhje me Kodin e Punës.

Neni 8

Transferimi ndërkombëtar

1. Transferimi ndërkombëtar i të dhënave personale kryhet, me marrës, nga shtete me një nivel të mjaftueshëm të mbrojtjes së të dhënave personale. Niveli i mbrojtjes së të dhënave personale për një shtet përcaktohet duke vlerësuar të gjitha rrethanat lidhur me përpunimin, natyrën, qëllimin dhe kohëzgjatjen e tij, shtetin e origjinës dhe destinacionin përfundimtar, aktet ligjore dhe standardet e sigurisë në fuqi në shtetin marrës. Shtetet, që kanë nivel të mjaftueshëm të mbrojtjes së të dhënave, përcaktohen me vendim të Komisionerit.

2. Transferimi ndërkombëtar i të dhënave personale me një shtet, që nuk ka nivel të mjaftueshëm të mbrojtjes së të dhënave personale mund të bëhet nëse:

a) autorizohet nga akte ndërkombëtare, të ratifikuara nga Republika e Shqipërisë dhe që janë të zbatueshme në mënyrë të drejtpërdrejtë;

b) subjekti i të dhënave ka dhënë pëlqimin për transferim ndërkombëtar;

c) transferimi është i nevojshëm për kryerjen e kontratës ndërmjet subjektit të të dhënave dhe

kontrolluesit ose për zbatimin e masave parakontraktore, të marra si përgjigje ndaj kërkesës së

subjektit, ose transferimi është i nevojshëm për përmbushjen apo kryerjen e një kontrate ndërmjet kontrolluesit dhe një pale të tretë, në interes të subjektit të të dhënave;

d) është i nevojshëm për mbrojtjen e interesave jetësorë të subjektit të të dhënave;

dh) është i nevojshëm apo përbën një kërkesë ligjore për një interes të rëndësishëm publik ose për ushtrimin dhe mbrojtjen e një të drejte ligjore;

e) është bërë nga një regjistër, i cili është i hapur për këshillime dhe siguron informacion për publikun në përgjithësi.

3. Shkëmbimi i të dhënave personale me përfaqësitë diplomatike të qeverive të huaja ose institucionet ndërkombëtare në Republikën e Shqipërisë vlerësohet transferim ndërkombëtar.

Neni 9

Transferimi ndërkombëtar i të dhënave që duhet të autorizohen

1. Transferimi ndërkombëtar i të dhënave personale me një shtet, që nuk ka nivel të mjaftueshëm të mbrojtjes së të dhënave, në raste të tjera nga ato të parashikuara në nenin 8 të këtij ligji, bëhet me autorizim të komisionerit kur parashtrohen siguri të mjaftueshme në lidhje me mbrojtjen e privatësisë dhe të të drejtave e lirive themelore të njeriut, si dhe në lidhje me ushtrimin e së drejtës përkatëse.

2. Komisioneri, pasi bën vlerësimin sipas përcaktimeve të pikës 1 të këtij neni dhe të pikës 1 të nenit 8, mund të japë autorizimin për transferimin e të dhënave personale në shtetin marrës, duke përcaktuar kushte dhe detyrime.

3. Komisioneri nxjerr udhëzime për lejimin e disa kategorive të transferimeve ndërkombëtare të të dhënave personale në një shtet që nuk ka nivel të mjaftueshëm të mbrojtjes së të dhënave personale. Në këto raste, kontrolluesi përjashtohet nga kërkesa për autorizim.

4. Kontrolluesi, përpara transferimit të të dhënave, bën kërkesë për autorizim te komisioneri. Në kërkesë kontrolluesi duhet të garantojë respektimin e interesave për ruajtjen e sekretit të subjektit të të dhënave jashtë Republikës së Shqipërisë.

KREU III
PËRPUNIMI I VEÇANTË I TË DHËNAVE

Neni 10

Përpunimi për qëllime historike, shkencore dhe statistikore

1. Të dhënat personale, të mbledhura për çfarëdolloj qëllimi, mund të përpunohen më tej për qëllime historike, shkencore ose statistikore, duke siguruar se nuk janë përpunuar, për të marrë masa ose vendime për një individ.

2. Transmetimi i të dhënave sensitive për kërkimet shkencore bëhet vetëm kur ekziston një interes i rëndësishëm publik. Të dhënat personale përdoren vetëm nga persona, të cilët janë të detyruar të ruajnë konfidencialitetin.

3. Në rastet kur përdorimi i të dhënave bëhet në një formë, që lejon identifikimin e subjektit të të dhënave, të dhënat duhet të kodohen menjëherë, në mënyrë që subjektet të mos jenë më të identifikueshme. Të dhënat personale të koduara përdoren vetëm nga persona, të cilët janë të detyruar të ruajnë konfidencialitetin.

Neni 11

Përpunimi i të dhënave personale dhe e liria të shprehurit

1. Komisioneri përcakton me udhëzim të veçantë kushtet dhe kriteret kur, për qëllime gazetarie, letrare dhe artistike, mund të bëhen përjashtime nga detyrimet që rrjedhin nga nenet 5, 6, 7, 8, 18 dhe 21 të këtij ligji.

2. Përjashtimet, sipas këtij neni, mund të lejohen deri në atë masë, për aq sa ato pajtojnë të drejtën për mbrojtjen e të dhënave personale me rregullat që administrojnë lirinë e informimit.

3. Veprimet e kontrolluesit ose përpunuesit, në kundërshtim me pikat e mësipërme dhe kodin etik përbëjnë kundërvajtje administrative.

KREU IV
TË DREJTAT E SUBJEKTIT TË TË DHËNAVE

Neni 12

E drejta për akses

1. Çdo person ka të drejtë që pa pagesë me kërkesë me shkrim, të marrë nga kontrolluesi: a) konfirmimin nëse të dhënat personale po i përpunohen ose jo, informacion për qëllimin e përpunimit, për kategoritë e të dhënave të përpunuara dhe për marrësit e kategoritë e marrësve, të cilëve u përhapen të dhënat personale;

b) në një formë të kuptueshme, të dhënat personale dhe informacionin e disponueshëm për burimin e tyre;

c) në rastet e vendimeve automatike, sipas nenit 14 të këtij ligji, informacion për logjikën e përfshirë në vendimmarrje.

Informacioni për të dhënat komunikohet në formën, në të cilën ishin në kohën kur është bërë kërkesa.

2. Kontrolluesi, brenda 30 ditëve nga data e marrjes së kërkesës, informon subjektin e të dhënave ose i shpjegon atij arsyet e mosdhënies së informacionit.

3. E drejta për akses, sipas pikës 1 të këtij neni, ushtrohet në përputhje me parimet kushtetuese të lirisë së shprehjes dhe informacionit, lirisë së shtypit dhe sekretit profesional dhe mund të kufizohet, nëse cenon interesat e sigurisë kombëtare, politikën e jashtme, interesat ekonomikë dhe financiarë të shtetit, parandalimin dhe ndjekjen e veprave penale.

4. E drejta e aksesit nuk mund të ushtrohet në rastet e parashikuara në pikën 1 të nenit 10 të këtij ligji.

5. Në rast se aksesi mohohet, duke argumentuar se cenohen interesat e sigurisë kombëtare, politika e jashtme, interesat ekonomikë dhe financiarë të shtetit, parandalimi dhe ndjekja e veprave penale ose liria e shprehjes dhe informimit apo liria e shtypit, subjekti i të dhënave mund t'i kërkojë komisionerit të kontrollojë përjashtimin në rastin konkret. Komisioneri informon subjektin e të dhënave për masat e marra.

Neni 13

E drejta për të kërkuar bllokimin, korrigjimin ose fshirjen

1. Çdo subjekt i të dhënave ka të drejtë të kërkojë bllokimin, korrigjimin ose fshirjen e të dhënave pa pagesë, kur vihet në dijeni se të dhënat rreth tij nuk janë të rregullta, të vërteta, të plota ose janë përpunuar dhe mbledhur në kundërshtim me dispozitat e këtij ligji.

2. Kontrolluesi, brenda 30 ditëve nga data e marrjes së kërkesës së subjektit të të dhënave, duhet ta informojë atë për përpunimin e ligjshëm të të dhënave, kryerjen ose moskryerjen e bllokimit, korrigjimit apo të fshirjes.

3. Kur kontrolluesi nuk bën bllokimin, korrigjimin ose fshirjen e të dhënave të kërkuara prej tij, subjekti i të dhënave ka të drejtë të ankohet te komisioneri.

Neni 14

Vendimmarrja automatike

1. Çdo person ka të drejtë të mos jetë subjekt i vendimeve, të cilat shkaktojnë efekte ligjore për të ose ndikojnë në mënyrë të rëndësishme tek ai dhe kur vendimi është bazuar vetëm në përpunimin automatik të të dhënave, që synojnë të vlerësojnë disa aspekte personale, që lidhen me të, veçanërisht, efektivitetin në punë, besueshmërinë ose sjelljen.

2. Një person mund të jetë subjekt i një vendimi të marrë, sipas pikës 1 të këtij neni, kur vendimi:
a) është marrë gjatë lidhjes ose zbatimit të një kontrate, nëse kërkesa e paraqitur nga subjekti i të dhënave për lidhjen ose zbatimin e kontratës është përmbushur, ose nëse ka masa të përshtatshme për të mbrojtur interesat e tij të ligjshëm, të tillë si mundësi që e lejojnë atë të parashtrojë pikëpamjet e tij;

b) autorizohet nga një ligj, i cili, gjithashtu, parashikon masa për të mbrojtur interesat e ligjshëm

të subjektit të të dhënave.

Neni 15

E drejta e subjektit të të dhënave për të kundërshtuar

1. Subjekti i të dhënave ka të drejtë të kundërshtojë, në çdo kohë, mbështetur në ligj, përpunimin e të dhënave rreth tij, sipas shkronjave "d" dhe "dh" të nenit 6 të këtij ligji, përveç kur parashikohet ndryshe me ligj.

2. Subjekti i të dhënave ka të drejtë pa pagesë t'i kërkojë kontrolluesit të mos fillojë ose, nëse përpunimi ka filluar, të ndalojë përpunimin e të dhënave personale, që lidhen me të, për qëllime të tregtimit të drejtpërdrejtë si dhe të informohet përpara përhapjes për herë të parë të të dhënave personale për këtë qëllim.

Neni 16

E drejta për t'u ankuar

1. Çdo person, që pretendon se i janë shkelur të drejtat, liritë dhe interesat e ligjshëm për të dhënat personale, ka të drejtë të ankohet ose të njoftojë komisionerin dhe të kërkojë ndërhyrjen e tij për vënien në vend të së drejtës së shkelur. Pas këtij ankimi, në përputhje me Kodin e Procedurës Civile, subjekti i të dhënave mund të ankohet në gjykatë.

2. Në rast se subjekti i të dhënave ka bërë ankim, kontrolluesi nuk ka të drejtë të ndryshojë të dhënat personale deri në dhënien e vendimit përfundimtar.

Neni 17

Kompensimi i dëmit

Çdo person, të cilit i është shkaktuar një dëm, si rezultat i përpunimit të paligjshëm të të dhënave personale, ka të drejtë t'i kërkojë kontrolluesit kompensim, sipas rregullave të përcaktuara në Kodin Civil.

KREU V
DETYRIMET E KONTROLLUESIT DHE TË PËRPUNUESIT

Neni 18

Detyrimi për informim

1. Kontrolluesi, kur mbledh të dhëna personale, duhet të informojë subjektin e të dhënave për fushën dhe qëllimin, për të cilin do të përpunohen të dhënat personale, për personin që do t'i përpunojë të dhënat, për mënyrën e përpunimit, përveç rastit kur subjekti i të dhënave është në

dijeni të këtij informacioni. Kontrolluesi duhet të informojë subjektin e të dhënave për të drejtën për akses, si dhe të drejtën për korrigjim të të dhënave të tij.

2. Në rast se kontrolluesi përpunon të dhëna personale, të marra nga subjekti i të dhënave, ai është i detyruar të informojë subjektin e të dhënave nëse dhënia e të dhënave personale është e detyrueshme apo vullnetare. Nëse subjekti i të dhënave, në bazë të një akti ligjor ose nënligjor, është i detyruar të japë të dhëna personale për përpunim, kontrolluesi e informon edhe rreth këtij fakti, si dhe rreth pasojave të refuzimit të dhënies së të dhënave personale.

3. Kontrolluesi nuk është i detyruar të japë informacion dhe të informojë për rastet kur të dhënat personale nuk janë marrë nga subjekti i të dhënave, nëse:

a) ai përpunon të dhëna personale ekskluzivisht për qëllime historike, statistikore dhe për kërkime shkencore dhe nëse dhënia e këtij informacioni është e pamundur, ose kërkon përpjekje joproporcionale;

b) ai detyrohet të kryejë përpunimin e të dhënave personale në bazë të një parashikimi ligjor; c) ai përpunon të dhëna të bëra publike;

ç) ai përpunon të dhëna personale, të marra me pëlqimin e subjektit të të dhënave.

4. Kontrolluesi, gjatë përpunimit të të dhënave personale, sipas shkronjës "dh" të pikës 1 të nenit 6 dhe shkronjës "ç" të pikës 2 të nenit 7, në lidhje me ushtrimin apo mbrojtjen e të drejtave të ligjshme, është i detyruar të informojë subjektin e të dhënave rreth përpunimit të të dhënave të tij.

5. Detyrimi për informim, që rregullohet me këtë nen, mund të kryhet nga përpunuesi në emër të kontrolluesit.

Neni 19

Detyrimi për korrigjim ose fshirje

1. Kontrolluesi kryen vetë ose me kërkesë të subjektit të të dhënave bllokimin, korrigjimin ose fshirjen e të dhënave personale, kur vëren se janë të parregullta, të pavërteta, të paplota ose janë përpunuar në kundërshtim me dispozitat e këtij ligji.

2. Kontrolluesi, brenda 30 ditëve nga marrja e kërkesës së subjektit të të dhënave, informon subjektin e të dhënave për kryerjen apo moskryerjen e bllokimit, korrigjimit ose të fshirjes.

3. Kontrolluesi informon marrësin e të dhënave personale për korrigjimin ose fshirjen e të dhënave personale, të transmetuara para korrigjimit apo fshirjes.

Neni 20

Detyrimet e përpunuesit

1. Kontrolluesit, për përpunimin e të dhënave personale, mund të punësojnë përpunues, të cilët garantojnë përdorimin e ligjshëm dhe të sigurt të të dhënave. Çdo përpunues i të dhënave

personale ka këto detyrime:

a) të përpunojë të dhënat vetëm në përputhje me udhëzimet e kontrolluesit; të mos i transmetojë ato, përveç kur ka marrë udhëzim nga kontrolluesi;

b) të marrë të gjitha masat e sigurisë, sipas këtij ligji dhe të punësojë operatorë, të cilët kanë detyrimin për ruajtjen e fshehtësisë;

c) të krijojë, në marrëveshje me kontrolluesin, kushtet e nevojshme teknike dhe organizative për përmbushjen e detyrimeve të kontrolluesit, për të siguruar të drejtat e subjekteve të të dhënave personale;

ç) t'i dorëzojë kontrolluesit, pas përfundimit të shërbimit të përpunimit, të gjitha rezultatet e përpunimit dhe dokumentacionit, që përmban të dhëna ose t'i mbajë apo t'i shkatërrojë ato me kërkesë të kontrolluesit;

d) të vërë në dispozicion të kontrolluesit të gjithë informacionin e nevojshëm, për të kontrolluar përputhshmërinë me detyrimet, që rrjedhin sipas shkronjave të mësipërme.

2. Detyrimet e pikës 1 përcaktohen në kontratën *e* shkruar e kontrolluesit me përpunuesin.

KREU VI
NJOFTIMI

Neni 21
Përgjegjësia për të njoftuar

1. Çdo kontrollues duhet të njoftojë komisionerin për përpunimin e të dhënave personale, për të cilat është përgjegjës. Njoftimi duhet të bëhet para se kontrolluesi të përpunojë të dhënat për herë të parë ose kur kërkohet ndryshimi i gjendjes së njoftimit të përpunimit, sipas nenit 22 të këtij ligji, të njoftuar më parë.

2. Përjashtohet nga detyrimi për të njoftuar përpunimi i të dhënave personale, me qëllim mbajtjen e një regjistri, i cili, në përputhje me ligjin ose aktet nënligjore, siguron informacion për publikun në përgjithësi.

3. Përjashtohen nga detyrimi për të njoftuar të dhënat personale që përpunohen, me qëllim mbrojtjen e institucioneve kushtetuese, të interesave të sigurisë kombëtare, politikës së jashtme, interesave ekonomikë ose financiarë të shtetit, apo për parandalimin e ndjekjen e veprave penale.

4. Rastet e tjera, për të cilat njoftimi nuk është i nevojshëm, përcaktohen me vendim të Komisionerit.

Neni 22
Përmbajtja e njoftimit

Njoftimi duhet të përmbajë:

a) emrin dhe adresën e kontrolluesit;

b) qëllimin e përpunimit të të dhënave personale;

c) kategoritë e subjekteve të të dhënave dhe kategoritë e të dhënave personale;
ç) marrësit dhe kategoritë e marrësve të të dhënave personale;

d) propozimin për transferimet ndërkombëtare që kontrolluesi synon të kryejë; dh) një përshkrim të përgjithshëm të masave për sigurinë e të dhënave personale.

Neni 23

Procedura e shqyrtimit

Komisioneri shqyrton të gjitha njoftimet dhe kur njoftimi është i pamjaftueshëm, ai urdhëron kontrolluesin të plotësojë përmbajtjen e njoftimit, duke përcaktuar edhe afatin kohor.

Nëse kontrolluesi nuk plotëson përmbajtjen e njoftimit brenda afatit të përcaktuar, njoftimi konsiderohet i pakryer.

Neni 24

Kontrolli paraprak

1. Autorizimi i komisionerit kërkohet për:

a) përpunimin e të dhënave sensitive, sipas shkronjës "c" të pikës 2 të nenit 7 të këtij ligji; b) përpunimin e të dhënave personale, sipas pikës 1 të nenit 9 të këtij ligji.

2. Nëse përpunimi i të dhënave, sipas pikës 1 të këtij neni, autorizohet nga një dispozitë ligjore, nuk kërkohet autorizim nga komisioneri.

Neni 25

Fillimi i përpunimit

1. Përpunimi i të dhënave fillon pas njoftimit.

2. Përpunimi i të dhënave, për të cilat kërkohet autorizim, sipas pikës 1 të nenit 24 të këtij ligji, mund të fillojë vetëm pas marrjes së autorizimit.

Neni 26

Publikimi i përpunimeve

1. Për të dhënat që kërkohet autorizim, merret vendim i veçantë dhe pasqyrohet në regjistrin që administrohet nga komisioneri, i cili është i hapur për njohje për çdo person. 2. Regjistrimi duhet të përmbajë informacionin, sipas nenit 22 të këtij ligji, përveç informacionit të përcaktuar në shkronjën "dh" të nenit 22 të këtij ligji, i cili nuk publikohet.

3. Kontrolluesi i përjashtuar nga detyrimi për njoftim duhet të bëjë të disponueshme, të paktën, të dhënat për emrin dhe adresën, kategoritë e të dhënave personale të përpunuara, qëllimet e

përpunimeve, kategoritë e marrësve.

Nëse do të bëhet transferim ndërkombëtar i të dhënave, kontrolluesi është i detyruar të njoftojë Komisionerin.

4. Ky nen nuk zbatohet për përpunime për mbajtjen e një regjistri, i cili, në përputhje me ligjin apo aktet nënligjore, siguron informacion për publikun në përgjithësi.

5. Komisioneri vendos për çregjistrimin e kontrolluesit, kryesisht ose me kërkesën e tij, nëse qëllimi ose qëllimet, për të cilat është kryer njoftimi dhe regjistrimi, pushojnë së ekzistuari.

KREU VII
SIGURIA E TË DHËNAVE PERSONALE

Neni 27
Masat për sigurinë e të dhënave personale

1. Kontrolluesi ose përpunuesi merr masa organizative dhe teknike të përshtatshme për të mbrojtur të dhënat personale nga shkatërrime të paligjshme, aksidentale, humbje aksidentale, për të mbrojtur aksesin ose përhapjen nga persona të paautorizuar, veçanërisht kur përpunimi i të dhënave bëhet në rrjet, si dhe nga çdo formë tjetër e paligjshme përpunimi. 2. Kontrolluesi merr këto masa të veçanta sigurie:

a) përcakton funksionet ndërmjet njësive organizative dhe operatorëve për përdorimin e të dhënave;

b) përdorimi i të dhënave bëhet me urdhër të njësive organizative ose të operatorëve të autorizuar;

c) udhëzon operatorët, pa përjashtim, për detyrimet që kanë, në përputhje me këtë ligj dhe rregulloret e brendshme për mbrojtjen e të dhënave, përfshirë edhe rregulloret për sigurinë e të dhënave;

ç) ndalon hyrjen në mjediset e kontrolluesit ose të përpunuesit të të dhënave të personave të paautorizuar;

d) hyrja në të dhënat dhe programet bëhet vetëm nga personat e autorizuar, dh) ndalon hyrjen në mjetet e arkivimit dhe përdorimin e tyre nga persona të paautorizuar; e) vënia në punë e pajisjeve të përpunimit të të dhënave bëhet vetëm me autorizim dhe çdo mjet sigurohet me masa parandaluese ndaj vënies së autorizuar në punë;

ë) regjistron dhe dokumenton modifikimet, korrigjimet, fshirjet, transmetimet etj.

2/1. Kontrolluesi është i detyruar të dokumentojë masat tekniko-organizative të përshtatura dhe të zbatuara për garantimin e mbrojtjes së të dhënave personale, në përputhje me ligjin dhe rregullore të tjera.

3. Të dhënat e regjistruara nuk përdoren për qëllime të ndryshme, që nuk janë në përputhje me qëllimin e grumbullimit. Ndalohet njohja ose çdo përpunim i të dhënave të regjistruara në dosje

për një qëllim të ndryshëm nga e drejta për të hedhur të dhëna. Përjashtohet nga ky rregull rasti kur të dhënat përdoren për të garantuar sigurinë kombëtare, sigurinë publike, parandalimin dhe hetimin e kryerjes së një vepre penale, apo ndjekjen e autorëve të saj, ose për shkelje të etikës për profesionet e rregulluara.

4. Dokumentacioni i të dhënave mbahet për aq kohë sa është i nevojshëm për qëllimin, për të cilin është grumbulluar.

5. Niveli i sigurisë duhet të jetë i përshtatshëm me natyrën e përpunimit të të dhënave personale. Rregulla të hollësishme për sigurimin e të dhënave përcaktohen me vendim të komisionerit.

6. Procedurat e administrimit të regjistrimit të të dhënave, të hedhjes së të dhënave, të përpunimit dhe nxjerrjes së tyre përcaktohen me vendim të komisionerit.

Neni 28

Konfidencialiteti i të dhënave

Kontrolluesit, përpunuesit dhe personat, që vihen në dijeni me të dhënat e përpunuara, gjatë ushtrimit të funksioneve të tyre, detyrohen të ruajnë konfidencialitetin dhe besueshmërinë edhe pas përfundimit të funksionit. Këto të dhëna nuk përhapen, përveç rasteve të parashikuara me ligj.

Çdo person që vepron nën autoritetin e kontrolluesit, nuk duhet t'i përpunojë të dhënat personale, tek të cilat ka akses, pa autorizimin e kontrolluesit, përveçse kur detyrohet me ligj.

KREU VIII
KOMISIONERI PËR MBROJTJEN E TË DHËNAVE PERSONALE

Neni 29

Komisioneri

1. Komisioneri për mbrojtjen e të dhënave personale është autoriteti përgjegjës i pavarur, që mbikëqyr dhe monitoron, në përputhje me ligjin, mbrojtjen e të dhënave personale, duke respektuar e garantuar të drejtat dhe liritë themelore të njeriut.

2. Komisioneri është person juridik publik.

3. Informacioni i siguruar nga komisioneri, gjatë ushtrimit të detyrës, përdoret vetëm për qëllime mbikëqyrjeje, në përputhje me legjislacionin për mbrojtjen e të dhënave personale. Komisioneri është i detyruar të ruajë konfidencialitetin e të dhënave edhe pas mbarimit të detyrës.

Neni 30

Të drejtat

1. Komisioneri ka këto të drejta:

a) kryen hetim administrativ dhe ka të drejtën e aksesit në përpunimet e të dhënave personale, si dhe ka të drejtë të mbledhë të gjithë informacionin e nevojshëm për përmbushjen e detyrave të mbikëqyrjes;

b) urdhëron bllokimin, fshirjen, shkatërrimin ose pezullon përpunimin e paligjshëm të të dhënave personale;

c) jep udhëzime përpara se përpunimet të kryhen dhe siguron publikimin e tyre. 2. Komisioneri, në rast shkeljesh serioze, të përsëritura ose të qëllimshme të ligjit nga një kontrollues ose përpunues, veçanërisht në rastet e përsëritura të moszbatimit të rekomandimeve të tij, vepron sipas nenit 39 të këtij ligji dhe e denoncon publikisht ose e raporton çështjen në Kuvend dhe në Këshillin e Ministrave.

2/1. Për rastet që shkelja përbën vepër penale, bën kallëzimin përkatës.

Neni 31

Përgjegjësitë

1. Komisioneri është përgjegjës për:

a) dhënien e mendimeve për projekt-aktet, ligjore dhe nënligjore, që kanë të bëjnë me të dhënat personale, si dhe projektet që kërkohen të zbatohen nga kontrolluesit vetëm apo në bashkëpunim me të tjerë;

a/1) dhënien e rekomandimeve për zbatimin e kërkesave të ligjit për mbrojtjen e të dhënave personale dhe siguron publikimin e tyre;

b) dhënien e autorizimit, në raste të veçanta, për përdorimin e të dhënave personale për qëllime jo të përcaktuara në grumbullimin e tyre, duke respektuar parimet e nenit 5 të këtij ligji;

c) dhënien e autorizimit për transferimin ndërkombëtar të të dhënave personale, në përputhje me nenin 9 të këtij ligji;

ç) nxjerrjen e udhëzimeve, ku përcaktohet koha e mbajtjes së të dhënave personale, sipas qëllimit të tyre, në veprimtarinë e sektorëve të veçantë;

d) sigurimin e së drejtës së informimit dhe të ushtrimit të së drejtës së korrigjimit e të përditësimit të të dhënave;

dh) dhënien e autorizimit për përdorimin e të dhënave sensitive, në përputhje me shkronjën "c" të pikës 2 të nenit 7 të këtij ligji;

e) kontrollimin e përpunimit të të dhënave, në përputhje me ligjin, kryesisht ose me kërkesë të një personi edhe, kur një përpunim i tillë është i përjashtuar nga e drejta e informacionit dhe vënien në dijeni të personit se kontrolli është kryer, si dhe verifikimin nëse procesi është i ligjshëm ose jo;

ë) zgjidhjen e ankimeve të subjektit të të dhënave për mbrojtjen e të drejtave dhe të lirive të tij, për përpunimet e të dhënave personale dhe vënien e tij në dijeni për zgjidhjen e ankesës së paraqitur;

f) nxjerrjen e udhëzimeve për marrjen e masave të sigurisë në veprimtarinë e sektorëve të veçantë;

g) kontrollin e zbatimit të gjobave;

gj) nxitjen e kontrolluesit për hartimin e kodeve të etikës dhe vlerësimin e tyre;

h) publikimin dhe shpjegimin e të drejtave për mbrojtjen e të dhënave dhe publikimin periodikisht të veprimtarive të zhvilluara prej tij;

i) bashkëpunimin me autoritetet mbikëqyrëse për të dhënat personale të shteteve të huaja, për mbrojtjen e të drejtave të individëve rezidentë në këto shtete;

j) përfaqësimin e autoritetit mbikëqyrës në fushën e mbrojtjes së të dhënave personale në veprimtaritë kombëtare dhe ndërkombëtare;

k) ushtrimin e detyrave të tjera ligjore.

2. Komisioneri krijon një regjistër për dokumentimin e të gjitha njoftimeve dhe autorizimeve, që ai kryen në ushtrim të kompetencave të tij, në fushën e mbrojtjes së të dhënave personale.

3. Komisioneri paraqet raport vjetor përpara Kuvendit dhe raporton përpara tij sa herë i kërkohet. Gjithashtu, ai mund t'i kërkojë Kuvendit të dëgjohet për çështje që i çmon të rëndësishme.

Neni 32

Detyrimi për bashkëpunim

1. Institucionet publike dhe private bashkëpunojnë me komisionerin, duke i siguruar të gjithë informacionin që ai kërkon për përmbushjen e detyrave, si dhe e njoftojnë atë për zbatimin e rekomandimeve të dhëna menjëherë pas mbarimit të afatit të caktuar për kryerjen e tyre. 2. Komisioneri ka akses në sistemin e kompjuterave, në sistemet e arkivimit, që kryejnë përpunimin e të dhënave personale dhe në të gjithë dokumentacionin, që lidhet me përpunimin dhe transferimin e tyre, për ushtrimin e të drejtave dhe të detyrave që i janë ngarkuar me ligj.

Neni 33

Zgjedhja dhe qëndrimi në detyrë

Komisioneri zgjidhet nga Kuvendi, me propozimin e Këshillit të Ministrave, për një mandat 5-vjeçar, me të drejtë rizgjedhjeje.

Neni 34

Papajtueshmëria e funksionit

Funksioni i komisionerit është i papajtueshëm me çdo funksion tjetër shtetëror, me anëtarësimin në partitë politike dhe pjesëmarrjen në veprimtaritë e tyre, si dhe me çdo veprimtari tjetër fitimprurëse, me përjashtim të mësimdhënies.

Neni 35

Kriteret për t'u zgjedhur

Komisioner mund të zgjidhet shtetasi shqiptar, që plotëson kushtet e mëposhtme:

a) ka arsim të lartë juridik;

b) ka njohuri dhe veprimtari të shquara në fushën e të drejtave dhe lirive themelore të njeriut;

c) shquhet për aftësi profesionale dhe figurë të pastër etiko-morale;

ç) ka vjetërsi pune në profesionin e juristit jo më pak se 10 vjet;

d) nuk është dënuar me vendim të formës së prerë për kryerjen e një vepre penale; dh) nuk është larguar nga puna ose shërbimi civil me masë disiplinore.

Neni 36

Mbarimi i mandatit

1. Mandati i komisionerit mbaron para kohe kur:

a) dënohet nga gjykata me vendim të formës së prerë për kryerjen e një vepre penale;

b) nuk paraqitet pa arsye në detyrë për më shumë se 1 muaj;

c) jep dorëheqjen;

ç) deklarohet i paaftë me vendim gjykate të formës së prerë. 2. Komisioneri mund të shkarkohet nga Kuvendi:

a) për shkelje të dispozitave të këtij ligji apo akteve të tjera ligjore;

b) kur kryen veprimtari, që krijon konflikt interesash;

c) kur zbulohen raste të papajtueshmërisë së funksionit të tij.

3. Në rast se vendi i komisionerit mbetet vakant, Këshilli i Ministrave, brenda 15 ditëve, i propozon Kuvendit kandidaturën e re. Kuvendi zgjedh komisionerin brenda 15 ditëve nga paraqitja e kandidaturës.

Neni 37

Zyra e komisionerit

Kuvendi vendos për pagën e komisionerit, strukturën organizative dhe klasifikimin e pagave për

punonjësit e zyrës së komisionerit për mbrojtjen e të dhënave personale. Punonjësit e kësaj zyre gëzojnë statusin e nëpunësit civil.

Neni 38

Buxheti

Komisioneri ka buxhetin e vet të pavarur, i cili financohet nga Buxheti i Shtetit dhe donatorë, të cilët nuk paraqesin konflikt interesi. Administrimi i këtyre donacioneve bëhet sipas marrëveshjeve me donatorët dhe legjislacionin shqiptar në fuqi.

Neni 38/a

Publikimi

1. Udhëzimet, vendimet e Komisionerit, me përjashtim të atyre të dhëna në zbatim të shkronjës "b" të nenit 30 dhe të nenit 39 të këtij ligji, botohen në Fletoren Zyrtare.
2. Raporti vjetor dhe raportet e veçanta bëhen publike.

KREU IX
SANKSIONE ADMINISTRATIVE

Neni 39

Kundërvajtjet administrative

1. Rastet e përpunimit të të dhënave në kundërshtim me dispozitat e këtij ligji kur nuk përbëjnë kundërvajtje penale përbëjnë kundërvajtje administrative dhe dënohen me gjobë, si më poshtë:

a) kontrolluesit, që përdorin të dhëna personale në kundërshtim me kreun II "Përpunimi i të dhënave personale", dënohen me 10 000 deri në 500 000 lekë;

a/1) kontrolluesit, që përdorin të dhëna personale në kundërshtim me kreun III, "Përpunimi i veçantë i të dhënave", dënohen me 15 000 deri në 200 000 lekë;

b) kontrolluesit, që nuk përmbushin detyrimin për të informuar, të përcaktuar në nenin 18 të këtij ligji, dënohen me 10 000 deri në 300 000 lekë;

c) kontrolluesit, që nuk përmbushin detyrimin për të korrigjuar ose fshirë të dhënat, të përcaktuar në nenin 19 të këtij ligji, dënohen me 15 000 deri në 300 000 lekë;

ç) kontrolluesit ose përpunuesit, që nuk zbatojnë detyrimet e përcaktuara në nenin 20 të këtij ligji, dënohen me 10 000 deri në 300 000 lekë;

d) kontrolluesit, që nuk përmbushin detyrimin për të njoftuar, sipas përcaktimit në nenin 21 të këtij ligji, dënohen me 10 000 deri në 500 000 lekë;

dh) kontrolluesit ose përpunuesit, që nuk marrin masat e sigurisë së të dhënave dhe nuk zbatojnë detyrimin për ruajtjen e konfidencialitetit, të përcaktuara përkatësisht në nenet 27 dhe 28 të këtij ligji, dënohen me nga 10 000 deri në 150 000 lekë;

dh/1) kontrolluesit dhe përpunuesit, që veprojnë në kundërshtim me pikën 2 të nenit 32 të këtij ligji, dënohen me 100 000 deri në 1 000 000 lekë.

2. Personat juridikë, për kundërvajtjet e mësipërme, dënohen me dyfishin e gjobës së përcaktuar në pikën 1 të këtij neni.

3. Maksimumi i gjobës dyfishohet në rastin kur veprohet në kundërshtim me pikën 2 të nenit 16 të këtij ligji dhe kur të dhënat përpunohen pa autorizim, sipas shkronjës "b" të pikës 1 të nenit 31 të këtij ligji.

4. Gjobat vendosen nga Komisioneri, kur vërehet se janë shkelur detyrimet e përcaktuara në ligj.

Neni 40

Ankimi

Ndaj dënimit administrativ me gjobë bëhet ankim në gjykatë në afatet dhe sipas procedurave që rregullojnë gjykimin administrativ.

Neni 41

Ekzekutimi i gjobave

1. Gjobat paguhen nga kundërvajtësi jo më vonë se 30 ditë nga komunikimi i tyre. Me kalimin e këtij afati, vendimi i dhënë shndërrohet në titull ekzekutiv dhe ekzekutohet në mënyrë të detyrueshme nga zyra e përmbarimit, me kërkesë të komisionerit.

2. Gjobat arkëtohen në Buxhetin e Shtetit.

KREU X

DISPOZITA TË FUNDIT

Neni 42

Aktet nënligjore

Ngarkohet Këshilli i Ministrave të nxjerrë aktet nënligjore në zbatim të neneve 7, 8 e 21 të këtij ligji.

Neni 43

Shfuqizime

Ligji nr.8517, datë 22.7.1999 "Për mbrojtjen e të dhënave personale", shfuqizohet.

NISATEL OPERATOR PUBLIK I TELEKOMUNIKACIONEVE
Pavaresia 1200,
Vlore, Albania
E-mail: info@nisatel.al;
nisatel@hotmail.com;

Neni 44

Hyrja në fuqi

Ky ligj hyn në fuqi 15 ditë pas botimit në Fletoren Zyrtare.

Shpallur me dekretin nr.5671, datë 21.03.2008 dhe nr.7451, datë 08.05.2012 të Presidentit të Republikës së Shqipërisë,

Bamir Topi

NISATEL OPERATOR PUBLIK I TELEKOMUNIKACIONEVE
Pavaresia 1200,
Vlore, Albania
E-mail: info@nisatel.al;
nisatel@hotmail.com;

Aneks 2 - Deklarata e Konfidencialitetit të Mbrojtjes, Perpunimit, Ruajtjes dhe Sigurise së të Dhënave Personale.

Deklarata për "Mbrojtjen & Ruajtjen e të Dhënave Personale"

Datë: |__|__|__|__|__|__| 201_ **Nr. Serial:** |__|__|__|__|__|__|__|__|

Nr.Prot. |__|__|__|__|__|__|

Shoqëria

Shoqëria **"Nisatel " sh.p.k**

L."Pavaresia", Rr."Nermin Vlora", Vlore, 1200
Shqipëri
Tel: **+355 33 40 50 06**;

Përfaqësues: _____

Regjistrimi ne Gjykate Dt. **30.01.2002**

Punëmarrësi

Emri: _____ **Mbiemri:** _____

Vendlindja: _____ **Nr. identifikimit:** |__|__|__|__|__|__|__|__|__|__|

Datëlindja: |__|__|__|__|__|__| ddmmyy

1. Qellimi

Nënshkrimi i kësaj deklarate bëhet nga të gjithë punonjësit e shoqerise "**Nisatel**" sh.p.k. punonjësve të përkohshëm, vullnetarëve dhe palëve të tjera të cilët kanë akses në të dhënat personale per paitimtaret e internetit. Ajo përcakton kërkesat dhe përgjegjësitë e atyre që kanë akses në informacione të tilla dhe siguron që të gjitha palët e interesuara të kuptojnë detyrimet e tyre të konfidencialitetit.

2. Fusha e Veprimit

Fusha veprimi i kësaj deklarate shtrihet për të gjitha të dhënat personale dhe informacione konfidenciale që merren gjatë punës në shoqerinë Nisatel sh.p.k. Dispozitat përkatëse zbatohen edhe pasi marrëdhënia e punës me punëmarrësin ka përfunduar.

3. Informacion Konfidencial

Me anë të kësaj deklarate marr përsipër të mos përdor dhe të mos i transmetoj personave të paautorizuar të dhëna personale apo informacione konfidenciale të marra gjate periudhes se punesimit ne shoqerine Nisatel sh.p.k. përveç nëse autorizohem shprehimisht nga Nisatel sh.p.k. ose kërkohet me ligj. Pranoj dhe kuptoj se ky detyrim vlen gjatë afatit të punësimit si dhe pas përfundimit të tij.

4. Informacioni Konfidencial

☐ Me anë të kësaj deklarate marr përsipër të mos përdor dhe të mos i transmetoj personave të paautorizuar të dhëna personale apo informacione konfidenciale të marra gjate periudhes se punesimit ne shoqerine Nisatel sh.p.k. përveç nëse autorizohem shprehimisht nga Nisatel sh.p.k. ose kërkohet me ligj. Pranoj dhe kuptoj se ky detyrim vlen gjatë afatit të punësimit si dhe pas përfundimit të tij.

☐ Unë e kuptoj se jam i detyruar të ruajë konfidencialitetin për të dhënat personale dhe t'i mbajë ato të sigurta, duke marrë të gjitha masat organizative dhe teknike të përshtatshme.

☐ Unë e kuptoj se përdorimi dhe zbulimi i të dhënave personale në lidhje me individët, trajtohet nga ligji nr.9887, datë 10.03.2008 për "Mbrojtjen e të Dhënave Personale", i ndryshuar. Unë nuk do të përdorë ose përhap asnjë të dhënë personale që marr dijeni gjatë punës time për ndonjë qëllim që është në kundërshtim me qëllimet e kësaj pune.

☐ Marr përgjegjësinë e plotë që në rastin se konstatohet se kam vepruar në kundërshtim me udhëzimet në lidhje me konfidencialitetin e të dhënave personale apo në rast të mosrespektimit të tyre, ndaj meje të merren masa të menjëhershme.

Nënshkrimi

Sot më datë |__|__|__|__|__|__| **pasi u njoha me rregulloren e "Mbrojtjes, përpunimit, ruajtjes dhe sigurinës të te dhënave personale", kuptova dhe pranova qe ky veprim mban lart standardet perofesionale të shoqërisë Abissnet, si dhe nënshkruaj me vullnet të lirë kete deklarate.**

Punëmarrësi	**Përfaqësuesi i Shoqërisë**
_____	_____
Emër Mbiemër, Nënshkrim	*Emër Mbiemër, Nënshkrim*

NISATEL OPERATOR PUBLIK I TELEKOMUNIKACIONEVE
Pavaresia 1200,
Vlore, Albania
E-mail: info@nisatel.al;
nisatel@hotmail.com;

Ankes 2- Inventari i Shkeljeve të të Dhenave Personale

NISATEL OPERATOR PUBLIK I TELEKOMUNIKACIONEVE
Pavaresia 1200,
Vlore, Albania
E-mail: info@nisatel.al;
nisatel@hotmail.com;

NISATEL

ID	Username	Emer Atesia Mbiemer	Adresa	e-Mail	Dt e depozitimit te ankeses	Specifikimi i ankeses	Niveli i rrezikshmerise	Masat e marra	Data e njoftimit

NISATEL OPERATOR PUBLIK I TELEKOMUNIKACIONEVE
Pavaresia 1200,
Vlore, Albania
E-mail: info@nisatel.al;
nisatel@hotmail.com;

AQSCERT®

CERTIFICATE

FOR
INFORMATION SECURITY MANAGEMENT ISO/IEC 27001:2013

(PER MANAXHIMIN E SIGURISE SE INFORMACIONIT ISO/IEC 27001:2013)

Certificate No	AQS/SI/3592015
Name of company / *Emri i kompanise*	"NISATEL" Sh.p.k
Adress / *Adresa*	Lagjja "Pavarësia" Kulla e parë tek Rrethi Skelë kati 2 ,Vlore, Albania
Standart / *Standarti*	ISO/IEC 27001:2013

Concerning the following ISO/IEC 27001:2013 for services
(Është ne perputhje me standartin ISO/IEC 27001:2013 në fushat e meposhtme te aktiviteti)

Provision of internet services television, telephony, webhosting, FTTH, data trasmission directly to customers, building underground telecommunications networks, paving and instalation of cable networks (ADSL, optical fiber), fitting and installation of wireless technology.

Ofrimi i shërbimeve të internetit, televizionit, telefonisë, web hosting, FTTH, transmetimin e të dhënave direkt te konsumatorët, ndërtimin e rrjeteve nëntokësore të telekomunikacionit, shtrimi dhe instalimi i rrjeteve kabllore (ADSL, fiber optike), montimi dhe instalimi i teknologjisë wireless.

Validity of the certificate / *Vlefshmeria e certifikates*	First issue / *(Leshimi i pare)*	The first maintenance	The second maintenance	Expiry date / *(Data e skadences)*
	06/04/2015	within 06/04/2016	within 06/04/2017	05/04/2018

Direzione Technica
Dr. Ing Patrick Olivier

For Certification Body

AQSCERT

AQSCERT : FORO BUONAPARTE, 59 - 20121, MILANO, ITALY .
Rr. Gj. FISHTA, P. 5, AP. 9, TIRANE, Albania

PLANI I TRAJTIMIT OSE REAGIMIT NDAJ INCIDENTEVE TË SIGURISË DHE PLANI I VAZHDIMIT TË BIZNESIT NË RASTET E SITUATAVE TË JASHTËZAKONSHME APO KATASTROFAVE

Baza ligjore

Pika 1 e nenit 6 të Rregullores 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".

Detyrimet që burojnë nga Rregullorja nr.37 datë 29.10.2015 "Mbi masat teknike dhe organizative per te garantuar sigurine dhe integritetin e rrjeteve dhe/ose sherbimeve te komunikimeve elektronike", bëjnë që komopania jonë në fushën e komunikimeve elektronike të informojë Autoritetin e Komunikimeve Elektronike dhe Postare (AKEP) në rast se:

a) ndodh nje nga incidentet e meposhtme:

- *Mohimi i Sherbimeve Elektronike*
- *Kompromentimi i Sistemeve te Informacionit*
- *Manipulimi ose modifikimi i paautorizuar i të Dhenave Elektronike*
- *Software te demshem te cilet dergohen e jane nen kontrollin e drejtperdrejte te sipermarresit te komunikimeve elektronike (virus, spyware etj)*

b) te informojne AKEP rreth incidenteve te zbuluara te sigurise dhe/ose cenimit te integritetit, te cilat kane pasur, kane ose mendohet se do te kene nje impakt te rendesishem dhe / ose mesatar ne ofrimin e rrjeteve te komunikimit publik dhe/ose ne sherbimet e komunikimit elektronik publik te perdoruesit, jo me vone se 24 ore nga evidentimi i incidentit.

c) te implementojne mjetet dhe metodat e duhura teknike dhe organizative per te garantuar sigurine e rrjeteve te komunikimit publik dhe te sherbimeve te ofruara prej tyre. Keto mjete duhet te garantojne nivelin e sigurise ne perputhje me rrezikun e paraqitur dhe te evitojne ndodhjen e incidenteve te sigurise ose te reduktojne impaktin ose pasojat kur keto incidente ndodhin.

d) te implementojne mjetet e duhura teknike dhe organizative per te garantuar integritetin e rrjeteve te komunikimit publik, duke siguruar ne kete menyre ofrimin e panderprere te sherbimeve te tyre.

e) te menaxhojne dhe mbrojne pajisjet dhe sistemet e perdorura per ruajtjen e te dhenave te perdoruesve te rrjeteve te komunikimit publik dhe/ose sherbimeve.

f) të sigurojnë një nivel të mbrojtjes dhe sigurisë së përshtatshme ndaj rreziqeve të mundshme, të parashikuara. Masat e ndermarra nga sipermarresit duhet që, të paktën: - të sigurojnë që të dhënat personale të jenë të aksesueshme vetëm nga personeli i autorizuar bazuar në legjislacionin përkatës;

Lidhur me sigurinë, integritetin dhe mirëmbajtjen e funksioneve të rrjetit, kompania "NISATEL" shpk ka përcaktuar polikat, objektivat dhe direktivat per te parandaluar problemet e lindura ne lidhje me sigurine e informacionit dhe te dhenave. Këto politika trajtojnë mbrojtjen e aseteve te kompanise dhe klientit duke trajtuar si aset cdo informacionin të klientit, cdo informacion te kompanise, cdo rrjet transmetimi te informacionit, cdo pajisje softwerike apo hardware-ike te Teknologjise se Informacionit, cdo sherbim te ofruar prej kompanise sidhe burimet njerezore te kompanise.

Objektivi i ketyre politikave eshte te minimizoje demet e biznesit duke parandaluar ndikimin e incidenteve te lidhura me sigurine e informacionit dhe te **dhenave mbi vazhdimesine e biznesit si dhe duke mbajtur ne kontroll risqet aktuale.**

Personi Pergjegjesi i Sigurise se Informacionit ne kompanine tone ka keto pergjegjesi:

1. Te siguroje qe proceset e nevojshme per Sistemin e Sigurise se Informacionit dhe te dhenave qe ato te themelohen, zbatohen dhe te mirembahen.

2. Te raportoje mbi performancen dhe nevojat per permiresim e Sistemit te Sigurise se Informacionit dhe te Dhenave.

3. Te promovoje ne kompani ndergjegjesimin per kerkesat e sigurise se informacionit dhe te Dhenave.

4. Te krijoje, identifikoje dhe te perditesoje Politiken e Sistemit te Sigurise se Informacionit dhe te Dhenave.

Eshte pergjegjesia e çdo punonjesi te kompanise te ndjeke Politiken e Sigurise se Informacionit dhe te Dhenave.

Politikat;

Informacioni dhe te dhenat, trajtohen si aset dhe konsiderohen si prone e kompanise. Punonjesit jane pergjegjes per mbrojtjen dhe trajtimin me kujdes te aseteve te kompanise.

Konfidencialiteti eshte nje vlere shume e rendesishme e kompanise. Te gjitha llojet e informacioneve dhe te dhenave, mbrohen me sisteme me standart te larta te sigurise.

Informacioni dhe te dhenat nuk mund te shperndahen pa autorizimi zoteruesit e informacionit dhe te dhenave.

Siguria dhe mbrojtjta e informacionit te klientit eshte shume e rendesishme per kompanine. Per kete qellim ne kontratat e nenshkruara me klientet eshte percaktuar qarte masatqe do merren ne drejtim te dy paleve ne rast te shkeljes se kushteve te konfidencialitetit. Aktivitetet e jashteligjshme qe krijohen duke perdorur asetet dhe burimet e informacionit te kompanise nuk jane te pranueshme per kompanine.

Me poshte jane listuar disa nga aktivitetet te cilat jane te pa pranueshme nga kompania:

1. Demtimi i te dhenave

2. Perdorimi i informacionit dhe te dhenave per veprimtari te jashteligjshme

3. Shkaterrimi i pajisjeve, software-eve apo i çdo burimi informacioni

4. Vjedhja e pajisjeve, software-eve apo i çdo burimi informacioni

5. Perdorimi i burimeve te informacionit dhe te dhenave ne menyre jo korrekte duke shkaktuar humbje te performances se sistemeve te informacionit

6. Ofrimi i burimeve te informacionit paleve te treat apo kompanive konkurente

Keto aktivitete konsiderohen te jashteligjshme dhe cojne ne marrje te masave disiplinore sidhe proçedura respektive ligjore.

Incidentet e sigurise se informacionit dhe te dhenave, perpjekjet per aktivitete te jashteligjshme apo kanosjet te burimeve te informacionit duhet ti raportohen menjehere Personit Pergjegjes te Sigurise se Informacionit dhe te Dhenave.

Inventar per Riskun e Mbrojtjes se te Dhenave Personale

Nr. Risku

Emertimi i Riskut

Trajtimi dhe Plan veprimi

Nr.Mbrojtja e te dhenave personale

Veprimi identifikues

Opsionet e trajtimit

Veprimet e marra

Pergjegjes

Data e konstatimit

MENAXHIMI I RISKUT

Qellimi i kesaj politike eshte te siguroj kontroll te vazhdueshem sidhe te siguroj mbajtjen ne nivele te ulta te risqeve te Sigurise se Informacionit.

Personi pergjegjes per Menaxhimin e Riskut ka per detyre zbulimin dhe identifikimin e kercenimeve perpara se ato te ndodhin duke bere te mundur planifikimin dhe veprimtarine parandaluese gjate kohes kur nje proces, aktivitet apo sherbim eshte duke u ekzekutuar.

Personi pergjegjes per Menaxhimin e Riskut eshte pergjegjes per:

- Identifikimin dhe raportimin e riskut ne menyre te pershtatshme drejt administratorit te kompanise, menaxhereve te tjere te kompanise, punonjesve te kompanise.

- Vleresimin dhe percaktimin e nivelit te riskut qe eshte i pranueshem dhe atij niveli i cili I kalon normat e mirefunksionimit te procesit, aktivitetit apo sherbimit.

- Ofrimin e informacionit per numrin e kercenimeve dhe nje informacion te detajuar mbi secilin prej tyre sebashku me nivelin e humbjeve qe ato shkaktojne.

- Organizimin e nje mbledhjeje periodike per informimin e kercenimeve ekzistuese sidhe masave te marra drejt kercenimeve te meparshme.

Personi pergjegjes per Menaxhimin e Riskut duhet te zbatoje nje procedure standarte per identifikimine e kercenimeve. Hapat qe duhet te ndiqen jane te listuara si me poshte:

- Analiza e Riskut e cila eshte procedura e pare ku aplikohet identifikimi i proceseve kur risqet e mundshme mund te iniciojne. Gjate kesaj faze kryhet edhe analiza per percaktimin e aseteve qe bejne pjese ne procedurat te cilat jane te zbuluara kundrejt ketij risku, kercenimet e ketyre aseteve, dobesimet e mundshme te tyre sidhe ndikimi ne teresine e sistemit nga ky kercenim.

- Vleresimi i Riskut i cili perfaqeson proceduren e nivelit te rezikut qe ky risk shfaq, periudhes kohore kur ky risk eshte i shfaqur sidhe frekuences se perseritjes se ketij risku.

- Trajtimi i Riskut i cili perfaqeson proceduren e veprimtatise se menaxhuesit te riskut per te ndaluar kete rist. Veprimtaria perbehet nga pikat e meposhtme:

- Vendosja ne kontroll e riskut.

- Minimizimi i riskut deri ne nivelet e pranueshme per sistemin.

- Eleminimi i riskut.

- Marrja e masave parandaluese per mos shfaqet e riskut te eleminuar.

Disa nga Risqet dhe kategorizimi i tyre eshte pershkruar si me poshte:

- Risqet nga burime njerezore:

- Publikim i Informacionit

- Kopje te informacionit jashte infrastrukturave te kompanise

 Vjedhje e informacionit

 Mos kryerje e detyrave specifike duke sabotuar sistemet

 Aktivitete joetike drejt aseteve te kompanise

- Risqe Natyrore:

 Zjarr

 Temperatura te larta apo te ulta

 Termete

 Permbytje

 Rrufe

 Lageshtire

- Risqe nga pa pergjegjshmeria:

 Viruse

 Humbje dokumentacioni

 Demtime te pavullnetshme te aseteve

 Gabime ne perdorimin e sistemeve

 Hedhje e materialeve te lengshme ne infrastriktura te ndrryshme.

SIGURIA E BURIMEVE NJEREZORE

Politikat e Burimeve Njerezore mbi sigurine, kontrollin, trajnimin si dhe trajtimin e shkeljeve

Qellimi i ketyre politikave eshte te siguroj nje kontroll te detajuar mbi personelin e kompanise.

Trajnimi i Kandidateve;

Zhvillimi i punonjesve permes trajnimit dhe edukimit te tyre mbi gjithe proceset dhe procedurat qe keta punonjes do kryejne ne kompani. Programet trajnuese jane dizenjuar per te zhvilluar aftesite e personelit ne kryerjen e pergjegjesive te percaktuara ne kompani. Nje element i programeve te trajnimit eshte dhe informimi I punonjesve mbi politikat e sigurise se informacionit sidhe politikat e trajtimit te shkeljeve apo akteve jashteligjore.

Aktiviteti i Punonjesit ne lidhje me Sigurine e Informacionit;

Gjate ushtrimit te pergjegjesive te percaktuara ne kompani punonjesi informohet mbi konfidencialitetin si nje ceshtje shume e rendesishme ne kompani.

SIGURIA E SISTEMEVE DHE PAJISJEVE

Siguria Fizike

Dhoma e Serverave dhe te gjithe aparaturave qe mundesojne lidhjen e rrjeteve te komunikimit eshte e vendosur ne nje ndertese, qe ploteson te gjitha kriteret e sigurise se objekteve me rendesi te vecante. Normat e sigurise survejimin me kamera qe transmetojne imazhe ne kohe reale tek personeli i autorizuar per mbikqyrjen dhe mirembajtjen.

Aksesi fizik eshte i rezervuar per nje numer te vogel personash. Ambjeti mbahet ne temperature konstante dhe pastrohet rregullisht per pluhura dhe grimca qe trasportohen nepermjet ajrit, qe mund te demtojne procesoret dhe sistemet e ventilimit te pajisjeve

Rrjeti i ISP eshte i mbrojtur nga Firewall per te evituar sulmet ne porta te ndryshme te aksesit. Rrjetet e menaxhimit jane te vendosura ne VLAN te vecuar dhe aksesohen vetem nga sherbimet VPN. Kontrolli dhe vezhgimi i aksesit ne rrjet monitorohet nepermjet Logfile te serverave.

Serverat dhe routerat perditesohen me versionet me te fundit te sistemeve operative dhe normave te sigurise nga burime zyrtare te kompanive qe ofrojne suportin e ketyre sistemeve.

SIGURIA E RRJETEVE, SISTEMEVE DHE APLIKACIONEVE MBESHTETESE

Komapnia jone nderton, ofron dhe zhvillon nje rrjet te komunikimeve elektronike me fibra optike dhe rrjet wireless me disa akses pointe te deklaruara dhe te regjistruara ne AKEP. Rrjeti me fibra optike shtrihet ne zonen/zonat e Autorizimit dhe sa here te kemi ndryshime ne kete rrjet, ato do raportohen periodikisht ne AKEP sipas rregullores per Atlasin Elektronik.

Rrjeti me baker suportohet me paisje ADSL2+ ku paisjet kryesore jane DSLAM dhe ne terren modema adsl2+ te modeleve te ndryshem.

Rrjeti me fibra optike suportohet me pajisje EPON/GPON te teknologjive te fundit ku pajisjet kryesore jane ato OLT dhe pajisjet ne terren jane ONU-te.

Per te marre internetin nga provideri ne perdorim nje ruter qendror i cili lidhet me pajisjen switch, pastaj me pajisjen OLT ose DSLAM e cila ka kapacitet te zgjerueshem ne varesi te numrit te klienteve.

Gjithashtu cdo akses point ka nje tjeter ruter Mikrotik, per te rritur efektet e sigurise si dhe per ta aksesuar ne rruge te mbyllur. Pas paisjes switch vendoset nje paisje ruter Mikrotik Cloud Core per te ndare rrjetin tim nga provideri internet por edhe per te ndare ngarkesen ne rrjetin e fibres optike me rrjetin e akses pointeve.

Ruteri Mikrotik i akses pointeve ben menaxhimin dhe funksionimin me internet te antenave ne frekuencat e lira, dhe kontrollon kapacitetin e internetit te klienteve. Ky ruter eshte me IP reale.

Paisja Mikrotik instalohet ne panelin e paisjeve ne zyre dhe ka energji te vazhdueshme elektrike e garantuar me inverter me bateri qe mbajne deri ne 12 ore. Kulla eshte e garantuar me tokezim te mire per te mbrojtur pajisjet e mia nga shkarkimet atmosferike qe ne ate pike jane shume te shpeshta ne shume muaj te vitit.

Energjia stabilizohet me stabilizator tensioni per te perballuar ngarkesen elektrike qe konsumojne pajisjet ne rack.

Disa nga funksionet e pajisjeve ruterave qendrore Mikrotik jane:

1. Krijim rrjeti te qenderzuar i cili ofron besueshmerine e te dhenave dhe backup te sigurte

2. Implementim sigurie i te dhenave pavaresisht nga cila pike e rrjetit.

3. Percaktimi i te drejtave te nje perdoruesi , username dhe password per autentifikim.

4. Krijim lidhjesh private (VPN) mes pikash larg njera-tjetres, pavaresisht nga distanca mes tyre.

5. Segmentim i rrjetit te brendshem aty ku eshte e nevojshme

6. Realizimi i lundrimit te sigurt ne internet duke ngritur firewaalin e brendshem te tij i paraprogramuar me te gjitha mbrojtjet ndaj sulmeve drejt rrjetit.

Protokollet e punes dhe komunikimit te Mikrotikut jane te mbrojtura dhe te kriptuara, dhe garantojne:

1. Authentifikimin (Authentication)

2. Fshehtesine (Confidentiality)

3. Menaxhimin e celesave (Key Management)

Authentifikimi-logimi i cdo user kryhet permes kodit HMAC (Hash based Message Authentication Code) me username dhe password personal. Siguria e ketij kodi varet drejteperdrejt nga siguria e hash funksionit me te cilin eshte llogaritur.

Tipari kryesor i tij eshte mundesia e authentifikimit dhe kriptimit te te gjithe trafikut nepermjet Internet Protocol.

Firewalli i Mikrotikut ndihmon ne filtrimin e trafikut ne internet, duke percaktuar rregulla strikte ndaj sulmeve dhe duke krijuar memorjen e nevojshme ne raste sulmesh, keshtu qe programe te demshme dhe hakere nuk kane asnje mundesi te kalojne Mikrotikun.

POLITIKAT E SIGURIMIT FIZIK, TE MJEDISIT DHE BURIMEVE

Qellimi i ketyre politikave eshte te siguroje parandalimin e rreziqeve qe perbejne asetet fizike, mjedisin e punes sidhe burimeve te ndrryshme.

Kjo politike aplikohet ndaj gjithe aseteve qe perbejne, jane pjese apo ndikojne ne shkembimin e informacionit ne kompani. Kjo politike mbulon gjithe ambientet e sistemeve te informacionit ku kompania kryen aktivitetin e saj.

Sigurimi Fizit i Aseteve te Kompanise;

Cdo aset i kompanise eshte i izoluar nga cdo akses fizik i jashtem.

Aksesimi i paautorizuar ne pajisjet e kompanise eshte parandaluar duke bllokuar dhe cdo lloj porte fizike apo virtuale. Te pa bllokuar jane vetem ato porta ku aksesi eshte i kontrolluar, enkriptuar dhe i mire izoluar nga kercenimet e jashtme.

Aksesi ne asetet e kompanise eshte gjithashtu i shkallezuar me nivele te ndryshme te drejtash ne cdo pajisje si pjese e kompanise.

Siguria fizike eshte gjithashtu e kontrolluar nepermjet nje kompanie te kontraktuar per te ushtruar aktivitetin e saj. Kjo kompani mbulon sigurine e kompanise 24 ore ne te 7 ditet e javes. Thyerja e rregullave te sigurise fizike dhe aksesi i paautirizuar i nje punonjesi apo personi te jashtem ne ambjentet e vecuara te kompanise ben te mundur aktivizimin e sistemit te sigurise se kompanise kontraktuale dhe veprimin e menjehershem te saj.

Kontrolli i funksionalitetit te sistemit te sigurise fizike behet cdo muaj ku nje stimulim i thyerjes se sistemit kryhet per te matur kohen e pergjigjes. Gjithashtu gjate ketij stimulimi matet edhe riskun gjate periudhes se thyerjes se sistemit dhe kohes se pergigjes.

Sigurimi i Mjedisit nga Katastrofat Natyrore;

Cdo ambjet ne te cilin sistemet e informacionit jane te vendosura eshte implementuar sistemet e sigurise ndaj katastrofave natyrore.

Ne cdo ambjen jane vendosur pajisjet e izolimit dhe ndalimit te zjarrit. Cdo sistem apo pajisje e sistemeve te informacionit eshte vendosur ne nje nivel mbi bazamentin fundor per te siguruar ruajtjen nga permbytjet apo lageshtia. Pajisjet e implementimit te sistemeve te informacionit jane izoluar hermetikisht per te bllokuar rrezigjet e jashtme.

Siguria e Burimeve;

Politika e kompanise per sigurine e burimeve eshte qe cdo burim i cili siguron mbarevajtjen e sistemeve te informacionit te jete i garantuar ne vazhdueshmerine e tij nga sistemet e backup-it.

Sistemi i sigurimit te energjise elektrike per furnizimin e sistemeve te informacionit eshte i siguruar me nje system backup i perbere nga UPS (Furnizues i Panderprere i Energjise) i cili eshte gjate gjithe kohes aktive. Sistem Inverter dhe Baterish i cili hyn ne fuqi pas nderprerjes se energjise elektrike. Sidhe sistemi i furnizimit me energji elektrike me ane te gjeneratoreve elektrike ne rast te nje nderprerje te energjise eleketrike per nje periudhe disa orarshe.

Sistemi i Ftohjes per sistemet e informacionit eshte i aktivizuar ne cdo kohe dhe lidhet me sistemin e backup-it te energjise elektrike ne rast nderprerje te saj.

POLITIKAT E KONTROLLIT TE AKSESIT

Qellimi i kesaj politike eshte percaktimi i kerkesave mbi sigurine per te pasur nje akses te kontrolluar mbi burimet e informacionit.

Kjo politike aplikohet ndaj gjithe perdoruesve te aseteve te informacionit perfshire punonjesit e kompanise sidhe klientet te cilet perdorin pajisjet transmetuese te sherbimit te ofruar prej kompanise.

Kjo politike mbulon te gjitha ambientet e Sistemeve te Informacionit ku kompania operon.

Politika;

Kontrolli i aksesit eshte i nevojshem per sistemet pasi kane ne perberje te dhena sensitive dhe nevojiten te kene akses te kufizuar. Kjo politike pershkruan procedurat e perodurura per te kontrolluar akseset me qellim sigurimin e informacionit.

- Aksesi ne informacion duhet te jete i autorizuar ne menyre specifike.

- Aksesi ne informacion duhet te kontrollohet bazuar ne kerkesat e kompanise, dhe rregullave specifike te percaktuara per çdo sistem informacioni.

- Te gjithe punonjesit e kompanise duhet te aksesojne vetem ato asete dhe sisteme te informacionit te cilat jane te nevojshme per te permbushur detyrat e tyre te punes.

Te gjithe perdoruesit duhet te pajisen me nje deklarate me shkrim ose elektronike mbi te drejtat e aksesit te tyre, termat dhe kushteve per perdorimin e ketyre te drejtave.

Llogaria e perdoruesit duhet te rishikohet çdo 2 muaj per privilegjet e duhura.

Llogarite e perdoruesve te cilet largohen nga kompania duhet te hiqen menjehere mbas perfundimit te punes se tyre.

Te gjitha privilegjet e perdoruesve fillestar dhe ekzistues duhet te caktohen nepermjet nje autorizimi te Administratorit te kompanise.

Te gjithe perdoruesit duhet te zbatojne Politiken e Fjalekalimit.

Politika e Fjalekalimit perben krijimin e nje fjalekalimi komplekt ne te cilin perfshihen 4 lloje te ndrryshme kategorish te karaktereve sidhe nje gjateso jo me pak se 8 karaktere.

Te gjitha fjalekalimet qe i perkasin Administratorit te Sistemit i cili ka dhene doreheqje ose eshte pezulluar duhet te ndryshohen.

Kontrolli i aksesit te rrjetit;

Aksesi ne rrjete sherbime te rrjetit do te kontrollohet mbi bazen e kerkesave te sigurise dhe biznesit, dhe rregullave te kontrollit te aksesit te percaktuara per çdo rrjet.

Rrjetet e sistemeve te informacionit te kompanise duhet te ndahen ne segmente logjike bazuar ne nevojat e aksesit. Rrjeti i brendshem duhet te ndahet nga rrjeti i jashtem me kontrolle te ndryshme te sigurise rrethuese ne secilin prej rrjeteve. Lidhja ndermjet rrjeteve te brendshme dhe te jashtme duhet te kontrollohet.

Mekanizmat e duhur per kontrollin e rrugezimit duhet te implementohet per te kufizuar rrjedhen e informacionit ne rruget e rrjetit te percaktuar brenda kontrollit te kompanise. Kontrollet e rrugezimit te rrjetit duhet te bazohet ne burimet pozitive dhe mekanizmat e kontrollit te adreses se destinacionit.

Te gjitha sistemet e rendesishme dhe delikate si Router-at Kryesore qe Menaxhojne Rrjetin dhe Sistemi i Menaxhimit te Abonenteve duhet te kene nje arkitekture te mbyllur dhe shume te sigurt.

Monitorimi;

Te gjitha detajet e ngjarjeve lidhur me sistemin e informacionit duhet te logohen dhe ruhen per 1 muaj per sistemet e zakonshme dhe 2 muaj per sistemet kritike.

Te gjitha sistemet e informacionit dhe aplikacioni i biznesit duhet te monitorohet ndersa rezultatet e monitorimit duhet te rishikohen periodikisht. Te gjitha oret e sistemit duhet te sinkronizohen dhe rishikohen per pasaktesite dhe luhatje. Nje perpjekje e pasuksesshme login ne serverat kritik duhet te regjistrohet, investigohet, dhe pershkallezohet tek eprori i linjes se pare.

Menaxheri duhet te sigurojne monitorim te vazhdueshem dhe ne pajtueshmeri brenda kompanise.

POLITIKA E INTEGRITETIT TE SISTEMEVE DHE RRJETIT

Kjo politike garanton mbrojtjen e infrastruktures se sistemeve te informacionit nepermjet sistemit te antivirus-eve. Kjo politike pershkruan masat e ndermarra per te mbrojtur sistemet e kompanise nga viruset, Trojan-et, spyware, spamet, etj.

Kjo politike aplikohet ne te gjithe sistemet e informacionit te kompanise duke perfshire pajisjet e transmetimit, sistemet e IT sidhe sistemet e rendesise se vecante.

Personi pergjegjes analizon dhe shperndan perditesimet e mundshme te sistemeve te antiviruseve.

Politika;

Te gjitha sistemet e cenueshme nga sulmet e viruseve, malware, spam,etj. duhet te mbrohen nga software antivirus sa here te jete e nevojshme, perveç se kur lejohet nje perjashtim specifik dhe merren masa alternative per te garantuar te njejten shkalle mbrojtjeje.

Burime potenciale te viruseve perfshijne mjete te perbashketa si CD, USB, poste elektronike bllokohen dhe kontrollohen paraprakisht dhe me pas lejohen te punohet mbi to.

Te gjithe punonjesit qe perdorin pajisjet e kompanise duhet te perdorin gjate gjithe kohes disa praktika te cilat jane listuar si me poshte:

- Te tregojne kujdes kur hapin materialet bashkangjitur postes elektronike dhe ti kontrollojne per viruse perpara se ti hapin. Duhet te shtypin opsionin scan paraprakisht.

- Te tregojne kujdes kur hapin materiale nga mjete te tilla si USB ose CD. Duhet te shtypin opsionin scan paraprakisht.

- Te skanojne te gjitha mjetet e jashtme per viruse perpara se ti perdorin.

- Te njoftojne me email Personin pergjegjes te sistemeve te antiviruseve ne rast te nje sulmi nga virus-et.

- Punonjesit qe jane te autorizuar qe te lidhin kompjuteret e tyre me rrjetin e kompanise duhet te sigurohen se kompjuteret qe ata perdorin jane te mbrojtur nga viruset dhe perputhen me standardet e percaktuar ne kete politike.

Duhet te perditesohen sa here eshte e mundur ne baze te sistemit te antiviruseve cdo produkt qe kryen funksionin e nje antivirusi.

Personi pergjegjes per sistemet e antiviruseve duhet te mbedh log-et nga keto sisteme per te analizuar, identifikuar edhe eleminuar mundesi te tjera te mundshme te sulmeve nga antiviruset.

Duhet te aktivizohen ne cdo pajisje te punonjesve sistemet e sigurise se postes elektronike.

MENAXHIMI I OPERACIONEVE

Politikat e Menaxhimit te Operacioneve

Qellimi i kesaj politike eshte te percaktoje proceset operacionale per pajisjet dhe sistemet, si dhe ti mirembaj ato. Proceset e mirembajtjes mbulojne teresine e proceseve, veprimeve ose funksionimit ndaj te gjithe pajisjeve, sistemeve dhe sherbimeve te infrastruktures se rrjetit ne kompani. Keto politika sigurojne funksionimin e panderprere te te gjithe elementeve te rrjetit te kompanise.

Proceset

Keto politika ndahen ne disa kategori ne baze te hapave qe ndiqen per realizimin e nje operacioni:

- Planifikimi

- Implementimi

- Testimi

- Monitorimi

Planifikimi;

Planifikimi i nje operacioni do te thote krijimi i detajuar i instruksioneve te funksionimit te tij. Keto instruksione do te ndiqen perpikmerisht gjete hapave te implementimit dhe monitorimit. Krijimi i dokumentacionit te planifikimit duhet te jete i mire detajuar ne cdo aspekt teknike duke perfshire edhe lidhjen dhe ndikimin me operacine te tjera te tij.

Ne fazen e planifikimin dhe ne kalimin e metejshem te hapave te mesiper bejne pjese dy lloje operacionesh.Operacione te cilat jane pjese e nje sistemi apo sherbimi te ri te planifikuar per implementim. Sidhe operacione te cilat kan funksion mirembajtes, update-ues apo ndrryshues ne sistemet ose sherbimet ekzistuese te infrastruktures se rrjetit.

Implementimi;

Implementimi eshte faza ne te cilen versioni perfundimtar i planifikimit vihet ne zbatim. Gjate kesaj faze duhet te behen implementimet perkatese ne pajisjet apo sistemet qe bejne pjese ne kete operacion sidhe ne ato pajisje apo sisteme qe kane nje lidhje llogjike apo fizike me funksionimin e ketij operacioni por qe nuk jane pjese se tij.

Gjate fazes se implementimit duhet te merret parasysh numri i burimeve te nevojshme per kryerjen e saj sidhe periudha kohore gjate te ciles ky operacion do kryhet.

Implementuesi i ketij operacioni duhet te mari ne konsiderate kryerjen e tij gjate periudhes e cila ndikon me pak ose nuk ndikon ne performancen e asnje sherbimi apo nje sistemi.

Implementuesi i ketij operacioni duhet te dokumentoje cdo proces te kryer gjate operacionit sidhe vlerat e dhena ne konfigurimin perfundimtare ne rast kur ky process konsiston ne konfigurimin e nje pajisje apo sistemi.

Testimi;

Procesi i testimit konsiston ne matjen e parametrave te percaktuara gjate fazes se planifikimit. Vlerat e nxjerra nga matja e elementeve te operacionit te implementuar nuk duhet te jene te ndrryshme nga ato te percaktuara ne planifikim. Bejne perjashtim ato vlera te cilat ne fazen e planifikimit jane percaktuar me nje nivel ndrryshimi por duhet te jene brenda parametrave te lejuara te ndrryshimit.

Cdo proces testimi se bashku me vlerat e nxjerra prej tij duhet te dokumentohet.

Gjate ketij procesi duhet te stimulohen edhe incidentet e ndrryshme te percaktuara ne fazen e planifikimit dhe impakti i tyre

ne nje pjese apo ne teresi te sistemeve dhe sherbimeve.

Procesi i testimit duhet te kryhet me shume se nje here sidhe duhet te kryhet gjate fazave te ndrryshme kohore gjate te cilit sistemi apo sherbimi ku ky operacion ben pjese ka sjellje apo vlera te ndrryshme.

Monitorimi;

Procesi i monitorimit eshte procesi me i rendesishem i fazes se menaxhimit te operacioneve. Pasi funksioni i ketij procesi eshte te kryej monitorimin dhe menaxhimin e operacionit i cili eshte pjese apo eshte ne teresi vete sherbimi ose sistemi I infrastruktures se rrjetit.

Monitorimi i proceseve kryhet ne dy menyra.

Menyra e pare eshte monitorimi i historise se funksionimit te procesit. Gjate ketij monitorimi personi pergjegjes kryen matje dhe analize mbi vlerat e meparshme te procesit nese ato jane brenda normave te percaktuara ne dokumentacionin perkates te operacionit.

Menyra e dyte eshte monitorimi ne kohe reale i procesit. Gjate ketij monitorimi personi pergjegjes merr ne konsiderate vlerat aktuale te procesit dhe i analizon ato duke i krahasuar me normat e parapercaktuara.

Te dy menyrat e monitorimeve te mesiperme mund te kryhen ne menyre te skeduluar ne varesi te kohes se percaktuar ne planifikimin e operacionit.

Gjate kesaj faze duhet te percaktohet dhe monitorohen edhe vlerat e burimeve te nevojshme per funksionimin e ketij operacioni te percaktuara ne fazen e planifikimit. Ne kete lloj monitorimi duhet te perdoren te dy menyrat e monitorimit.

Cdo vlere e regjistruar gjate fazes se monitorimit duhet te dokumentohet ne dokumentacionin perkates te operacionit apo sistemit te operimit.

Sistemet Operacionale te Backup;

Keto sisteme bejne pjese ne operacionet te cilet kryejne funksionin e tyre ne rast se cdo sistem apo sherbim nuk funksionin ose funksionimi i tij eshte jashte vlerave te lejuara.

Sistemet Operacionale te Backup duhet te jene te implementuara dhe te konfiguruara ne menyre qe ne rast mos funksionimi te sistemeve paresore sherbimet apo infrastruktura ne teresi e rrjetit te mos ndikoje nga mos funksionimi i nje pjese te tij.

Gjendja aktive e sistemeve operacionale te backup eshte ne varesi te cdo operacioni. Ne nje pjese te operacioneve eshte e nevojshme mos qendrimi aktive I ketyre sistemeve. Ndersa ne pjese te tjera operacionale eshte e nevojshme qendrimi i sistemeve operacionale te backup aktive.

Ne secilin nga operacionet ose funksionet e ndrryshme te sistemit ose sherbimeve duhet te jene te percaktuara dhe te dokumentuara sistemet operacionale te backup ne tre elementet perberes te tyre:

- Menyra e Funksionimit

- Vlerat e Funksionimit

- Koha e aktivizimit

Menyra e funksionimit percakton menyren se si sistemet operacionale te backup do kryejne funksionin e zevendesimit te sistemeve paresore.

Vlerat e funksionimit percaktojne vlerat te cilat sistemet e mesiperme do zevendesojne vlerat e sistemeve paresore.

Koha e aktivizimit percakton kohen e nevojshme te hyrjes ne funksion te sistemeve operacionale te backup nga momenti I nderprerjes se funksionimit te sistemeve paresore.

Per cdo sistem ose sherbim te infrastruktures se rrjetit te kompanise duhet te dokumentohen sistemet operacionale te backup dhe tre elementet e siperpermendur te tyre.

MENAXHIMI I INCIDENTEVE TE SIGURISE

Politikat e Menaxhimit te Incidenteve te Sigurise

Kjo politike kryen funksionin e raportimit dhe regjistrimit te incidenteve, vlerave jashte standarteve normale te funksionimit dhe masave te marra ne keto situata. Ne kete politike jane te perfshire te gjithe llojet e incidenteve qe lidhen me sistemet, pajisjet apo sherbimet e infrastruktures se rrjetit te kompanise.

Te gjithe punonjesit e kompanise duhet te raportojne dhe te informohen per cdo regjistrim incidenti qe ka ndikim ne procesin e punes se tyre.

Raportimi;

- Incidentet duhet ti komunikohen personit pergjegjes per regjistrimin e tyre.

- Duhet te zbatohen procedurat operacionale kur ky incident ndodh duke perfshire ekzaminimin, izolimin dhe masat e rikuperimit.

- Duhet te raportohen te gjithe procedurat e marra gjate procesit te ekzaminimit, izolimit dhe rikuperimit te sherbimin apo sistemit.

- Duhet te raportohen rezultatet e zgjidhjes se incidentit dhe vlerat e mbylljes se tij.

- Duhet te merren masa ndaj shkakut te ndodhjes se ketij incidenti perfshire burimet, proceset e punes apo individet.

- Identifikuesit e incidentit nese nuk jane personi pergjegjes i menaxhimit te incidenteve nuk duhet te nderhyjne ne riparimin e tij por duhet vetem te raportojne personin pergjegjes.

Me poshte jane te listuar kategorite ne te cilat incidentet grupohen:

- Nderprerje e sherbimit

- Difekte ne sistem apo sherbim

- Renie e cilesise se sherbimit

- Demtim hardware apo software i pajisjeve

- Vjedhje e pajisjeve

- Gabime njerezore

- Thyerje e sigurise

Nje grupin i rendesishem i incidenteve jane ato incidente te lidhura me cenueshmerine e sigurise se informacionit. Per kete arsye cdo punonjes i kompanise duhet te jete i vemendshem nda ndonje akti apo situate te cenuesshmerise se sigurise se informacionit duke raportuar menjehere tek personi pergjegjes.

Monitorimi;

Personi pergjegjes per menaxhimin e incidenteve duhet te jete ne gjendje jo vetem te identifikoj, regjistroj dhe analizoj nje incident por edhe te marri masa paraprake per identifikimin e incidenteve te ndrryshem. Per kete arsye duhet te kryhen monitorime apo te ngrihen sisteme

sigurie dhe alarmi ne menyre qe nje ngjarje e padeshiruar te identifikohet dhe te bllokohet pa kryer funksionin e saj.

Monitorimi duhet te kryhet per disa elemente thelbesore te sistemeve dhe sherbimeve te kompanise si:

- Funksionimi apo renia e sherbimeve ose sistemeve

- Sulme nga persona apo software te jashtem

- Aksese te pa kontrolluara ne sisteme apo pajisje

- Nderprerje e pa paralajmeruar e burimeve te ndrryshme

- Gabime njerezore ne operimin e sistemeve apo pajisjeve

Permiresimi;

Mbas zbulimit te shkakut te incidentit dhe marrjes se masave kundrejt tij duhet te zbatohen procedurat e permiresimit te operacioneve te ndikuara ne incident ne menyre qe te eleminohen raste te ngjashme ne te ardhmen. Disa nga procedurat qe duhet te zbatohen ne kete faze jane te listuara me poshte:

- Analiza e incidentit

- Identifikimi i shkakut te incidentit

- Izolimi i procesit, operacionit, sistemit apo pajisjet qe ka shkaktuar incident

- Planifikim i masave parandaluese ne raste te tilla te ngjashme

- Analize e rekordeve per incidente te ngjashme per te marre masat e duhura ne parandalimin e tij . Raportimi i Incidenteve do te kryhet ne nje sistem rekordesh sipas skemes se meposhtme dhe duhet te perditesohet nga personi pergjegjes i menaxhimit te incidenteve.

MENAXHIMI I VAZHDIMIT TE BIZNESIT

Politikat e vazhduesshmerise se sistemeve dhe sherbimeve

Qellimi i ketyre politikave eshte te krijojne nje procedure operacionale per te lejuar vazhdueshmerine e sistemeve dhe sherbimeve ne raste incidentesh apo katastrofe natyrore.

Me marrjen e masave dhe kryerjen e procedurave operacionale do te bej te mundur qe kompania te:

- Vazhdoj ofromin e sherbimit.

- Vazhdoj ruajtjen e informacionit te kompanise dhe klienteve te saj

- Venien ne fuqi te sistemeve operacionale te backup

- Kete humje minimale ne sherbim dhe funksionin te proceseve

- Ndaloj ndikimin e tyre ne mireqenien e punonjesve apo klienteve te kompanise

Aplikimi

Me poshte eshte diagrama e hapave qe merren ne rastin e nje incidenti apo katastrofe natyrore:

Operacione Standarte

Incidet apo Fatkeqesi Natyrore

Izolim i Procesit te Perfshire

Ngritja e Sistemeve Operacionale te Backup

Rikuperim I Procesit

Implementim I Operacioneve Standarte

Informimi;

Duhet te behet e mundur dallimi i katastrofes apo incidentit duke i kategorizuar ato. Ne kete menyre per cdo kategori te meren masat dhe aksionet perkatese per evitimin, izolimin dhe eleminimin e tyre. Kategorite jane si me poshte:

- Natyrore

 Zjarr Termet Permbytje

- Njerezore

 Shperthim Kimike Difekt ne proces pune Vjedhje Humbje

- Infrastrukture Sisteme te ndaluara Energji e nderprere Humbje komunikimi Ftohje/Ngrohje jashte normave te lejuara

- Teknologji Informacioni Sulme Cybernetike Demtim Hardware Kodim I gabuar Humbje te dhenash Demtim Software Gabime Njerezore

Veprimet e Rikuperimit

Elementi me i rendesishem i menaxhimit te situatave te emergjences eshte koha e pergjigjes ndaj situatave te tilla. Per kete arsye duhet te kategorizihet lloji I situates se emergjences dhe koha e pergjigjes respektive.

Niveli i Prioritetit;

Pershkrimi i Sistemit apo sherbimit

Koha e Pergjigjes, Kritike

-Sistemi apo Sherbimi eshte jo aktive

-Pjese kritike te Sistemit apo Sherbimit nuk eshte funksional

-Veprimtari jashte standartit te Sistemit apo Sherbimit

-Humbje e te Dhenave sensitive te kompanise

0-6 Ore, I Larte

-Pjese te rendesishme te Sistemit apo Sherbimit nuk jane funksional

-Aksese te pjesshme ne Sisteme apo Sherbime nuk jane aktive

7-14 Ore, Mesatar

-Sistemet apo Sherbimet jane duhe funksionuar por nje pjese e vogel e tyre nuk funksionin brenda standarteve

-Instalime te ndrryshme kane pasur incidente minimale

15-24 Ore, I Ulet

-Probleme minimale qe nuk ndikojne ne funksionalitetin e punes

-Probleme minimale qe nuk ndikojne ne ofrimin e sherbimit

24-72 Ore

POLITIKAT E LOGIMIT

Qellimi i kesaj politike eshte te menaxhosh

sistemin e ruajtjes dhe perdorimit te logeve te gjeneruara gjate gjithe aktiviteteve te sistemeve ose sherbimeve kryesore ne infrastrukturen e rrjetit te kompanise. Te dhenat e logeve permbajne informacion te detajuar te aktiviteteve mbi pajisjet, aplikacionet, sistemet dhe sherbimet qe bejne pjese ne infrastrukturen e rrjetit.

Pajisjet e rrjetit duke perfshire router, akses point apo switch mund te gjenerojne informacione prej logeve duke informuar administratorin e rrjetit mbi aktivitetet e kryera ne keto pajisje.

Aplikacionet mund te identifikojne veprimet e kryera ne to, kohen e kryerjes dhe qellimin prej logeve te regjistruara.

Sistemet apo sherbimet jane te kategorizuar ne elemente te infrastruktures se rrjetit te cilat do implementohet sistemi i regjistrimit te logeve per aktivitet qe kryhen ne to.

Duke menaxhuar sistemet e logeve perfitohet shume informacione te rendesishme per sigurine, performance dhe menaxhimin e burimeve te ndrryshme te sistemeve apo sherbimeve te rrjetit. Disa nga keto informacione kategorizohen si me poshte:

- Aksesi. Perdoruesi i cili ka aksesuar nje pajisje apo sistem te rrjetit.

- Ndrryshimi. Parametrat e ndryshuara ne nje pajisje apo sistem te rrjetit.

- Siguria. Veprimtari te ndryshme ne elementet e infrastruktures qe cenojne sigurine e sistemeve apo sherbimeve.

- Sherbimet e ofruara. Kategorizim, ndrryshim apo modifikim i sherbimeve te ofruara.

- Problematikat. Probleme ne funksionimin brenda parametrave te elementeve te infrastruktures se rrjetit.

- Perdorim i Burimeve. Analize e perdorimit te burimeve te ndryshme ne sistemet e rrjetit.

- Aktivitet Standarte. Aktivitetet standarte brenda operacioneve te lejuara nga ana e perdoruesve te ketyre pajisjeve, sistemeve apo sherbimeve.

Administratori i rrjetit eshte pergjegjes per menaxhimin e sistemeve te logeve per elementet e percaktuar te infrastruktures se rrjetit.

Loget e Pajisjeve te Rrjetit

Ne kete kategori bejne pjese ato pajisje qe perbejne infrastrukturen e rrjetit te komanise:

- Router

- Access Point

- Switch

- Firewall

Informacionet qe mund te gjenerohen nga keto sisteme log-esh jane te ndryshme, por perqendrimi eshte fokusuar ne disa prej tyre:

- IP Address te pikave fundore te rrjetit

- Parametrat teknike te rrjetit per aktivitetin e nje pajisje apo klienti

- Sherbimi i kryer

- Ora dhe Data e aktiviteteve

- Vlerat e trafikut te gjeneruar

- Veprimtaria e marre nga pajisja per kerkesat e mesiperme

Loget e Sistemeve dhe Sherbimeve

Ne kete kategori bejne pjese ato pajisje qe operojne per nje sistem te caktuar apo per te ofruar nje sherbim te caktuar. Atom und te karakterizohen si me poshte:

- Sisteme Operacionale

- DNS Server

- Web Hosting Server

- Virtual Server

- Radius Hosting Server

Informacionet qe mund te gjenerohen nga keto sisteme log-esh jane te kategorizuara si me poshte:

- Kerkese per aksesim

- Kerkese per veprim

- Ora dhe Data e aktiviteteve

- Veprimtaria e marre nga perdoruesit e ketyre sistemeve apo sherbimeve

- Parametrat e ndrryshimeve te kryera

Loget e Aplikacioneve

Ne kete kategori bejne pjese ato aplikacione te cilat ofrojne nje sherbim te rendesishem ne infrastrukturen e kompanise.

- Radius Server

- Aplikacioni Financiar

Informacionet qe mund te gjenerohen nga keto sistem log-esh jane te kategorizuara si me poshte:

- Operacionet e kryera ne to

- Ndrryshimet ne kategorite e sherbimeve te ofruara

- Ora dhe Data e aktiviteteve

- Veprimtaria e marre nga perdoruesi

- Informacion mbi aktivitetin e klienteve te regjistruar

Keto informacione mund te perdoren ne menyre te vazhduar nga cdo punonjes I kompanise per te mbarevajtur detyrat e

percaktuara por kjo kerkese duhet te jete e shoqeruar me autorizimin e Administratorit te kompanise per informacionin e kerkuar.

Keto informacione mund te perdoren nga Administratori i Rrjetit per te analizuar veprimtarite e meparshme nga sistemet, pajisjet apo sherbimet per vlerat e trafikut te gjeneruar, vlerat e burimeve te perdorura apo veprimtari te tjera qe kane ndikim ne administrimin e rrjetit.

Keto informacione mund te perdoren per te identifikuar anomali, sulme apo sjellje jo brenda standartit te lejuar te pajisjeve, sistemeve apo personave fizike punonjes ose kliente te kompanise.

Sistemet e Logeve ruajne te dhena deri ne nje muaj nga momenti i regjistrimit te logeve ne sistem.