Republika e Kosovës
Republika Kosova-Republic of Kosovo
Qeveria-Vlada-Government

Ministria e Administratës Publike - Ministarstvo Javne Uprave - Ministry of Public Administration

UDHËZIM ADMINISTRATIV NR. NR. 02/2010 PËR MENAXHIMIN E SIGURISË INFORMATIVE

ADMINISTRATIVE INSTRUCTION NO. 02/2010 FOR INFORMATION SECURITY MANAGEMENT

ADMINISTRATIVNO UPUSTVO BR. 02/2010 ZA MENADŽIRANJE INFORMATIVNE BEZBEDNOSTI

Ministrja e Ministrisë së Administratë Publike, Në mbështetje të nenit 25, paragrafi 7, të Rregullores së Punës së Qeverisë së Kosovës Nr. 01/2007, Nxjerr:	**Minister of Ministry of Public Administration,** Based on article 25, paragraph 7, of the Regulation on the Work of the Government of Kosovo No. 01/2007, Hereby issues:	**Ministar Ministarstva Javne Uprave,** Osnivajući se na član 25, stav 7, Uredbe Rada Vlade Kosova br. 01/2007 god, Donosimo:
UDHËZIMIN ADMINISTRATIV NR.02/2010 PËR MENAXHIMIN E SIGURISË INFORMATIVE	**ADMINISTRATIVE INSTRUCTION NO. 02/2010 FOR INFORMATION SECURITY MANAGEMENT**	**ADMINISTRATIVNO UPUSTVO BR. 02/2010 ZA MENADŽIRANJE INFORMATIVNE BEZBEDNOSTI**
Neni 1 **Qëllimi**	**Article 1** **Purpose**	**Član 1** **Svrha**
Ky Udhëzim Administrativ përcakton mënyrën e menaxhimit të sigurisë së informatave nga personat përgjegjës për zbatimin dhe mirëmbajtjen e sigurisë informative në institucionet e Republikës së Kosovës.	This Administrative Instruction determines the way the information security is managed by responsible people for implementing and maintaining information security in the Republic of Kosovo institutions.	Ovo Administrativno Upustvo odredjuje način menadžiranja informativne bezbednosti od strane odgovornih lica za sprovodjenje održavanja informativne bezbednosti u institucijama Republike Kosova.
Neni 2 **Përkufizimet**	**Article 2** **Definitions**	**Član 2** **Definisanje**

1. Fshehtësia- Të siguruarit që informatat t'u vihen në dispozicion vetëm atyre personave që janë të autorizuar të kenë qasje në to. 2. Integriteti- Ruajtja e tërësisë dhe saktësisë së informatave dhe metodave të përpunimit. 3. Disponueshmëria- Shfrytëzuesit e autorizuar kanë qasje në informata dhe në pajisje. 4. Vlerësimi i rrezikut- Vlerësimi i kërcënimeve, efekteve dhe rrezikueshmërisë së informatave dhe pajisjeve. 5. Menaxhimi i rrezikut- Procesi i identifikimit, kontrollimit dhe minimizimit ose eliminimit të rreziqeve ndaj sigurisë. **Neni 3** **Siguria informative** Siguria e informatave është përgjegjësi e të gjithë nëpunësve në institucionet e Republikës së Kosovës, që menaxhohet nga institucioni përgjegjës për Teknologjinë informative (me tej: institucioni).	1. Confidentiality - Ensure that the information is available only to those persons who are authorized to have access to them. 2. Integrity – Keep the integrity and accuracy of information and processing methods. 3. Availability - Authorized users have access to information and equipment. 4. Risk Assessment - Assessment of threats, effects and riskiness of information and equipment. 5. Risk Management - The process of identifying, controlling and minimizing or eliminating security risks. **Article 3** **Information Security** Information security is the responsibility of all employees in the institutions of the Republic of Kosovo, which is managed by the institution responsible for Information Technology (hereinafter: the institution).	1. Tajna- Bezbednost informacije da im se stavlja na dispoziciju samo licima koja su ovlaščena da imaju pristup. 2. Integritet- Očuvati celu tačnost informacije i metode prerade. 3. Raspolaganje- ovlaščeni korisnici imaju pristup na informacije i opremu. 4. Vredovanje rizika- Vredovanje pretnji, koliko su efekti rizika za informacije i opremu. 5. Menadžiranje rizika- Proces identifikovanja, kontrole i minimiziranja ili elimininiranja rizika ka bezbednosti. **Član 3** **Bezbednost informacija** Bezbednost informacija je odgovornost svakog službenika u institucijama Republike Kosova, koji se menadžuje od odgovorne institucije iz oblasti informativne Tehnologije (dalje: institucija).

Neni 4 **Përgjegjësitë e Institucionit për Sigurinë e Informatave**	**Article 4** **Responsibilities of Information Security Institution**	**Član 4** **Odgovornost Institucije za bezbednost informacija**
1. Institucioni, në përputhje me masat e Qeverisë për siguri në teknologjinë informative, ndërmerr këto aktivitete për avancimin e sigurisë së informatave: 1.1. Miratimin dhe rishqyrtimin politikës së sigurisë së informatave dhe përgjegjësitë e përgjithshme; 1.2. Mbikëqyrjen e ndryshimeve të rëndësishme në ekspozimin e informatave ndaj rreziqeve; 1.3. Rishqyrtimin dhe mbikëqyrjen e incidenteve lidhur me sigurinë e informatave; 1.4. Inicimin dhe miratimin e nismave për përmirësimin e sigurisë së informatave.	1. The institution, in accordance with Government security measures in information technology, undertakes the following activities for the advancement of information security: 1.1. Approval and review of information security policy and overall responsibilities; 1.2. Supervision of important changes in the exposure of information to risks; 1.3. Review and supervision of information security-related incidents; 1.4. Initiation and adoption of initiatives to improve information security.	1. Institucija, shodno Vladenih bezbednosnih mera informativne tehnologije, preduzima sledeće aktivnosti o avansiranju informativne bezbednosti: 1.1. Usvajanje i ponovo razmatranje politike informativne bezbednosti i opšta odgovornost; 1.2. Nadgledanje značajnih izmena, ekspoziranih informacija pri opasnostima; 1.3. Ponovo razmatranje i nadgledanje incidenata u vezi bezbednosti informacija 1.4. Iniciranja i usvajanje ojačanja bezbednosti informacija.
Neni 5 **Procesi i autorizimit për pajisjet e Teknologjisë Informative**	**Article 5** **The process of authorization for Information Technology Devices**	**Član 5** **Proces ovlaščenja za opremu Informativne Tehnologije**
1. Në përcaktimin e procesit të menaxhimit të autorizimit për pajisje të reja të përpunimit të informatave merren parasysh	1. In determining the process of authorization management for new devices for the processing of information the	1. Na odredjivanju procesa menadžiranja ovlaščenja za novu opremu za preradu informacija preduzimaju se sldeća pravila:

këto rregulla: 1.1. Pajisjet e reja të teknologjisë informative (më tej:TI) duhet të kenë aprovimin e menaxhmentit të shfrytëzuesve, me të cilin autorizohet qëllimi dhe shfrytëzimi i tyre; 1.2. Aprovimi sigurohet nga menaxheri përgjegjës për mirëmbajtjen e sigurisë së sistemit informativ për t'u përkujdesur që politikat dhe kushtet relevante të sigurisë të jenë plotësuar; 1.3. Sipas nevojës, hardueri dhe softueri të kontrollohet për t'u përkujdesur që këto të jenë në përputhje me komponentë të tjerë të sistemit; 1.4. Përdorimi i pajisjeve personale dhe kontrollet adekuate për përpunimin e informatave duhet të autorizohen. **Neni 6** **Identifikimi i rreziqeve nga qasja e palëve të treta** 1. Qasja që i jepet palës së tretë është me rëndësi të veçantë dhe duhet të merren parasysh: 1.1. Qasja fizike: në zyrë, në dhoma	following rules shall be taken into account: 1.1. New devices of information technology (hereinafter: IT) must have the approval of the management of users, which authorizes their purpose and use; 1.2. Approval shall be provided by the manager responsible for maintaining the security of information system to ensure that relevant security policies and conditions are met; 1.3. If needed, the hardware and software shall be checked in order to ensure that these are consistent with other system components; 1.4. Use of personal device and adequate controls for the processing of information must be authorized. **Article 6** **Identification of risks from third party access** 1. Access provided to third parties is essential and the following should be taken into account: 1.1. Physical access: to office, computer	1.1. Nova oprema informativne tehnologije (dalje:TI) treba da se usvaja menadžiranje korisnika, kojim se ovlašćuje svrha korišćenja istih; 1.2. Usvajanje se obezbedjuje od odgovornog menadžera za održavanje bezbednosti informativnog sistema da se stara za politike i relevantne uslove koja treba da budu popunjene; 1.3. Prema potrebi , harduer i softueri da se kontrolišu i da budu u slaganju sa ostalim komponentima sistema; 1.4. Korišćenje lične opreme i adekuatne kontrole za preradu informacija potrebno je ovlaščenje. **Član 6** **Identifikovanje rizika sa nastupa trećom strankom** 1. Nastup se daje trećoj stranki i ovo je posebnog značaja i ode treba uzimati u obzir sledeće: 1.1. fizički nastup: u kancelariji, u

kompjuterike, në kabinete me dokumentacion etj.; 1.2. Qasja logjike: baza e të dhënave, sisteme informative etj.	rooms, to documents cabinets etc.; 1.2. Logical access: database, information systems, etc.	kompjuterskim sobama, u kabinetima sa dokumentacijom itd.; 1.2. logični nastup: bazapodataka, informativnog sistema itd.
2. Palëve të treta mund t'iu lejohet qasja në raste të arsyeshme.	2. The access to third parties may be allowed in reasonable cases.	2. Trečim strankama se odobri nastup prema posebnim razlozima.
3. Palët e treta, që qëndrojnë në lokacionin e institucionit për një periudhë kohore, me kontratë, po ashtu mund të shkaktojnë dobësi në siguri. Në palët e treta përfshihen:	3. Third parties, who are located in the institution for a period of time, by contract, may also cause weakness in security. Third parties include:	3. Treče stranke, koje su u lokaciji institucije za jedan vremenski period, pod ugovorom, mogu da stvaraju oslabljenje bezbednosti. U trečim strankama se obuhvataju:
3.1. Stafi për mirëmbajtje dhe mbështetje të harduerit dhe softuerit; 3.2. Pastruesit, furnizuesit, rojat dhe shërbimet e tjera mbështetëse që janë dhënë me nënkontratë; 3.3. Qëndrimi i studentëve dhe emërime të tjera afatshkurtra të rastit; 3.4. Këshilltarët e jashtëm.	3.1. Staff for maintenance and support of hardware and software; 3.2. Cleaners, suppliers, guards and other subcontracting supporting services; 3.3. Students stay and other short-term and random appointments; 3.4 External advisers.	3.1. Staf za održavanje i podršku harduera i softuera; 3.2. Čistaći, snabdevači, čuvari i ostale usluge koja su predvidjena pod ugovorom; 3.3. Stav studenata i druga imenovanja u kratkim rokovimaili prema slučaju; 3.4. Strani savetnici.
4. Qasja në informata dhe pajisje për përpunim të informatave, nga palët e treta, nuk lejohet përderisa të mos jenë vënë në zbatim kontrollimet përkatëse dhe përderisa të mos jetë nënshkruar, kontrata me të cilën definohen kushtet për qasje.	4. Access to information and tools for processing information is not allowed to third parties, until appropriate checks take place and while the contract which defines the conditions for access is signed.	4. Nastup u informacijama i opremi prerade informacija, od trečeg lica, ne dozvoljavase dok nije se izvršila potrebna kontrola dok nije se izvršilo poptpis, ugovor na osnovu čega se definiču uskovi za nastup.

Neni 7 Siguria e nevojshme kontraktuese me palët e treta	Article 7 Required contracting security with third parties	Član 7 Potrebna bezbednost ugovaranja sa trečim strankama
1. Marrëveshja me të cilën lejohet qasja e palës së tretë në pajisjet qeveritare për përpunim të informatave bazohet në kontratë, e cila përmban gjithë sigurinë e nevojshme në përputhje me politikat dhe standardet e sigurisë, duke respektuar kushtet vijuese:	1. The agreement allowing the access to the third party in government facilities for processing information is based on the contract, which contains all the necessary security in accordance with security policies and standards, by respecting the following conditions:	1. Sporazum kojim se odobrava nastup sa trčom strankom u Vladenu opremi za obradjivanju informacija se obazira na ugovor, koja sadrži potrebnu bezbednost shodno politika i standarda bezbednosti, poštovajući sledeće uslove:
1.1. Politika e përgjithshme e sigurisë së informatave; 1.2. Procedurat për të mbrojtur mjetet qeveritare, ku përfshihen: informatat, softueri dhe hardueri; 1.3. Procedurat për të përcaktuar nëse është paraqitur ndonjë rrezikim i mjeteve; 1.4. Kontrolli për të siguruar kthimin apo shkatërrimin e informatave dhe mjeteve në fund të kontratës, apo në ndonjë periudhë të caktuar të saj; 1.5. Integritetin dhe disponueshmërinë; 1.6. Kufizimet në kopjime dhe shpalosje të informatave; 1.7. Përshkrimi i çdo shërbimi që duhet të vihet në dispozicion; 1.8. Përgjegjësitë reciproke të palëve në kontratë;	1.1. General policy of information security; 1.2. Procedures to protect government devices, including: information, software and hardware; 1.3. Procedures to determine whether a risk to devices occurred; 1.4. Control to ensure the return or destruction of information and devices at the end of contract, or in any of its certain periods; 1.5. Integrity and availability; 1.6. Limitations to copying and disclosure of information; 1.7. Description of every available service; 1.8. Mutual responsibilities of parties under the contract;	1.1. Opšta Politika informacione bezbednosti; 1.2. Procedure za zaštitu vladenih srestava,i to : informacije, softuer i hardueri; 1.3. Odredjena procedura ako se pojavila neki rizik na srestava; 1.4. Kontrol nad obezbedjenju koja obavezuje povratak informacija i srestava do kraja ugovora, ili na odredjeno vreme; 1.5. Integritet i raspolaganje; 1.6. Ograničenje na kopiranja i otvaranje informacija; 1.7. Prepis svake usluge koja treba da se stavlja u dispoziciji; 1.8. Uzajamna odgovornost ugovorača;

1.9. Përgjegjësitë lidhur me çështjet juridike, në përputhje me legjislacionin në fuqi; 1.10. Të drejtat e pronës intelektuale, të drejtën e kopjimit dhe mbrojtjes së ndonjë bashkëpunimi; 1.11. Marrëveshjet mbi kontrollimin e qasjes: 1.11.1. Metodat e lejuara të qasjes, kontrollimi dhe përdorimi i identifikuesve unik; 1.11.2. Procesin e autorizimit të qasjes dhe të privilegjeve të shfrytëzuesve. 1.12. Të drejtën për të mbikëqyrur dhe ndaluar aktivitetin e palës së tretë; 1.13. Të drejtën për të reviduar përgjegjësitë kontraktuese ose kryerjen e revizioneve nga pala e tretë; 1.14. Përgjegjësitë për instalimin dhe mirëmbajtjen e harduerit dhe të softuerit; 1.15. Strukturë të qartë raportuese dhe format e raportimit; 1.16. Proces të qartë dhe të definuar për ndryshimin e menaxhimit; 1.17. Rregulla dhe mekanizma mbrojtës fizikë, të nevojshëm për t'u përkujdesur	1.9. Responsibilities related to legal matters, in accordance with legislation in force; 1.10. The rights of intellectual property, the right to copying and protection of any cooperation; 1.11. Agreements on the control of access: 1.11.1. Allowed methods for Access, control and use of unique identifiers; 1.11.2. Process of access authorisation and user's privileges. 1.12. The right to oversee and stop the activity of the third party; 1.13. The right to revise contractual responsibilities or carrying out audits by the third party; 1.14. Responsibility for installation and maintenance of hardware and software; 1.15. Clear reporting structure and reporting forms; 1.16. Clear and defined process for change of management; 1.17. Rules and natural protective mechanisms, necessary to ensure that	1.9. Odgovornost o pranim pitanjima, shodno legislacije na snagu; 1.10. Prava na intelektualnu imovinu, kopiranja i zaštita saradnje; 1.11. Sporazum o kontroli pristupa**:** 1.11.1. odobrene metode nastupa, kontroll i korišćenje zajedničkih identifikovana; 1.11.2. Proces ovlaščenja nastupa i privilegijde korisnika. 1.12. Pravo revidiranja, odgovornost ugovaranja ili obavljanje revizije od strane trečeg lica; 1.13. Prava za revidvanje kontraktivne odgovornosti i zaveršanje od trček straga; 1.14. Odgovornost za instaliranje i održavanje harduerit i softuera; 1.15. Jasna struktura izveštaja i forme izveštaja; 1.16. Jasan proces definisanja za izmenu menadžera; 1.17. Pravila i potrebna fizika zaštita mekanizma, je neophodna da se

që këto kontrolle të zbatohen; 1.18. Trajnimi i shfrytëzuesve dhe administratorëve në metoda, procedura dhe siguri; 1.19. Kujdesi dhe mbrojtja nga softueri i dëmshëm; 1.20. Dispozita për raportimin, njoftimin dhe hetimin e incidenteve të sigurisë dhe uljes së nivelit të sigurisë.	these controls are implemented; 1.18. Training users and administrators on methods, procedures and safety; 1.19. Caution and protection against harmful software; 1.20. Provisions for reporting, notification, and investigation of incidents of security and reduce the level of security.	sprovodi; 1.18. Trajniranje korisnika i administratora, metode, procedure i bezbednost; 1.19. Pažnja i zaštita od štetnog softuera; 1.20. Odredbe za izveštavanje, informisanje o otkrivanju incidenata bezbednosti i smanjenje nivoa bezbednosti.
Neni 8 **Inventarizimi i mjeteve**	**Article 8** **Inventory of devices**	**Član 8** **Inventarizovanje srestava**
1. Çdo institucion identifikon mjetet e veta, vlerën dhe rëndësinë relative të këtyre mjeteve. Bazuar në këto informata, institucioni ofron nivelin e mbrojtjes, që është në përpjesëtim me vlerën dhe rëndësinë e mjeteve.	1. Each institution shall identify its devices, the value and relative importance of these devices. Based on this information, the institution provides the level of protection that is commensurate with the value and importance of devices.	1. Svaka institucija identifikoje svoja srestva, vrednost i relativnu vrednost ovih srestava Osnivajući se na informacije, institucija ponudi nivo zaštite, koja ide prema vrednovanju i značajnost srestava.
2. Inventari i mjeteve të rëndësishme, të ndërlidhura me çdo sistem informativ, përpilohet dhe ruhet. Për çdo pajisje identifikohet qartë përkatësia dhe niveli i sigurimit i dokumentuar, së bashku me lokacionin e tij aktual.	2. Inventory of important devices, related to any information system shall be compiled and stored. For every device, level of security shall be clearly identified and documented, along with its current location.	2. Inventar značajnih srestava, koja se nadvezuju sa informativnim sistemom, sastavljase i očuvase. Svaka oprema identificirase jasno inivo bezbednosti koji dokumentiran zajedno sa aktuelnom lokaciom.
3. Mjetet e ndërlidhura me sistemet e TI-së,	3. Devices related to IT systems are:	3. Medjuvezana srestava sa sistemom IT-a

janë: 3.1. Kapitali i informatave: bazat e të dhënave dhe skedarët e të dhënave, dokumentacioni sistemor, doracakët për shfrytëzuesit, materiali trajnues, procedurat operacionale ose mbështetëse, planet e vazhdimësisë, aranzhmanet rezervë, informatat e arkivuara; 3.2. Mjete softuerike: sistemet operative dhe programet e ndryshme programuese; 3.3. Pajisjet-kapitali fizik: pajisjet kompjuterike, pajisjet për komunikim (rrjetit), mbrojtësit e sistemit (firewall-et), dhe pajisjet e tjera teknike; 3.4. Shërbimet: shërbimet kompjuterike dhe të komunikimit si dhe shërbimet e përgjithshme, si ngrohja, ndriçimi, rryma, klimatizimi etj. **Neni 9** **Raportimi i incidenteve të sigurisë** Nëpunësi dhe kontraktuesi obligohet që incidentin e sigurisë ta paraqes në afatin më të shkurtë të mundshëm te organi përgjegjës.	3.1. Information capital: data bases and filing cabinets, system documentation, manuals for users, training material, operational or support procedures, continuity plans, backup arrangements, archived information; 3.2. Software devices: operating systems and various programming programs; 3.3. Physical capital-devices: computer devices, communications devices (network), the protective system (firewalls), other technical devices; 3.4. Services: computer and communication services, general services, such as heating, lighting, power, air conditioning, etc. **Article 9** **Reporting security incidents** Employee and contractor are obliged to inform the responsible body on the security incident as soon as possible.	su: 3.1. Kapital informacija: baza podataka i skedari podataka, sistematika dokumentacija, priručnici za korisnike, literatura za trajniranje, operacione procedure ili naslaganja, planovi u kontinuitetu, rezervni aranžmani, arkivirana informacija; 3.2. Softuerski sistem : sistemi operative vrsne programe, programirane; 3.3. Oprema - fizički kapital, kompjuterska oprema, oprema za komuniciranje (mreža) zaštitnici sistema (firewall-et), i ostale tehničke opreme; 3.4. usluge: kompjuterske usluge i komuniciranja, opšte usluge, kao grejanje, svetlost, struja, klimatizacija itd. **Član 9** **Izveštavanje o bezbednosnom incidentu** Zvaničnik ugovarača obavezujese za incident bezbednosti da prijavi u što kracem roku kod odgovornog organa.

Neni 10 **Raportimi i dobësive në siguri** Shfrytëzuesi i shërbimeve të TI-së është i obliguar të vëzhgojë dhe raportojë te organi përgjegjës çdo dobësi të parë apo të dyshuar në siguri, ose rreziqe që iu kërcënohen sistemeve apo shërbimeve, dhe në asnjë rrethanë, të mos provojë ta evitojë dobësinë e dyshuar.	**Article 10** **Reporting security weakness** The user of IT services is obliged to observe and report any weakness seen or suspected about the security, or risks that are threatening systems or services. He must report to the management or the responsible body. The user, under no circumstances, shall not try to avoid the alleged weakness, for security reasons**.**	**Član 10** **Izveštavanje o slabostima u obezbedjenje** Korišćenje usluga IT-a je obavezno saslušanje i izveštavati o svakoj primećenoj slabosti ili sumnje na bezbednost, ili opasnostima koja preti sistemima ili uslugama. On treba izveštavati kod menadžmenta ili odgovornog organa. Korisnik u nijednom okolnošću ne smije da evitira slabosti na koja sumnja.
Neni 11 **Raportimi i defekteve në softuer** 1. Raportimi i defekteve në softuer bëhet sipas procedurave vijuese: 1.1. Duhet t'iu kushtohet vëmendje indikacioneve të problemit dhe porosive që paraqiten në ekran; 1.2. Kompjuteri me softuer të dëmtuar duhet të izolohet, sipas mundësisë, shfrytëzimi i tij të ndalohet derisa të evitohet defekti; 1.3. Nëse nevojitet kontrollimi i pajisjes, atëherë ajo shkyçet nga rrjeti dhe disqet	**Article 11** **Reporting software defects** 1. Reporting software defects shall be made by the following procedures: 1.1. Indications to the problem and messages that appear on the screen should be taken into account; 1.2. The computer with damaged software must be isolated, if possible, its use shall be prohibited until the defect is avoided; 1.3. If checking of devices is required, they will be automatically switched off	**Član 11** **Izveštavanje o defeku softuera** 1. Izveštaj o defektima u softueru izvrši se prema sledečim procedurama: 1.1. Treba voditi računa indikacijama problema i poruka koja se pojavljuju na ekranu; 1.2. kompjuter sa oštecenim softuerom treba izolovati, prema mogučnosti, njegovo korisčenje se zabranjuje sve dok se evitiraju defekti; 1.3. Ako je potreba za kontrolu opreme onda ona se isključi sa mreže, disk

kopjuese nuk duhet të transferohen te kompjuterët e tjerë; 1.4. Shfrytëzuesi nuk mund ta largojë softuerin për të cilin dyshojnë, përveç nëse është i autorizuar të veprojë ashtu. 1.5. Çështja menjëherë i raportohet organit përgjegjës. 2. Në raste të tilla rimëkëmbjen e bën personi kompetent.	by the network and copy discs should not be transferred to other computers; 1.4. The user can not remove software for which they suspect, unless is authorized to do so. 1.5. The matter shall be immediately reported to the responsible body. 2. In such cases, the recovery shall be made by a competent person.	kopiranja ne sme da se transferiše u drugim kompjuterima; 1.4. Korisnik ne može da otkloni softuer na koga sumlja, osim ako je ovlaščen da radi isto. 1.5. Ovaj problem odmah se izveštava odgovornom organu. 2. U hovim slučajevima obnovljanje izvrši kompetentno lice.
Neni 12 **Mbrojtja fizike e mjediseve të punës**	**Article 12** **Physical protection of working environment**	**Član 12** **Fizička zaštita radne sredine**
1. Institucionet përdorin parametrat e sigurisë për të mbrojtur hapësirat, që kanë stabilimente për përpunim të informatave. Vend-ndodhja dhe forca e çdo barriere varen nga rezultati i vlerësimit të rrezikut. 2. Rregullat dhe udhëzimet vijuese merren parasysh dhe zbatohen sipas nevojës: 2.1. Hapësira e sigurt, definohet qartë; 2.2. Ndërtesa apo vendi që përmban stabilimente për përpunim të informatave të jetë e mbrojtur mirë fizikisht;	1. Institutions shall use the security parameters to protect areas that have devices for processing information. Location and strength of each barrier depends on the outcome of risk assessment. 2. The following rules and guidelines be considered and implemented as appropriate: 2.1. Safe environment shall be clearly defined; 2.2. Building or place containing devices for information processing shall be well protected physically;	1. Institucije koriste parametri bezbednosti da zaštiti sredine gde se izvrši prerada sa stabilimentima informacija. Mesto dogadjaja-i jačina svake bariere zavisne su od rezultata ocenjenog rizika. 2. Pravila i i upustva se koriste prema potrebe: 2.1. sigurna sredina, definišese jasno; 2.2. Zgrada ili mesto koje sadrži srestva za preradu informacija treba da bude fizički bezbedno;

2.3. Të vihen në zbatim recepcioni dhe kontrollet fizike të qasjes; 2.4. Barrierat fizike, nëse është e nevojshme, të zgjerohen prej dyshemesë deri te plafoni për të parandaluar hyrjet e paautorizuara dhe rrezikimin ambiental.	2.3. The Reception and physical access controls to be applied; 2.4. Physical barriers, if necessary, to be extended from floor to the ceiling in order to prevent unauthorized entry and environmental risk.	2.3. Sprovesti recepciju i fiziku kontrolu nastupa; 2.4. Fizička bariera, ako je potrebno da se proširi od patosa do plafona da bih sprečili neovlaščene ulaze i ambientalno rizikovanja.
Neni 13 **Kontrollimet fizike të hyrjes në ambiente**	**Article 13** **Physical checks of entry into premises**	**Član 13** **Fizička kontrola ulaza u ambijentu**
1. Hapësirat e sigurta janë të mbrojtura me anë të kontrolleve përkatëse në hyrje për t'u përkujdesur që vetëm personelit të autorizuar t'i mundësohet qasja.	1. Safe spaces are protected by relevant entry access controls in order to ensure that the access is allowed only to the authorized personnel.	1. Sigurne površine su bezbedjene putem dotične kontrole na ulazu da se stara da samo ovlaščenom licu se odobrava pristup.
2. Kriteret që duhet të merren parasysh janë:	2. Criteria to be considered are:	2. Kriteri koji treba da se uzimaju u obzir su:
2.1. Personeli i autorizuar në hapësirat e sigurta duhet mbikëqyrur dhe regjistruar: data, koha, vendi i hyrjes dhe largimit. Atij i lejohet qasja vetëm për qëllime specifike të autorizuara dhe duhet t'i jepen udhëzime mbi sigurinë e nevojshme të hapësirës në rast të emergjencës; 2.2. Qasja në informata të ndjeshme dhe pajisjet për përpunim të informatave, janë	2.1. Authorized personnel in secure areas should be supervised and recorded: date, time, place of entry and departure, they are going to be allowed to have access only for authorized specific purposes and they should be provided with instructions on necessary security of space in case of emergency; 2.2. Access to sensitive information and devices for information processing, are	2.1. Ovlaščeno lice u sigurnim prostorima,treba nadgledati i registrovati : datum, vreme, mesto ulaza i izlaza, Njemu se dozvoljava nastup samo za specifične svrhe ovlaščenjem , njemu treba da se daju u pustva o potrebnoj bezbednošću u slučaju emergencije; 2.2. Nastup na osetljive informacije i opremu za preradu informacija, su pod

nën kontroll dhe të lejuara vetëm për personat e autorizuar. 2.3. Kontrollet e autenticitetit, si: kartela identifikuese plus PIN-i, duhet të përdoren për të autorizuar dhe për të bërë të vlefshme qasjen. Gjurmët e të gjitha qasjeve ruhen; 2.4. Çdonjëri duhet të mbajë ndonjë formë të identifikimit të dukshëm; 2.5. E drejtat e qasjes në hapësirat e sigurta rregullisht rishqyrtohet dhe përditësohet.	under control and are allowed only for authorized persons; 2.3. Authenticity controls such as identification card plus PIN must be used to authorize and to make access available. All access trails shall be saved; 2.4. Everyone must have a visible form of identification; 2.5. The right to access secure areas shall be regularly reviewed and updated.	kontrolom dozvoljene samo za ovlašćena lica; 2.3. Kontrola autenticiteta, kao: kartice identifikovanja plus PIN-i, treba koristit za ovlašćene kako bih postalo značajan nastup. Tragovi svakog nastupa se čuvaju; 2.4. Svako lice treba da zadrži na vidno mesto znak identifikovanja; 2.5. Pravo nastupa u sigurnim prostorima vazda treba da ponovo razmatra i objelodani.
Neni 14 **Sigurimi i zyrave, dhomave dhe pajisjeve**	**Article 14** **Office, rooms and tools security**	**Član 14** **Obezbedjenje kancelarija, prostora i opreme**
1. Gjatë dizajnimit të hapësirës së sigurt duhet të merren parasysh mundësitë e dëmit nga zjarri, eksplozioni, trazirat civile, fatkeqësitë natyrore dhe format e tjera të fatkeqësive.	1. During the design of secure space the possibilities of damage by fire, explosion, civil disorder, natural disasters and other forms of disasters should be taken into account**.**	1. Tokom dizajniranja sigurne površine i da se predvidja mogučnost štete od požara, eksplozije, civilneo uznemirenje, prirodne nepogode i druge forme nepogoda.
2. Pajisjet kyçe vendosen në atë mënyrë, e cila mundëson shmangien e qasjes nga personat e paautorizuar.	2. Key equipment shall be placed in a manner which avoids access by unauthorized persons.	2. Ključnu opremu treba postavljati na taj način da nemože pristupiti neovlaščeno.
3. Ndërtesa duhet të jetë e dizajnuar që të mos bien në sy dhe pa shenja të dukshme,	3. The building must be designed not to be noticeable and without visible signs outside	3. Zgrada treba da bude dizajnirano i da ne bude na centar pažnje da ne pada na

jashtë dhe përbrenda ndërtesës, me të cilën tregohet prania e veprimtarive për përpunim të informatave.	and inside the building, which is indicated by the presence of information processing activities.	oko i bez istaknutih znakova, vani i unutra Zgrade, kojim se dokaže. prisutnost obavljanja prerade informacija.
4. Sistem i përshtatshëm për zbulim të ndërhyrjeve pa leje, të instaluar sipas standardeve profesionale dhe të testuar rregullisht, të jetë i vendosura për të mbyllur të gjitha dyert dhe dritaret e jashtme. Hapësirat që përkohësisht janë pa personel të jenë nën alarm gjatë tërë kohës.	4. Suitable system for detection of interventions without permission, installed by professional standards and regularly tested, shall be located close to all external doors and windows. Spaces, which temporarily have no personnel, must be under the alert at all times.	4. Udoban Sistem za otkrivanje ulaska bez dozvole, koji je instaliran prema stručnim standardima i to testirani redovno, postavljeni u spoljnim prozorima i vratima. Prostorija koja su privremeno bez personela treba obavezno da budu pod alarmom.
5. Pajisjet për përpunim të informatave që menaxhohen nga institucionet të jenë fizikisht të ndara nga ato që menaxhohen nga palët e treta.	5. Information processing devices that are managed by institutions to be physically separated from those managed by third parties.	5. prema za preradu informacija koja se menadžiraju od institucija treba da budu fizički opredelene od onih koja se menadžiraju od treće stranke.
6. Për publikun nuk lejohet qasje në emërtues intern telefonik me të cilët identifikohen lokacionet e pajisjeve që përpunojnë informata të ndjeshme.	6. Access to internal telephone denominator, which identifies the equipment locations that process sensitive information, is not allowed to the public.	6. Za javnost se ne dozvoljava nastup imenovanjem internim telefonom kojim se identifikoju lokacije opreme za preradu osetljivih informacija.
7. Materialet e rrezikshme të ruhen në hapësirë të sigurt.	7. Hazardous materials shall be stored in a safe place.	7. Rizične materiale se očuvaju na sigurnim prostorima.
8. Furnizimet me shumicë, nuk ruhen përbrenda hapësirës së sigurt deri në kohën kur janë të nevojshme për përdorim.	8. Wholesale supplies shall not be stored inside the safe area, until the time when are necessary for use.	8. Snabdevanje na veliko ,se ne čuvaju unutar sigurne prostorije do na ono vreme kada su potrebne za korišćenje.
9. Pajisjet dhe mediumet rezervë vendosen	9. Spare devices and media shall be placed	9. Oprema i rezervni mediumi

në një distancë të sigurt për t'iu shmangur dëmit nga fatkeqësia në vendin kryesor.	in a safe distance in order to avoid damage from disasters at the main place.	postavljajuse u sigurnoj distanci da bih izbegavali štete koja može da se desi na glavnom mestu.
10. Pajisjet fotografike, video, audio apo pajisjet e tjera për regjistrim nuk janë të lejuara, përveç me autorizim.	10. Photographic devices, video, audio or other recording devices are not permitted, except if authorised.	10. Oprema za fotografije, video, audio ili druga oprema za registraciju nisu dozvoljene osim sa ovlaščenjem.
Neni 15 **Siguria e pajisjeve**	**Article 15** **Devices Security**	**Član 15** **Bezbednost opreme**
1. Pajisjet duhet të vendosen dhe të ruhen për të zvogëluar rrezikun nga kërcënimet ambientore dhe mundësitë për qasje të paautorizuar, duke pasur parasysh që:	1. Devices should be placed and maintained in order to reduce the risk of environmental threats and possibilities for unauthorized access, given that:	1. Opreme treba da se postavljaju i da se očuvaju da bih izbegavali rezik, t ambientalne smetnje i mogučnosti upadanja bez ovlaščenje, imajući u obzir sledeće:
1.1. Pajisjet të jenë të vendosura në mënyrën e cila minimizon qasjen e panevojshme në hapësira punuese;	1.1. Devices are located in a manner that minimizes unnecessary access to working space;	1.1. Opreme treba da se postavljaju na taj način da bih minimizirali nepotrebni nastup u radnim prostorijama;
1.2. Pajisjet për përpunim dhe ruajtje të informatave me të dhënat e ndjeshme të jenë të vendosura ashtu që të zvogëlohet rreziku i shikimit nga të tjerët gjatë përdorimit të tyre;	1.2. Devices for processing and storage of information with sensitive data are located so as to reduce the risk to be seen by others during their use;	1.2. Opreme za preradu i očuvanju informacija osetljivim podacima postavljaju da bih minimizirali rizik da ne bih mogli drugi da vide tokom njihove upotrebe;
1.3. Pajisjet të cilat kërkojnë mbrojtje të veçantë të jenë të izoluara;	1.3. Equipment requiring special protection should be isolated;	1.3. Oprema koja zahteva posebnu zaštitu treba da budu izolovana;
1.4. Të përvetësohen mënyrat e	1.4. To appropriate ways to minimize the	1.4. Savladati način kontrole da bih

kontrollimit për të minimizuar rrezikun nga: vjedhja, zjarri, eksplozioni, tymi, uji (ose ndërprerja e furnizimit të ujit), pluhuri, vibracionet, efektet kimike, pengesat nga furnizimi me rrymë, radioaktiviteti elektromagnetik etj.; 1.5. Të ndalohet ngrënia, pija dhe pirja e duhanit në afërsi të pajisjeve për përpunim të informatave; 1.6. Efektet e ndonjë fatkeqësie, që ndodhin në lokalet e afërta, të merren parasysh.	risk control by theft, fire, explosion, smoke, water (or water supply interruption), dust, vibrations, chemical effects, barriers of power supply, electromagnetic radioactivity etc.; 1.5. Eating, drinking and smoking in the vicinity of equipment and information processing is prohibited; 1.6. The effects of any disaster, occurring close to the premises must be taken into account.	minimizirali rizik: kradja, požar, eksplozija, dim, voda (ili isključenje snabdevanje vode), prašina, vibracije, hemički efeki, prepreke u snabdevanju sa strujom, elektromagnetski radioaktivnosti itd.; 1.5. Zabranjujese hrana , piće, i pušenje u blizini opreme za preradu informacija; 1.6. Efekti nezgode, koje se dešavaju u bližnim lokalima, treba imati na umu.
Neni 16 **Furnizimi me energji elektrike**	**Article 16** **Electricity supply**	**Član 16** **Snabdevanje električnom energijom**
Pajisjet të jenë të mbrojtura nga ndërprerjet e furnizimit me rrymë dhe anomalitë e tjera elektrike, duke siguruar pajisje adekuate me rrymë e cila është në përputhje me specifikimet e prodhuesit të pajisjes.	Devices must be protected from power supply interruptions and other power anomalies, providing adequate power device which is in accordance with the specifications of the manufacturer of the device.	Oprema treba da bude zaštićena od isključenja struje i ostalih električnih nereda, za to se obezbedjuje adekuatna struja shodno specifikacija proizvodjača opreme.
Neni 17 **Siguria e kabllove**	**Article 17** **Cable security**	**Član 17** **Bezbednost kablova**
1. Kabllot e rrymës dhe telekomunikimit për	1. Electricity and telecommunication cables	1. Električni kabal telekomuniciranja u

pajisjet për përpunim të informatave, të jenë nën tokë apo nën ndonjë mbrojtje tjetër.	of information processing devices, to be placed under ground or under any other protection.	opremi za preradu informacija, da budu podzemni ili pod nekom drugom zaštitom
2. Kabllot e rrjetave të jenë të mbrojtura nga dëmtimet dhe ndërhyrjet e paautorizuara, duke përdorur gypa apo duke iu shmangur kalimit nëpër hapësira publike.	2. Network cables be protected from damage and unauthorized intervention, using pipes or avoiding passage through public space.	2. Kablovi mreži treba da budu zaštićeni od kvara i od neovlaščenih upletnji, koristeći cevi ili izbegavanju prolaza na javnim.
3. Kabllot e rrymës dhe kabllot e telekomunikimit, të jenë të ndara.	3. Power cables and telecommunication cables, be separated.	3. Električni kabal i kabal telekomuniciranja,da budu zabranjeni.
4. Për sistemet e ndjeshme dhe me rëndësi të veçantë, të merren parasysh kushtet vijuese: 4.1. Instalimi i gypave të hekurt; 4.2. Përdorimi i medieve alternative për rutim ose transmetim; 4.3. Përdorimi i kabllove me fije optike; 4.4. Kontrollimi i përhershëm i kabllove për të evituar ndërhyrjet nga jashtë.	4. For sensitive systems with specific importance the following conditions must be taken into account: 4.1. Installation of iron pipes; 4.2. Use of Alternative Media for routing or broadcast; 4.3. Using fibre optic cables; 4.4. Permanent control of cables in order to avoid interference from outside.	4. Osetljiv sistem i sa posebnog značaja, treba imati u obzir sledeći uslovi: 4.1. Instaliranja metalnih cevi; 4.2. Upotreba alternativnih medija za transmetiranje; 4.3. Upotreba kablova optičkim nitima; 4.4. Stalna Kontrola kablova da bih evitirali upletanja sa vani
Neni 18 **Mirëmbajtja e pajisjeve**	**Article 18** **Maintenance of devices**	**Član 18** **Održavanje opreme**
1. Bëhet në mënyrë adekuate, për të mundësuar vazhdimësinë e punës, duke respektuar kushtet vijuese:	1. Maintenance of devices must be adequately done in order to enable the continuation of work, by respecting the following conditions:	1. obavljase adekuatan način, da bih omogučili kontinuitet rada, poštovajući sledeće uslove:

1.1. Që mirëmbajtja të bëhet në përputhje me udhëzimet dhe specifikimet e rekomanduara nga furnizuesi; 1.2. Vetëm personeli i autorizuar për mirëmbajtje, i kryen riparimet e pajisjeve; 1.3. Për defektet e dyshuara apo të shkaktuara dhe për mirëmbajtjen preventive apo korrigjuese, të mbahen shënime; 1.4. Pajisjet që dërgohen jashtë lokaleve për mirëmbajtje të kontrollohen në mënyrë adekuate; 1.5. Të respektohen të gjitha kushtet që parashtrohen nga polisat e sigurimit.	1.1. Maintenance must be consistent with instructions and specifications recommended by the supplier; 1.2. Only authorized personnel for maintenance shall perform repairs of equipment; 1.3. For alleged or caused defects and for preventive or corrective maintenance, records must be kept; 1.4. Equipment sent outside premises for maintenance must be adequately controlled; 1.5. Respect all conditions set forth by insurance policies.	1.1. Održavanje da bude s hodno upustava i specifikacija koje preporučuje snabdevač; 1.2. Samo ovlaščeni personel održavanja, obavlja popravku opreme; 1.3. Ako se sumnja na učinjene defekte i preventivu održavanja , korigovanja, treba da se drže beleške; 1.4. Oprema koja se postavlja van prostorija održavanja da se kontrolišu adekuatno; 1.5. Da se poštuju uslovi koji predvidja polisa bezbednosti.
Neni 19 **Siguria e pajisjeve jashtë objekteve institucionale**	**Article 19** **Security of devices outside institutional premises**	**Član 19** **Bezbednost opreme van objektima institucija**
1. Përdorimi i pajisjeve jashtë objekteve institucionale, të autorizohet nga personi zyrtar. 2. Pajisjet dhe mediumet që nxirren jashtë lokaleve nuk lihen pa përkujdesje në vendet publike. 3. Të respektohen udhëzimet e prodhuesit	1. Use of devices outside institutional facilities for processing the information is authorized by the official person. 2. Devices and media that are sent outside shall not be left without attention in public places. 3. Respect manufacturer’s guidelines for	1. Korišćenje opreme van objekata institucija, ovlaščujese od službenog lica. 2. Oprema i mediumi koja se izvade van službenih prostorija trebada se postaraju na službenim mestima. 3. Treba da se poštuju upustva

për mbrojtjen e pajisjes. 4. Mbrojtja e pajisjes jashtë lokaleve bëhet në mënyr adekuate dhe të organizuar, sipas standardeve të sigurisë.	protection of equipments. 4. Protection of devices outside the premises shall be made in adequate and organized manner, according to security standards.	proizvodjača za zaštitu opreme. 4. Zaštita opreme van prostorija izvši se na adekuatan način i organizovano prema standardima bezbednosti.
Neni 20 **Asgjësimi i sigurt dhe ripërdorimi i pajisjes** 1. Aparaturat për ruajtjen e të dhënave që përmbajnë informata të ndjeshme duhet fizikisht të shkatërrohen ose të mbishkruhen në mënyrë të sigurt, e jo të përdoret funksioni standard i fshirjes. 2. Për aparaturat e dëmtuara të ruajtjes së të dhënave, me të dhënat të ndjeshme nevojitet vlerësim i rrezikut, për të përcaktuar nëse artikujt duhet të prishen, të riparohen ose të hidhen.	**Article 20** **Safe destruction and re-use of equipment** 1. Equipment for storing data containing sensitive information must be physically destroyed or securely inscribed, and not using the standard delete function. 2. For damaged equipment for data storage with sensitive data, the risk assessment is required in order to determine whether items should be destroyed, repaired or disposed of.	**Član 20** **Sigurno poništenje ponovokorišćtene opreme** 1. Aparatura za očuvanje podataka sadrže osetljivu informaciju, koja treba fizikčki da se poništi ili da se nadpisuju na siguran i ne na taj način je bolje nego da se upotrebljava standardja funkcija brisanja. 2. O oštečenoj aparaturi prilikom očuvanja podataka, tom prilikom potrebno je vrednovanje rizika, i da se odredjuje dali treba da se artikli poništavaju, obonove ili izbace.
Neni 21 **Politika e tavolinës së pastër dhe ekrani të pastër**	**Article 21** **The policy of clear table and clear display**	**Član 21** **Politika čistog stola i čistog ekrana**

1. Në institucione qeveritare të përvetësohet politika e tavolinës dhe ekranit të pastër për letrat dhe pajisjet për përpunim të informatave, duke iu përmbajtur rregullave vijuese: 1.1. Në rast nevoje, letrat dhe mediet kompjuterike të ruhen në kabinete të mbyllura; 1.2. Informatat e ndjeshme mbyllen në kabinet apo arkë rezistuese ndaj zjarrit; 1.3. Kompjuterët personalë, terminalet e kompjuterëve, printerët nuk bën të lihen të hapur kur janë pa përkujdesje; 1.4. Vendi ku hyn dhe del posta, faksaparatet dhe fotokopjet pa përkujdesje, duhet të jenë të mbrojtura; 1.5. Informatat e ndjeshme dhe të klasifikuara, kur janë në formë të shtypur, të largohen menjëherë nga shtypësi; 1.6. Informatat e panevojshme në formë të shtypur duhet të grisen. **Neni 22** **Largimi i pajisjeve apo softuerit** 1. Pajisjet, informatat apo softueri, nuk mund të largohen nga vendi i punës pa	1. In government institutions appropriate table policy and clear display for papers and equipment for information processing, by following these rules: 1.1. If necessary, papers and computer media to be stored in closed cabinets; 1.2. Sensitive information must be closed in the cabinet or fire resistant box; 1.3. Personal computers, computer terminals, printers should not be left open when are not under caution; 1.4. The place of entry and exit of mail, fax and photocopy machines without caution must be protected; 1.5. Sensitive and classified information in printed form must immediately withdraw from the printer; 1.6. Unnecessary information in printed form must be destroyed. **Article 22** **Removal of software devices** 1. Devices, information or software, can not be removed from the working place without	1. U vladenim institucijama da se suvaja politika stola i čistog ekrana za papire i opremu o preradu informacija, treba da se podržavamo sledećim pravilima: 1.1. Prema potrebi, papiri i kompjuterska media da se očuvaju u zatvorenim kabinetima; 1.2. Osetljiva Informacija očuvaju u zatvorenim kabinetima ili u posebnim kutijam koja su rezistentna nad požarom 1.3.Lični Kompjuteri, terminali kompjutera, printeri ne dozvoljavase da se ostavljaju otvoreni kada su nepripazeni; 1.4. Mesto gde ultazi i izlazi pošta, faksaparati, fotokopirači bez posebne pažnje treba da budu zaštičeni; 1.5. Osetljiva informacija i klasifikovana, kada se nalaze u otkucanoj formi, da se izvlače odmah od prekucavanja; 1.6.Nepotrebna Informacija na otkucanoj formi treba da se pocepaju. **Član 22** **Udaljenje opreme ili softuerit** 1. Prema tome informacije ni softuera, ne mogu da se uklanjaju sa radnog

autorizim. Sipas nevojës dhe rastit, pajisjet të çregjistrohen në dalje dhe të regjistrohen në hyrje. 2. Të organizohen kontrolle të paparalajmëruara për të evituar largimin e paautorizuar të pronës. **Neni 23** **Menaxhimi i ndryshimeve operacionale** 1. Të kontrollohen ndryshimet në stabilimente për përpunim të informatave dhe në sisteme. 2. Programet operative t'i nënshtrohen kontrollit rigoroz të ndryshimeve. 3. Kur ndërrohen programet, përgatitet një raport revizioni, i cili përmban të gjitha informatat relevante, duke marrë parasysh: 3.1. Identifikimi dhe regjistrimi i ndryshimeve domethënëse; 3.2. Vlerësimi i ndikimit të mundshëm të ndryshimeve të tilla; 3.3. Procedura formale e miratimit të ndryshimeve të propozuara;	authorization. As necessary and appropriate, devices should be deregistered when outgoing and registered when incoming. 2. Unexpected checks must be organized in order to prevent unauthorized removal of property. **Article 23** **Change operation management** 1. Changes in information processing equipment and systems shall be checked. 2. Operational programs are subject to rigorous change control. 3. When programs are changed, an audit report containing all relevant information shall be prepared, taking into account the following: 3.1. Identification and registration of significant changes; 3.2. Assessment of possible impact of such changes; 3.3. Formal procedure of proposed changes approval;	mesta bez ovlaščenje. Prema potrebi i slušaju, opreme treba otpisati prilikom izlaza i da se registruju na ulazu. 2. Treba organizovati nenajavljene kontrole kako bih evitirali neovlašćeno vlasništvo. **Član 23** **Menadžiranje operacionih izmena** 1. Treba kontrolisati izmene u stabilimentima za preradu informacija i u sistemu. 2. Operativni Programi da se podlažu rigoroznoj kontroli izmena. 3. Kada se programi izmene, da se priremi izveštaj za reviziju, koji sadrži svaku relevantnu informaciju, kao sledeće: 3.1. Identifikovanje i registracija značajnih izmena; 3.2. Vrednovanje mogućeg uticaja istih izmena; 3.3. Formalna procedura usvajanja predloženih izmena;

3.4. Komunikimi i detajeve të ndryshuara të gjithë personave relevant; 3.5. Procedurat me të cilat identifikohen përgjegjësit për ndërprerjen dhe rimëkëmbjen nga ndryshimet jo të suksesshme.	3.4. Communicating the changed details of all relevant persons; 3.5. Procedures which identify those responsible for the termination and recovery from unsuccessful changes.	3.4. Komuniciranje o vrsnim detaljima svakog relevantnog lica; 3.5. Procedure kojim se identifikoju odgovornosti za prekid i obnovu od neuspešnih izmena.
Neni 24 **Procedura e menaxhimit të incidenteve**	**Article 24** **Incident procedure management**	**Član 24** **Procedura menadžiranja incidenata**
1. Për të arritur një reagim të shpejtë, efektiv dhe të rregullt ndaj incidenteve të sigurisë të TI-së, duhet të caktohen përgjegjësit dhe procedurat për menaxhim të incidenteve si:	1. To achieve a rapid, effective and regular response towards security incidents to IT, procedures and responsible people for dealing with security incidents shall be determined, such as:	1. Da bih postigli brzu reakciju, efektivnu, urednu pri incidentima bezbednosti IT-a, treba da se odredjuju odgovornosti i procedure za menadžiranje incidenata i to:
1.1. Procedurat për mbulimin e të gjitha llojeve të incidenteve të sigurisë, përfshirë:	1.1. Procedures for covering all types of security incidents, including:	1.1. Procedure za pokriće svakog vrsta pokrića bezbednosnih incidenata koja obuhvata:
1.1.1. Rëniet e sistemit informativ dhe humbjen e shërbimit; 1.1.2. Refuzimin e shërbimit; 1.1.3. Gabimet që rrjedhin nga të dhënat e pakompletuara ose të pasakta;	1.1.1. Crash of information system and loss of service; 1.1.2. Denial of service; 1.1.3. Errors resulting from incomplete or incorrect information;	1.1.1. Pad informativnog sistema i izgubljenje usluga; 1.1.2. Odbijanje usluga; 1.1.3. Greške koje mogu da se učine od nekompletiranih podataka ili netačnih;
1.1.4. Shkeljet e fshehtësisë; 1.1.5. Analizën dhe identifikimin e	1.1.4. Breach of confidentiality; 1.1.5. Analysis and identification of the	1.1.4. Otkrivanje tajne; 1.1.5. Analiza i identifikovanje razloga

shkakut të incidentit; 1.1.6. Planifikimin dhe zbatimin e masave për të parandaluar përsëritjen; 1.1.7. Mbledhjen e gjurmëve nga revizioni dhe dëshmitë e ngjashme; 1.1.8. Komunikimi me personat që janë prekur nga incidenti ose që kanë qenë të përfshirë në rimëkëmbjen nga incidenti.	cause of the incident; 1.1.6. Planning and implementation of measures to prevent iteration; 1.1.7. Collection of audit trails and similar evidence and 1.1.8. Communication with people who are affected by the incident or who have been involved in the recovery from the incident.	incidenta; 1.1.6. Planiranje i preduzimanje mera da bih sprečili ponavljanje istog; 1.1.7. Prikupljenje tragova od revizije i slični dorazi i 1.1.8. Komuniciranje sa licima koja su dotaknuta incidentom ili da su bili obuhvaćeni na saniranju incidenta.
1.2. Masat që merren për t'u rimëkëmbur sistemi nga rëniet dhe për të korrigjuar dështimet në sistem janë: 1.2.1. Vetëm personeli i autorizuar të ketë qasje në sisteme dhe të dhëna; 1.2.2. Të gjitha masat emergjente të jenë të dokumentuara në detaje; 1.2.3. Masat emergjente i raportohen menaxhmentit dhe rishqyrtohen në mënyrë të rregullt.	1.2. Measures taken to recover the system from falling and to correct failures in the system are: 1.2.1. Only authorized personnel shall have access to systems and data; 1.2.2. All emergency measures to be documented in detail; 1.2.3. Emergency measures to be reported to the management and regularly reviewed.	1.2. Mere koje se prduzimaju na saniranju pada sistema i koja će korigovati neuspešnog sistema su: 1.2.1. samo ovlaščeni personel može nastupiti u sisteme i podacima; 1.2.2. Svaka hitna mera da se detalno dokumentira; 1.2.3. Svaka hitna mera da se izveštava menadžmentima i da se ponovorazmatraju redovno.
Neni 25 **Planifikimi i kapaciteteve**	**Article 25** **Capacity planning**	**Član 25** **Planiranje kapaciteta**
Planifikimi i zgjerimit të kapaciteteve teknologjike, për përpunim, ruajtje dhe siguri të informatave, bëhet me kujdes të veçantë për t'iu shmangur pengesave që	Planning of expansion of technology capacities for processing, storage and security of information is made with special attention in order to avoid obstacles that	Planiranje proširenj tehnološkog kapaciteta, za preradu, očuvanje i bezbednost informacija, izvrši posebnom pažnjom i izbegavanje prepreka koje

mund të paraqesin rrezikim dhe ngadalësim të sistemit, uljen e sigurisë etj.	may pose risk and system slowdown, lowering security etc.	prestavljaju rezik i osporavanje sistema, umanjenje bezbednosti itd.
Neni 26 **Pranueshmeria e sistemit**	**Article 26** **System eligibility**	**Član 26** **Prijem sistema**
1. Kriteret e praneushmërisë për sistemet e reja informative, përmirësimet dhe versionet e reja, përcaktohen nga testimet paraprake të sistemit. Menaxherët përkujdesen që kushtet dhe kriteret për pranim të sistemeve të reja të definohen qartë, të dakordohen, të dokumentohen dhe të testohen, duke marrë parasysh:	1. Eligibility criteria for new information systems, new upgrades and versions are determined by preliminary system testing. Managers ensure that conditions and criteria for acceptance of new systems are clearly defined, agreed, documented and tested, by taking into account:	1. Kriterijumi nepristrasvenosti za novi informativni sistem, popravke i nove verzije, se odredjuju prema prethodnih testiraja sistema. Menadžmenti se staraju za uslove i kriterijume u prijemu novih sistema koji se definiraju jasno, da se dakorduju, dokumentiraju i testiraju uzimajući u obzir:
1.1. Puna dhe kapaciteti i nevojshëm i pajisjeve të sistemit; 1.2. Procedurat për rimëkëmbje nga dëmtimet, si dhe planet rezervë; 1.3. Përgatitja dhe testimi i procedurave rutinore operative në përputhje me standardet e definuara; 1.4. Dëshmi që instalimi i sistemit të ri nuk do të ndikojë negativisht në sistemet ekzistuese, posaçërisht në kohën me vëllim më të madh të punës; 1.5. Dëshmi që i është kushtuar vëmendje e mjaftueshme sistemi të ri mbi sigurinë e përgjithshme të institucionit;	1.1. Necessary work and capacity of the system devices; 1.2. Procedures for recovery from damages, and backup plans; 1.3. Preparation and testing of routine operating procedures in accordance with defined standards; 1.4. Evidence that the installation of the new system will not negatively affect in existing systems, especially in time with greater volume of work; 1.5. Evidence that sufficient attention is paid to the new system of general security of the institution;	1.1. Posao i potrebni kapaciteti za opremu sistema; 1.2. Procedure za obnovu oštečenja, kao i rezervni planovi; 1.3. Priprema i testiranje rutinskih procedura operative s hodno definisanim uara standardima; 1.4. Dokaze koji dokaže da instalacja novog sistema neće negativno uticati u postojećim sistemima, posebno za vreme intenzivnog rada; 1.5. Dokaz kome je predata posebna pažnja novom sistemu i opšte bezbednosti institucije;

1.6. Trajnim adekuat për punën me sistemet e reja dhe shfrytëzimi i tyre.	1.6. Adequate training to work with new systems and their use.	1.6. Adekuatno trajniranje o poslovima sa novim sistemima i njihovo korišćenje.
Neni 27 **Mbrojtja kundër softuerit të dëmshëm**	**Article 27** **Protection against harmful software**	**Član 27** **Zaštita protiv štetnog softuera**
1. Mbrojtja kundër softuerit të dëmshëm të jetë e bazuar në përgjegjësinë mbi sigurinë, qasjen adekuate sistemit dhe rregullat në ndryshimin e menaxhimit, duke iu përmbajtur procedurave vijuese: 1.1. Qasje të formësuar me të cilën obligohet respektimi i licencave softuerike dhe ndalimi i shfrytëzimit të softuerit të paautorizuar; 1.2. Qasje të formësuar për mbrojtje nga rreziqet që ndërlidhen me sigurimin e skedarëve (file) dhe softuerit, qoftë përmes rrjetave të jashtme, qoftë përmes ndonjë mediumi tjetër; 1.3. Instalimi dhe përditësimi i rregullt i softuerit antivirus për zbulimin dhe eliminimin e viruse-ve, për të skanuar kompjuterët dhe mediumet qoftë si kontrollim paraprak, mbrojtës ose si rutinë;	1. Protection against harmful software is based on responsibility for security, adequate access to the system and change management rules by complying with the following procedures: 1.1. Formed approach which obligate respecting software licenses and preventing unauthorized use of software; 1.2. Formed access for protection against risks related to file security and software, either through external networks or through any other medium; 1.3. Regular installation and update of antivirus software to detect and eliminate viruses, to scan computers and media either as a preliminary, protection or as a routine examination;	1. Zaštita protiv štetnog softuera Treba biti osnivana na odgovornost nad bezbednost, adekuatan nastup po sistemima i pravila o izmeni menadžiranja, pridržavajućise sledečim procedurama: 1.1. Formirase nastup kojim obavezujese poštovanje licencijama softuera i sprećavanje korišćenja neovlaščenog softuera; 1.2. Formirase zaštita od rizika koja su podvezana sa obezbedjenjem skedara (file) i softuera, bilo i preko vanjskih mreži, bilo preko nekog drugog mediuma; 1.3. Instaliranje i redovna upotreba softuera antivirus za otkrivanje i elimininranje virusa, skaniranje kompjutera i mediuma bilo kao prethodna kontrola, zaštite ili kao rutina;

1.4. Prania e ndonjë skedari të paautorizuar ose ndryshimeve jo të autorizuara duhet zyrtarisht të hetohen; 1.5. Kontrollimi para përdorimit i shtojcave elektronike dhe gjësendeve të nxjerra nga interneti se mos përmbajnë softuer të dëmshëm; 1.6. Procedurat e menaxhimit dhe përgjegjësia për punë në mbrojtje kundër viruseve, trajnim për përdorim të tyre; 1.7. Planet përkatëse për vazhdimësi të punës pas rimëkëmbjes nga sulmet e viruseve, duke përfshirë kopjet rezervë të të dhënave dhe softuerit të nevojshëm; 1.8. Procedurat për të verifikuar të gjitha informatat lidhur me softuerin e dëmshëm, si dhe përpilimi i buletineve paralajmëruese dhe informuese.	1.4. The presence of an unauthorized file or change must be investigated; 1.5. Checking before using e-mail attachments and items taken from the Internet if they contain harmful software; 1.6. Management and accountability procedures for work in protection against viruses, training for their use; 1.7. Respective plans for ongoing work after recovery from virus attacks, including backup copies of data and software needed; 1.8. Procedures for verifying all information related to harmful software, and production of warning and information bulletins.	1.4. Prisutnost bilo kog neovlaščenog skedara ili izmenama treba da se službeno istraga; 1.5. Kontrola prie upotrebe elektronike dodatne pošte i ostalim stvarima koja su vadjena od interneta da li imaju štetnog softuera; 1.6. Procedure menadžiranja i odgovornost za rad u zaštiti protiv virusa, trajniranjeza njihovu upotrebu; 1.7. dotični Planovi za rad u nastavku za atakiranje virusa, obuhvativši i rezerve kopije podataka i potrebnog softuera; 1.8. Procedure za verifikovanje svake informacije o štetnom softueru, kao i sastavljanje prijvljenih buletina i informisanja.
Neni 28 **Kopjet rezervë të informatave** 1. Kopjimi i informatave dhe softuerit kryesor të bëhen rregullisht**.** 2. Të sigurohen pajisjet adekuate për kopjet rezervë në mënyrë që të gjitha informatat dhe softueri kyç të rimëkëmbet pas ndonjë fatkeqësie apo prishjeje të mediumeve, duke	**Article 28** **Backup information** 1. Copy of information and main software must be done regularly. 2.Adequate backup device, in order that all key information and software recover after a disaster or media failure must be provided by taking into account the following	**Član 28** **Rezervna Kopija informacije** 1. Kopiranje informacije i glavnog softuera treba uraditi redovno. 2. Da se obezbede redovno adekuatja oprema za rezervna kopija na taj način svaka informacija i glavni softueri treba daa se obnovi nakon incidenta ili kvara

marrë parasysh kriteret vijuese: 2.1. Kopjet rezervë dhe procedurat për riaktivizim të dokumenteve të ruhen në një lokacion të largët, në largësi të mjaftueshme për t'iu shmangur dëmeve nga fatkeqësia; 2.2. Ruajtja e informatave dhe softuerëve rezerve të ketë nivel adekuat të mbrojtjes fizike dhe ambientore në përputhje me standardet e sigurisë; 2.3. Mediet rezervë të testohen rregullisht; 2.4. Aftësia për rimëkëmbje të sistemit të kontrollohet dhe të testohet rregullisht në mënyrë që të jetë efektive për kryerjen e detyrave të parapara me procedura operacionale për rimëkëmbje; 2.5. Periudha e ruajtjes së kopjeve rezervë për dokumentet me rëndësi kyçe dhe mënyra e ruajtjes së kopjes arkivore rregullohet në përputhje me legjislacionin në fuqi. 3. Personeli operues të mbajë regjistër të aktivitetit të vet që duhet të përfshijnë: 3.1. Kohën e fillimit dhe mbylljes së sistemit;	criteria: 2.1. Backup copies and procedures for reactivation of documents must be stored in a distant location; distant enough to avoid damages from disaster; 2.2. Storing of information and backup software must have adequate level of physical and environmental protection in accordance with the security standards; 2.3. Backup media must be regularly tested; 2.4. The ability for system recovery must be controlled and tested regularly in order to be effective for performing tasks under the operational procedures for recovery; 2.5. Period of backup storage for important documents and the way of preserving archival copy shall be regulated in accordance with the legislation in force. 3. Operating personnel shall keep records of its activities which shall include: 3.1. Starting and closing time of the system;	mediuma, imajući u obzir sledeće kriteriume: 2.1. Rezervna kopija i procedure za reaktiviziranje dokumenata da se očuvaju u jednoj daljnoj lokaciji, u dovoljnoj daljini da bih izbegli teti od nesreće; 2.2. Sačuvanje informacija u rezervnim softuerima u adekuatnom nivou fizike zaštite i ambijenta u sklapu bezbednog standarda; 2.3. Rezervna Medija redovno se testiraju; 2.4. Sposobnost za obnovu sistema kontrole testirase redovno na taj način obezbedjuje efektivnost na obavljanju predvidjenih zadataka operacionih procedura za obnavljenju; 2.5. Period sačuvanja rezervnih kopija za značajnu dokumentaciju i namin sačuvanja arhivskog kopija i sredjujese s hodno legislacije u snagu. 3. Operacioni Personel održavaju registar o svojoj aktivnosti koja obuhvataju: 3.1.Vreme početka i kraja sistema;

3.2. Gabimet sistemore dhe masat korrigjuese që janë ndërmarrë; 3.3. Konfirmimin mbi punën e drejtë me skedarët e të dhënave dhe me rezultatet e konfirmuara nga pajisjet kompjuterike; 3.4. Emrin e personit që regjistron këto të dhëna në regjistër; 3.5. Regjistrat e operatorëve t'iu nënshtrohen kontrollimeve të rregullta zyrtare sipas procedurave operacionale. 4. Gabimet raportohen dhe regjistrohen, si dhe merren masat korrigjuese: 4.1. Shqyrtimi i gabimeve të regjistruara - për të parë nëse këto janë zgjidhur në mënyrë të kënaqshme; 4.2. Shqyrtimi i masave korrigjuese - për të parë nëse janë rrezikuar rregullat, dhe nëse veprimet e ndërmarra janë plotësisht të autorizuara. **Neni 29** **Menaxhimi i rrjetit** 1. Menaxherët e rrjeteve duhet të zbatojnë mbikëqyrje profesionale për të arritur mbrojtjen e të dhënave në rrjet dhe	3.2. System errors and corrective measures undertaken; 3.3. Confirmation of the correct work with data files and confirmed results by computer equipment; 3.4. The name of person who records the data in the database and 3.5. Operator's registers shall be subject to regular official examinations according to operational procedures. 4. Errors shall be reported and recorded, and correctional measures shall be undertaken: 4.1. Review of recorded errors - to see if they are satisfactorily resolved; 4.2. Review of correctional measures - to see if the rules are risked, and whether actions taken are fully authorized. **Article 29** **Network management** 1. Network managers need to implement professional supervision in order to achieve data protection in network and protection of	3.2. Greške u sistemu i preduzete mere korigovanja; 3.3. izlaganje o njegovim pravilima rada skedara podataka i prestavljanje rezultatima vrednovanje kompjuterike opreme; 3.4. Ime persone koja izvrši registraciju podataka u registar; 3.5. Registri operatora koja podlažu redovnoj službenoj kontroli prema operacionoj proceduri. 4. Greške se izveštavaju i registruju, kao i preduzimajuse mere korigovanja: 4.1. Razmatranje grešaka u registraciji – da bih videli ukoliko su rešavane u zadovoljavajući način; 4.2. Razmatranje mera korigovanja –da bih videli koliko su rezikovana pravila, i dali su preduzeta dela potpuno ovlaščene. **Član 29** **Menadžiranje mreže** 1. Menadžer mreže treba da sprovede stručno nadgledanje da bih sigurno postigo zaštitu podataka u mreži i zaštitu

mbrojtjen e shërbimeve të përfshira nga qasja e paautorizuar, duke marrë parasysh kontrollimet vijuese: 1.1. Përgjegjësia operacionale për rrjet, të ndahet nga përgjegjësia për operacionet kompjuterike; 1.2. Përcaktohen përgjegjësitë dhe procedurat për menaxhimin e pajisjes; 1.3. Të vihen në zbatim kriteret e veçanta të kontrollit për të ruajtur fshehtësinë dhe tërësinë e të dhënave që kalojnë në rrjetin publik, dhe të mbrohen sistemet e kyçura; 1.4. Aktivitetet e menaxhmentit duhet ngushtë të koordinohen, për t'i ngritur nivelet e shërbimeve dhe për të qenë të sigurt se kriteret zbatohen në mënyrë të njëjtë, në të gjithë infrastrukturën e përpunimit të informatave. **Neni 30** **Puna me mediume dhe siguria e tyre** 1. Menaxhimi i mediumeve të lëvizshme kompjuterike, siç janë: shiritat, disqet, kasetat dhe raportet e shtypura, bëhet duke respektuar këto kritere:	services included from unauthorized access, taking into account the following checking: 1.1. Operational responsibility for network must be separated from responsibility for computer operations; 1.2. Responsibilities and procedures for managing devices is defined; 1.3. To implement control specific criteria in order to maintain the confidentiality and integrity of data passing through the public network and to protect systems involved; 1.4. Management activities should be closely coordinated in order to raise the level of services and to be sure that the criteria are applied in the same way, in the whole information processing infrastructure. **Article 30** **Working with media and their security** 1. Computer removable media management, such as tapes, discs, cassettes and printed reports, shall be made by respecting the following criteria:	usluga od neovlašđčenih pristupa, imajući u obzir sledeću kontrolu: 1.1. Operacionalna odgovornost za mreže, odvajase od kompjuterske Operacionalne odgovornosti; 1.2. Odredjujuse odgovornosti i procedure za menadžiranje visoke opreme**;** 1.3. Sprovesti posebne kriterijume kontrole da se očuva tajna svakog podatka koja idu na javnoj mreži, i time se zaštite uključeni sistemi; 1.4. Aktivnosti menadžmenta treba da se koordiniraju, da bih ojačali svaki nivo usluga i da bi zagarantovali da kriterjumi sesprovode pod jednake, u celoj infrastrukturi prerade informacija. **Član 30** **Rad u medijama i njihova bezbednost** 1. Menadžiranje pokretnih kompjuterh medija, i to : trake, disk, kasete i otkucani izveštaji, poštovanjem sledećih kriterijuma:

1.1. Nëse mediume të ndryshme të përdorura në institucione të caktuara më nuk janë të nevojshme, atëherë përmbajtja e tyre duhet të fshihet para se të përdoret përsëri; 1.2. Për të gjitha mediumet e larguara kërkohet autorizim përkatës dhe mbahen shënimet mbi largimet e tilla për nevoja të revizionit; 1.3. Të gjitha mediumet ruhen në ambient të sigurt, në përputhje me specifikimet e prodhuesve.	1.1. If different media used in certain institutions are no longer needed, then their contents must be removed before it is used again; 1.2. For all removed media, respective authorization is required and records must be kept for such removals for audit purposes; 1.3. All media is stored in a safe environment, in accordance with manufacturer's specifications.	1.1. Ako neki mediumi nisu potrebni za odredjene institucije, u toj prilici treba da se obriše prije iduće upotrebe; 1.2. Za svaku pomerenju, udaljanju medijuma potrebno je dotično ovlaščenje i održavajuse na pismeno beleške o istim udaljavanju za postove revizije; 1.3. Svaki medium očuvase u sigurnom ambijentu, s hodno specifikacijama proizvodjača.
Neni 31 **Asgjësimi i mediumeve** 1. Asgjësimi i mediumeve të pa nevojshme bëhet në mënyrë të sigurt. 2. Asgjësimi i artikujve të ndjeshëm regjistrohet çdoherë që është e mundur në mënyrë që të ruhet një gjurmë për revizionin.	**Article 31** **Destruction of media** 1. The destruction of unnecessary media shall be done in secured way. 2. Destruction of sensitive items shall be recorded every time when possible in order to keep a trail for audit.	**Član 31** **Poništenje medijuma** 1. Poništenje nepotrebnih medijuma izvrši se na siguran način. 2. Poništenje osetljivih artikala, registrujese vaki put kada je moguće kako bih očuvali tragove za reviziju.
Neni 32 **Procedurat e punës me informata** 1. Mbrojtja e informatave nga shpalosja e	**Article 32** **Information working procedures** 1. Protecting information from unauthorized	**Član 32** **Procedura rada sa informacijama** 1. Zaštita informacija od neovlaščenih

paautorizuar apo nga keqpërdorimi, duhet të punohet në përputhje me klasifikimin e tyre, duke respektuar kriteret vijuese: 1.1. Puna me mediume dhe emërtimi i tyre; 1.2. Kufizimi i qasjes në mënyrë që të identifikohet personeli i paautorizuar; 1.3. Mirëmbajtja e regjistrit zyrtar të përdoruesve të autorizuar të të dhënave; 1.4. Përkujdesja që të dhënat e vendosura të jenë të sakta; 1.5. Mbrojtja e të dhënave që janë në pritje për t'u përpunuar, në përputhje me ndjeshmërinë e tyre; 1.6. Shënjimi i qartë i të gjitha kopjeve të të dhënave që duhet të pranohen nga zyrtari i autorizuar. 2. Regjistrimet e operuesve i nënshtrohen kontrollimit të rregullt zyrtar sipas procedurave të punës. 3. Siguria e dokumentacionit të sistemuar nga qasjet e paautorizuara përfshirë: 3.1. Dokumentacioni i sistemuar ruhet në mënyrë dhe vend të sigurt;	display or misuse should be done in accordance with their classification, respecting the following criteria: 1.1. Working with the media and their naming; 1.2. Restriction of access in order to identify unauthorized personnel; 1.3. Maintaining the official registry of authorized data users; 1.4. Ensure that the data set to be accurate; 1.5. Protection of data that are pending to be processed in accordance with their sensitivity; 1.6. Marking clear of all copies of data that must be received by the authorized official. 2. Operator's recordings are subject to regular official inspection, in accordance to working procedures. 3. Safety of systemized documentation from unauthorized access includes: 3.1. Documentation systemized and stored in a safe place;	prelistanja iliod zloupotrebe, treba da se radi u skladu sa njihovim klasifikovanjem, poštovajući sledeće kriterijume: 1.1. Rad sa medijama i njihovo imenovanje; 1.2. Ograničenje pristupa na taj način da se identifikuje neovlaščeno lice; 1.3. održavanje službenog regjistra neovlaščenih korisnika za podatke; 1.4. Potruditi se da podatke postavljene budu tačne; 1.5. Zaštita podataka koja su na čekanju za preradu, shodno njihove osetljivosti; 1.6. Beležavati jasno svaku datu kopiju koja treba da se primi od strane ovlaščenog lica. 2. Registracija operatora podlažuse redovnoj službenoj kontroli prema procedurama rada. 3. Bezbednost dokumentacije koja su sistemirana od neovlađčenih nastupa: obuhvatati: 3.1. Sistemirana Dokumentacija očuvase na sigurnom i sugurnim načinima;

3.2. Lista e qasjes në dokumentacione sistemore të mbahet në nivelin minimal dhe të jetë e autorizuar nga përgjegjësi i programit; 3.3. Dokumentacioni i sistemuar që mbahet në rrjetin publik, apo që furnizohet përmes rrjetit publik, duhet të jetë i mbrojtur në mënyrë adekuate.	3.2. List of access to systemized documents shall be held at the minimum level and be authorized by the one responsible for the program; 3.3. Systemized documentation held in public network, or supplied through the public network must be protected adequately.	3.2. Spisak nastupa u sistematiku dokumentaciju održavase u minimalu i treba da bude ovlaščena od odgovorna lica programa; 3.3. Sistemirana Dokumentacija koja se održava u javnohj mreži, ili koja se snabdeva preko jave mreže, treba biti zaštičena prema posebnom načinu.
Neni 33 **Siguria e mediumeve gjatë transportit**	**Article 33** **Media safety during transportation**	**Član 33** **Bezbednost medijuma tokom transporta**
1. Për sigurinë e mediumeve gjatë transportimit duhet të merren parasysh: 1.1. Shfrytëzimi i transportit të besueshëm; 1.2. Paketimi të jetë i mjaftueshëm për të mbrojtur përmbajtjen nga çfarëdo dëmi fizik; 1.3. Miratohen rregulla të veçanta, çdoherë që është e nevojshme, për të mbrojtur të dhënat e ndjeshme prej shpalosjes dhe ndryshimeve të paautorizuara.	1. For media safety during transport the following should be taken into account: 1.1. Using a reliable transport; 1.2. Packing to be sufficient to protect the contents from any physical damage; 1.3. Special rules are adopted, any time when necessary to protect sensitive data from unauthorized disclosure and changes.	1. Za bezbednost medijuma tokom transporta treba imati u vidu sledeće: 1.1. uipotrebljavati poverljiv transport; 1.2. Paketiranje da bude prema potrebi da bih se zaštitilo od slučajne fizike štete; 1.3.Usvajajuse posebna pravila, uvek oseča se potreba da se zaštiti osetljive podatke,od raznih prelistavanja i neovlaščene izmene.

Neni 34 Siguria e postës elektronike	Article 34 Electronic mail security	Član 34 Bezbednost elektronike Pošte
1. Politika e sigurisë për postën elektronike përfshinë: 1.1. Mbrojtjen e postës elektronike; 1.2. Udhëzimet se kur nuk duhet të përdoret posta elektronike; 1.3. Përgjegjësinë e nëpunësit që të mos keqpërdor postën elektronike për shpifje, ngacmime, blerja e paautorizuar etj.; 1.4. Përdorimin e teknikave kriptografike për të mbrojtur fshehtësinë dhe integritetin e porosive elektronike; 1.5. Kontrollet shtesë për të verifikuar shkëmbimin e porosive, për të cilat nuk mund të vërtetohet autenticiteti.	1. Email security policy includes: 1.1. Protection of electronic mail; 1.2. Instructions when electronic mail should not be used; 1.3. Responsibility of employee not to misuse the email for defamation, harassment, unauthorized acquisition, etc.; 1.4. Using cryptographic techniques to protect the confidentiality and integrity of electronic messages; 1.5. Additional controls to verify the exchange of messages for which the authenticity can not be verified.	1. Politika bezbednosti za elektroniku poštu obuhvata: 1.1.Zaštita elektron ske pošte; 1.2. Upustva kada ne treba da se koristi elektronska pošta; 1.3. Odgovornost službenika da ne zloupotrebljava elektronska pošta za intrige,povrede, neovlaščenu kupovinu itd.; 1.4. Korišćenje kriptografske teknike kriptografike da bi sačuvao tajnu dhe integritet elektronskih poruka; 1.5. Dodatna kontrola za poveravanje i izmenu poruka, za koja nemože da se potvdi autenticitet.
2. Sistemet që vihen në dispozicion të publikut në mënyrë elektronike, duhet të jetë në përputhje me legjislacionin në fuqi.	2. Systems that are available to the public electronically must be in accordance with applicable law.	2. Sistemi koji se stavljaju na dispoziciji u javnosti elektronski, treba da bude u skladu legislacije na snagu.
Neni 35 Menaxhimi i qasjes dhe privilegjeve të shfrytëzuesve	**Article 35 Management of user access and privileges**	**Član 35 Menadžiranje nastupa i privilegje korisnika**
1. Menaxhimi i qasjes së shfrytëzuesve	1. Management of user access covers all	1. Menadžiranje nastupa korisnika pokrije

mbulon të gjitha fazat ciklike, duke filluar prej regjistrimit fillestar të shfrytëzuesve të rinj e deri te çregjistrimi përfundimtar i shfrytëzuesve.	cyclic stages, beginning from initial registration of new users to the final cancellation of most users.	svaku fazu, počevši od početne registracije novih korisnika do konačnog otpisanja korisnika.
2. Dhënia dhe shfrytëzimi i privilegjeve duhet të jetë e kufizuar dhe e kontrolluar, duke i marrë parasysh hapat vijues: 2.1. Duhet të identifikohen privilegjet e ndërlidhura me çdo sistem, si: sistemi operativ, sistemi i menaxhimit të bazës së të dhënave, dhe për çdo program të bëhet kategorizimi i stafit për këto privilegje; 2.2. Privilegjet iu ndahen shfrytëzuesve sipas detyrave të punës; 2.3. Përcaktohet procesi i autorizimit dhe ruhet regjistri i të gjitha privilegjeve që janë të ndara; 2.4. Privilegjet nuk ndahen përderisa të mos jetë kryer procesi i autorizimit.	2. Provision and use of privileges should be limited and controlled, taking into account the following steps: 2.1. Privileges linked with each system must be identified, such as operating system, database management system, and categorization of staff privileges must be done for every program; 2.2. Privileges shall be divided to users according to their working tasks; 2.3. The authorization process is defined and database of all divided privileges is stored; 2.4. Privileges shall not be divided while the authorization process is not performed.	2. Davanje i korišćenje privilegija treba da bude ograničena i kontrolisana imajući u vidu sledeće korake: 2.1. Treba identifikovati povezane privilegje sa svakim sistemima, i to: operativni sistem, sistemi menadžiranja baze podataka,i za svaki program izvršavase kategorizovanje stafa pod istim privilegijama; 2.2. Privilegije se dele korisnicima prema radnim zadacima; 2.3. odredjujese proces ovlaščenja, očuvase registar svake dodeljene privilegije; 2.4. Privilegije se ne dele sve dok se ne izvrši proces ovlaščenja.
3. Të drejtat e shfrytëzuesve në qasje të rishqyrtohen në intervale të rregullta (rekomandohet një periudhë çdo 6 muaj) dhe pas çfarëdo ndryshimi.	3. The rights of users to access to be reviewed at regular intervals (recommended every six months period) and after any changes.	3. Prava korisnika u nastup ponovnog razmatranja u redovnim intervalima (preporučujese period svakog 6 meseca) i nakon svake izmene.
4. Autorizimet për të drejtat speciale të	4. Authorization for special rights to	4. Ovlaščenja za specialja prava ,

qasjes së privilegjuar rishqyrtohen në periudha të shpeshta kohore, së paku në çdo 3 muaj. 5. Dhënia e privilegjeve kontrollohet në intervale të rregullta në mënyrë që të mos jepen privilegje të paautorizuara.	privileged access is revised in frequent periods of time, at least every three months. 5. The granting of privileges is checked at regular intervals in order to prevent unauthorized privileges.	privilegovani nastup ponovnog razmatranja u čestim vremenskim periodima, najmanje svakog 3 meseca. 5. Davanje privilegija je pod kontrolom u redovnim intervalima da bih se ne izdavale privilegije neovlaščeno.
Neni 36 **Menaxhimi i Fjalëkalimeve** 1. Ndarja e fjalëkalimeve kontrollohet përmes një procesi formal të menaxhimit dhe merren parasysh rregullat vijuese: 1.1. Shfrytëzuesit nënshkruajnë deklaratën për t'i ruajtur të fshehta, fjalëkalimet personale dhe ato të punës grupore; 1.2. Kur shfrytëzuesit kërkojnë t'i kenë fjalëkalimet e veta, atyre në fillim iu jepet një fjalëkalim i përkohshëm, të cilin ata janë të detyruar menjëherë ta ndërrojnë; 1.3. Fjalëkalimet e sigurta t'iu jepen shfrytëzuesve në mënyrë të sigurt dhe pranuesit duhet të konfirmojë pranimin e fjalëkalimeve; 1.4. Fjalëkalimet nuk duhet të ruhen në sisteme kompjuterike në formë të	**Article 36** **Password Management** 1. Sharing of passwords is controlled through a formal process of management and the following rules shall be taken into account: 1.1. Users sign a statement to keep confidential the personal passwords and group work; 1.2. When users seek to have their passwords, they were initially given a temporary password, which they must change immediately; 1.3. Secure passwords shall be given to users in a secured way and the recipient must confirm acceptance of passwords; 1.4. Passwords should not be stored in computer systems in unprotected form.	**Član 36** **Menadjiranje Lozinke(pasworda)** 1. Dodela lozinke je pod kontrolom preko formalnog procesa menadžiranja pod sledećim pravilima: 1.1. Korisnici potpisuju deklaraciju za očuvanje tajne, ličnu lozinku i one sa radhe grupe; 1.2. Ako korisnici zahtevaju posedovati svoju lozinku, njima se daje jedna privremena lozinka, koju su prinudjeni odmah da promene; 1.3. sigurna lozinka daje se korisnicima i oni treba da utvrdjuju prijem lozinke; 1.4. Lozinke ne treba da se sačuvaju u kompjuterskim sistemima u ne zaštičenoj

pambrojtur. 2. Për përdorim të fjalëkalimeve shfrytëzuesit udhëzohen që: 2.1. Fjalëkalimet t'i mbajnë të fshehta; 2.2. T'iu shmangen regjistrimit të fjalëkalimeve në letër, përveç nëse ai mund të ruhet në vend të sigurt; 2.3. Të ndryshojnë fjalëkalimin çdoherë që ekzistojnë shenja të rrezikimit të mundshëm të sistemit apo fjalëkalimit; 2.4. Të përzgjedhin fjalëkalimet cilësore me një gjatësi minimale prej gjashtë karaktereve: 2.4.1. Të jenë lehtë për t'u mbajtur në mend; 2.4.2. Të mos jenë të bazuar në: emra, numra telefoni dhe data të lindje; 2.4.3. Të mos jenë me karakter identik ose grupe shenjash që përmbajnë vetëm numra apo vetëm shkronja. 2.5. Të ndryshojnë fjalëkalimet në intervale të rregullta; 2.6. Ndalohet ripërdorimi i fjalëkalimeve të vjetra; 2.7. T'i ndryshojnë fjalëkalimet e	2. In order to use passwords, users are instructed to: 2.1. Keep passwords confidential; 2.2. Avoid registration of password in the paper, unless it can be stored in a safe place; 2.3. To change password anytime there are signs of possible risk of system or password; 2.4. Select quality passwords with a minimum length of six characters: 2.4.1. Easy to remember; 2.4.2. Not to be based on: names, phone numbers and date of birth; 2.4.3. Not to be of identical character or sets of signs containing only numbers or letters. 2.5. Change passwords at regular intervals; 2.6. The reuse of old password is prohibited; 2.7. To change temporary passwords by	formi. 2. Za korišćenje lozinke i korisnika upućujuse kao sledeće: 2.1. Lozinka da se održava tajna; 2.2.Da izbegavaju registracji lozinke u papiru, osim ako isti može da se sačuva na sigurno mesto; 2.3. za izmenu lozinke uvek postoji znaci rizika sistema ili lozinke; 2.4. treba da se izaberu lozinke minimalnom dužinom od šest karaktera: 2.4.1. Da budu lake za pamćenje; 2.4.2. Ne mora da su vezane ili bazirane na: imena, brojeva telefona i rodjendana; 2.4.3. Ne mora da su identičnim karakterom ili grupa znakova koja sadrži samo brojke ili slova. 2.5. Izmena lozinke u redovnim intervalima; 2.6. zabranjuje se ponovokorišćenje starih lozinki; 2.7. Izmeniti privremene lozinke kada

përkohshme me të hyrë në program për herë të parë.	entering the program for the first time.	se ultazi u programu po prvi put.
Neni 37 **Kriteri i qasjes në rrjet**	**Article 37** **Network Access criteria**	**Član 37** **Kriterijumi nastupa na mreži**
1. Qasja në rrjetin e brendshëm dhe të jashtëm duhet të jetë e kontrolluar dhe rruga në çdo pikë të rrjetit të jetë paraprakisht e definuar:	1. Access to internal and external network should be checked and the route at any network point to be defined in advance:	1. Nastup na unutrašnju i spoljnu mrežu treba da bude pod kontrolom i svaka tačka treba da bude prethodno definisana:
1.1. Caktimi i linjave dhe numrave të posaçëm të telefonave; 1.2. Kufizimi i opsioneve nga menyja dhe nënmenyja për shfrytëzuesit e caktuar; 1.3. Parandalimi i bredhjes së pakufizuar nëpër rrjet (roaming); 1.4. Zbatimi i shfrytëzimit të detyrueshëm të sistemeve të caktuara programore dhe portave të sigurisë për shfrytëzuesit e jashtëm të rrjetit; 1.5. Kontrollimi aktiv i komunikimeve burim – destinacion përmes portave të sigurta; 1.6. Kufizimi i qasjes në rrjet, duke rregulluar domene të veçanta logjike, për grupet e shfrytëzuesve përbrenda institucioneve.	1.1. Determination of special lines and phone numbers; 1.2. Restriction of menu and sub-menu options for certain users; 1.3. Prevention of unlimited roaming to the network; 1.4. The implementation of mandatory use of certain programming systems and security gates for external users of network; 1.5. Active control of communications source - destination through secure gates; 1.6. Restriction of access to the network by adjusting the specific domains of logical user groups within institutions.	1.1. Odredjivanje linija i posebnih brojki telefona; 1.2. Ograničenje opsija od menija i podmenija za odredjenog korisnika; 1.3. Predzabrana neograničenih šetnji po mreži (roaming); 1.4. Sprovodjenje obaveznog korisnika, odredjenog programskog sistema i bezbednosnih ulaza za vanjski korisnici mreže; 1.5. aktivna Kontrola izvornih komuniciranja – destinacija preko sigurnim ulazima; 1.6. Ograničenje nastupa u mreži, sredjiva posebne domene i logične, za grupe korisnika unutar institucija.

2. Kyçjet e jashtme në rrjet, i nënshtrohen kontrollimit dhe verifikimit. 3. Politika e kontrollit të qasjes për rrjetet e përbashkëta, posaçërisht ato që shtrihen përtej kufijve të rrjetit qeveritar, kërkojnë trupëzimin e kontrolluesve për të kufizuar mundësinë e kyçjes së shfrytëzuesve. Kufizimet që zbatohen të jenë të bazuara mbi politikën e qasjes dhe nevojat qeveritare dhe duhet të mirëmbahen dhe përditësohen në përputhje me to. 4. Qasja në sisteme operative të jetë e kontrolluar. 5. Të gjithë shfrytëzuesit duhet të kenë numër identifikues, në mënyrë që çdo veprim të ketë gjurmë, që të shpie deri te personi përgjegjës. **Neni 38** **Puna nga largësia** 1. Puna nga largësia të jetë e autorizuar dhe e kontrolluar: 1.1. Sigurimi i pajisjes së përshtatshme për arkivim nga largësia;	2. External connection to the network is subject to controlling and verification. 3. Access control policies for shared networks, especially those that lie beyond the government network, require solidification of controllers in order to limit the possibility of user's access. Restrictions that apply must be based on access policy and governmental needs and must be maintained and updated accordingly. 4. Access to operating systems to be controlled. 5. All users must have identification numbers so that every action has a trail that leads to the responsible person. **Article 38** **Work from the distance** 1. Work form the distance must be authorized and controlled: 1.1. Ensure appropriate archiving device from a distance;	2. vanjsko uključenje u mreži, podlažu se kontroli, utvrdjivanje. 3. Politika kontrole nastupa u zajedničkoj mreži,osobito one koje se šire van granica vladene mreže, zahtevaju osvajanje kontrolera koja ograničava mogučnost uključenja korisnika. Ograničenje se sprovedu bazirajućise u politici nastupa i vladenim potrebama i treba da se održavaju. 4. Nastup u operativni sistem je pod kontrolom. 5. Svaki korisnik treba da ima identifikovani broj, na taj način svaka radnja ostavlja trag, koja te postavlja pored odgovornog lica. **Član 38** **Posao sa daljine** 1. Posao sa daljine treba da bude pod ovlaščenjem i kontrolom: 1.1.Bezbednost opreme su prijatne za arhivira je sa daljine;

1.2. Përkufizimi i punës së nevojshme, orari i punës, klasifikimi i informatave që mund të ruhen, sistemi dhe shërbimet e brendshme për të cilat shfrytëzuesi ka leje t'iu qaset; 1.3. Sigurimi i pajisjes adekuate për komunikim, duke përfshirë metodat për sigurimin e qasjes nga larg; 1.4. Siguria fizike; 1.5. Sigurimi i mbështetjes dhe mirëmbajtjes për harduer dhe softuer; 1.6. Mbikëqyrja e revizionit dhe sigurisë; 1.7. Marrja e autorizimit dhe të drejtave në qasje, si dhe kthimi i pajisjeve kur të kryhen aktivitetet e punës nga largësia.	1.2. Definition of required work, working hours, classification of information that can be saved, the system and internal services that the user is allowed to have access; 1.3. Ensure adequate communication device, including methods for providing access from distance; 1.4. Physical security; 1.5. Provide support and maintenance for hardware and software; 1.6. Supervision of audit and security; 1.7. Obtaining authorization and access rights, and return the device when work activities are carried out from a distance**.**	1.2. Definisanje potrebnog rada, radno vreme, klasifikovanje informacija koja mogu da se sačuvaju, sistem i usluge unutrašnjih usluga za koja korisnik ima pravo nastupa; 1.3. Bezbednost adekuatne opreme za komuniciranje, metode za osiguravanje nastupa na daljini; 1.4. Fizička bezbednost; 1.5. Bezbednost naslaganja i održavanja harduera i softuera; 1.6. Nadgledanja bezbednosti revizije; 1.7. dobija ovlaščenje i pravo nastupa, kao i vraćenje opreme nakon obavljanja posla sa daljine.
Neni 39 **Zhvillimi dhe mirëmbajtja e sistemit**	**Article 39** **System Development and Maintenance**	**Član 39** **Razvoj i održavanje sistema**
1. Të dhënat mund të dëmtohen nga gabimet gjatë përpunimit dhe përmes veprimeve të qëllimshme. Kontrollet për vërtetim të tyre të përfshihen në sistem dhe të zbulojnë dëmtimet e tilla. 2. Përdorimi i programeve të sakta për rimëkëmbje pas dështimit, për të arritur përpunimin e saktë të të dhënave.	1. The data can be damaged by errors during processing and through deliberate actions. Controls for their verification should be included in the system and detect such damage. 2. Using the correct programs for recovery after failure in order to reach the correct data processing.	1. Podaci mogu da se oštećuju tokom prerade namernim dejstvom. Kontrola za njihovo utvrdjenje obuhvataju se u sistemu i otkriju ista oštečenja. 2. Upotreba tačnih programa za obnovu nakon neuspevanja, da bih postigli tačnu preradu podataka.

3. Për mbrojtjen e informatës, që konsiderohet e rrezikuar e për të cilën kontrollet e tjera nuk ofrojnë mbrojtje adekuate, duhet të përdorën sistemet dhe teknikat kriptografike. Rregullat e shfrytëzimit bazohen në: 3.1. Qasjen e menaxhmentit ndaj shfrytëzimit të kontrolleve kriptografike në të gjitha institucionet, duke përfshirë parimet e përgjithshme në bazë të të cilave informata duhet të mbrohet; 3.2. Qasja ndaj menaxhimit të çelësit, duke përfshirë metodat për t'u ballafaquar me rikthimin e informatës së koduar në rast se çelësat humben, rrezikohen apo dëmtohen. **Neni 40** **Kodimi** 1. Kodimi përdoret për mbrojtjen e informatave të ndjeshme dhe atyre të rëndësisë së veçantë. 2. Gjatë zbatimit të rregullave për kriptografi merren parasysh rregulloret dhe kufizimet shtetërore, që vlejnë për përdorimin e teknikave kriptografike.	3. For the protection of information, which is considered as risked and for which other controls do not provide adequate protection, cryptographic systems and techniques should be used. Terms of use are based on: 3.1. Management approach to the use of cryptographic controls in all institutions, including the general principles under which the information must be protected; 3.2. Access to key management, including methods for dealing with the return of coded information in the event that keys are lost, risked or damaged. **Article 40** **Coding** 1. Coding is used to protect sensitive information and those of particular importance. 2. During the implementation of rules for Cryptography, regulation and state restrictions that apply for the use of cryptographic techniques shall be taken into	3. Za zaštitu informacije, koja se smatra oštećena i ostala kontrola ne ponudi adekuatnu zaštitu, treba da se upotrebljava sistem i kriptografske tehnike.Pravila korišćenja se obaziraju na sledeće: 3.1. Nastup menadžmenta pri korišćenja kriptografske teknike u svaku instituciju, opštim načelima na osnovu kojih obezbedjujese zaštita informacije; 3.2. Nastup menadžmenta ključeva, koristeći metodponovnog vračanja kodirane informacije u slučaju ako se klučevi se izgube ili oštečuju. **Član 40** **Kodiranje** 1. Kodiranje se koristi za zaštitu osetljive informacije i posebne značajnosti. 2. Tokom sprovoda pravila kriptografije uzimaju se u obzir pravila i državna ograničenje, koje se koriste za upotrebu kriptografskih tehnika.

	account.	
Neni 41 **Nënshkrimet digjitale**	**Article 41** **Digital signatures**	**Član 41** **Digitalna potpisivanja**
1. Nënshkrimet digjitale mund të aplikohen në cilëndo formë dokumenti që përpunohet në mënyrë elektronike.	1. Digital signatures can be applied to any form of document that is processed electronically.	1. Digitalna potpisivanja mogu se aplicirati u svakoj formi dokumenta koja se radi elektronskoj formi.
2. Nënshkrimet digjitale mund të aplikohen duke përdorur teknika kriptografie të bazuar në një çift të çelësave të lidhur mes veti në mënyrë unike, ku njëri çelës përdoret për të krijuar nënshkrimin (çelësi privat) dhe tjetri për të kontrolluar nënshkrimin (çelësi publik).	2. Digital signatures can be applied using Cryptography techniques based in a couple of keys linked to each other in a unique way, where one key is used to create the signature (private key) and the other one to check the signature (public key).	2. Digitalna potpisivanja mogu se aplicirati kriptografskom tehnikom bazirana dvojnim ključevima koja su vezana unički izmedju sebi, jedan ključ se upotrebljava da bih napravio privatni kjluč (privatni kjluč) dok drugi za kontroll potpisa (javni kjluč).
3. Çelësat kriptografikë që përdoren për nënshkrime digjitale duhet të jenë të ndryshëm nga ata që përdorën për kodim.	3. Cryptographic keys used for digital signatures must be different from those used for coding.	3. Kriptografski ključevi koji se koriste za digitalni popis treba da se razlikuju od ključeva koja se koriste za kodiranje.
4. Menaxhimi i çelësave kriptografikë bazohet në këto teknika: 4.1. Teknikat e çelësit sekret, ku dy apo më shumë palë e mbajnë të njëjtin çelës dhe ky çelës përdoret si për kodim, ashtu edhe për dekodim; 4.2. Teknikat e çelësit publik, ku çdo	4. Management of cryptographic keys is based on these techniques: 4.1. Secret key techniques, where two or more parties share the same key and this key is used for coding, as well as for decoding; 4.2. Public key techniques, where each	4. Menadžiranje kriptografski ključeva obazirajuse u sledećoj tehnici: 4.1. Tehnika tajnog ključa, kada dva ili više stranke imaju isti ključ koji se koristi za kodiranje ili dekodiranje; 4.2. Tehnika javnog ključa, vaki korisnik

shfrytëzues ka një palë çelësa, një çelës publik dhe një çelës privat; 4.3. Të gjithë çelësat kyç të jenë të mbrojtur nga ndryshimi dhe shkatërrimi; 4.4. Mbrojtja fizike duhet të përdoret për të mbrojtur pajisjet që përdoren për përgatitjen, ruajtjen dhe arkivimin e çelësave.	user has a pair of keys, one public key and one private key; 4.3. All main keys to be protected from change and destruction; 4.4. Physical protection must be used to protect devices used for preparation, storage and archiving of keys.	ima par ključeva, jedan jahni i jedan privatni ključ; 4.3. Svaki značajni ključ treba biti zaštićen od izmene ili poništenja; 4.4. Fizička zaštita treba da se upotrebljava za zaštitu korišćene opreme koja se koristi tokom pripreme, očuvanju i arhiviranje ključeva;
Neni 42 **Siguria e skedarëve**	**Article 42** **File security**	**Član 42** **Bezbednost skedara**
1. Siguria e skedarëve dhe ruajtja e integritetit të sistemit është përgjegjësi e shfrytëzuesit dhe grupit programues të cilit i takon sistemi programor apo softueri.	1. Files security and maintaining system integrity is the responsibility of the user and programming group to whom the program system or software belongs.	1. Bezbednost skedara i očuvanje integriteta sistema je odgovornost korisnika i grupe programiranjakome pripala sistem programiranja ili softueri.
2. Kontrollimi i softuerit operacional mbështetet në këto rregulla:	2. Control of operational software shall be based on these rules:	2. Kontrola operacionog softuera ima sledeća pravila:
2.1. Përditësimi i librarive të programit operativ kryhet vetëm nga bibliotekari i emëruar pas autorizimit nga menaxhmenti; 2.2. Kodi ekzekutiv nuk duhet të zbatohet në një sistem operativ para sigurimit të dëshmive mbi testimin e suksesshëm dhe pranueshmërinë nga shfrytëzuesit, dhe	2.1. Update of operating library program shall be carried out only by the appointed librarian, upon authorized by the management; 2.2. Executive code shall not be applied to an operating system before providing evidence of successful testing and acceptability by the users, and after	2.1. Ažuriranje knižara operacionog programa obavljase samo od strane bibliotekara imenovan nakon ovlaščenja menadžmenta; 2.2. Kod ekzekutiva ne sme se sprovesti u operativnom sistemu pored sigurnih podataka o uspešnom testiranju i prisutnost korisnika,i nakon ažuriranja

pasi të jenë përditësuar libraritë burimore gjegjëse; 2.3. Për të gjitha përditësimet e librarive të programit operativ, duhet bërë raport; 2.4. Versionet e mëhershme të softuerit të ruhen si një masë rezervë; 2.5. Softueri që përdoret në sistemet operative mirëmbahet në nivelin që kërkohet nga furnizuesi; 2.6. Kalimi në versionin e ri, merr parasysh sigurinë e atij versioni; 2.7. Arnat softuerike (software patch) duhet të përdoren për të zvogëluar dobësitë në siguri.	relevant resource libraries are updated; 2.3. For all updates of operating program libraries a report should be drafted; 2.4. Previous versions of software shall be stored as a backup measure; 2.5. Software used in operational systems is maintained at the level required by the supplier; 2.6. Transition to the new version takes into account the safety of that version; 2.7. Software patches should be used in order to reduce weaknesses in security.	izvornih odgovoravajuće knižara; 2.3. Za vako ažuriranje knižara operativnog programa, treba izveštavati; 2.4. Stalna verzija softuera da se očuvaju kao rezerva; 2.5. Softuer koji se koristi operativnom sistemu održavase na nivou koji se zahteva od strane snabdevača; 2.6. Predjemo u novu verziju, imamo u vidu bezbednost iste verzije; 2.7. zakrpljenje u softueru (software patch) koriste se za smanjenje slabosti koji se pojavljuju tokom bezbednosti.
Neni 43 **Siguria gjatë proceseve të programimit dhe mbështetjes**	**Article 43** **Security during programming and support processes**	**Član 43** **Bezbednost tokom procesa programiranja i naslanjanja**
1. Procedurat e ndryshimeve operacionale përfshijnë: 1.1. Ndryshimet të jenë parashtruar nga shfrytëzuesit e autorizuar; 1.2. Rishqyrtimin e procedurave të kontrollimit dhe integritetit për të qenë të sigurt që këto nuk do të rrezikohen nga ndryshimet; 1.3. Identifikimin e të gjithë softuerit	1. Procedures of operational changes include: 1.1. Changes to be submitted by authorized users; 1.2. Review of controlling procedures and integrity in order to be sure that these will not be risked by changes; 1.3. Identification of all computer	1. Procedura operacionih izmena obuhvataju sledeće: 1.1. Izmene se predlažu od ovlaščenog korisnika; 1.2. Ponovo razmatranje procedura kontrole i integriteta treba da budu na sigurno da neće biti u rezik izmene; 1.3. Identifikovanje svakog

kompjuterik, informatave, bazave të të dhënave dhe harduerit që duhet t'iu nënshtrohen ndryshimeve; 1.4. Të sigurohet aprovimi zyrtar për propozimet e detajuara para fillimit të punës; 1.5. Pranimin e ndryshimeve nga ana e shfrytëzuesve të autorizuar para zbatimit të tyre; 1.6. Të sigurohet që zbatimi të kryhet në mënyrën, e cila do të minimizonte çrregullimet në sistem; 1.7. Të sigurohet që dokumentacioni sistemor të përditësohet pas kryerjes së çdo ndryshimi dhe dokumentacioni i vjetër të arkivohet apo të asgjësohet; 1.8. Ruajtja e gjurmës për revizionin për të gjitha kërkesat për ndryshime; 1.9. Të sigurohet që dokumentacioni operacional dhe procedurat për shfrytëzuesit të ndryshohen sipas nevojës, në mënyrë që të jenë adekuate.	software, information, databases and hardware that should be subject to change; 1.4. To provide formal approval for detailed proposals before starting the job; 1.5. Acceptance of changes by authorized users before their implementation; 1.6. To ensure that implementation be carried out in a manner that will minimize disturbance to the system; 1.7. Ensure that system documentation be updated after making any changes and old documents archived or destroyed; 1.8. Maintaining trails for all requests for changes for the audit; 1.9. To ensure that operational documentation and procedures for users to change as needed, in order to be adequate.	kompjuterskog softuera, informacija, baza podataka i harduera koji se podlažu izmenama; 1.4. Obezbediti službeno usvajanje za detale predloge prije početka sa radon; 1.5. Priznanje izmena od strane ovlaščenih korisnika prije njihovog sprovodjenja; 1.6. obavljati na taj način da se minimiziraju nered u sistemu; 1.7. Obezbediti da sistem dokumentacije treba ažurirati nakon svakog obavljanja izmena u staroj dokumentaciji , arhivirati ili poništiti; 1.8. Očuvanje tragova za reviziju za svaku izmenu i zahteve; 1.9. Obezbediti operacionu dokumentaciju i procedure za vrsne korisnike prema potrebi da bih bile adekuatne.
2. Shqyrtimi teknik i ndryshimeve në sistemin operativ përfshin:	2. Technical review of changes in the operating system includes:	2. Tehničko razmatranje izmena u operativnom na operativ sistemu obuhvatasu:
2.1. Rishqyrtimin e procedurave mbi kontrollin dhe tërësinë e programit për t'u përkujdesur që këto nuk janë rrezikuar	2.1. Review of procedures on the overall control program to ensure that these are not threatened by changes in the	2.1. PonovoPonovno razmatranje procedura o kontrolinad kontrolom i sadržaj celovitost programa, ostaratise za

nga ndryshimet në sistemin operativ; 2.2. Të sigurohet që njoftimi mbi ndryshimin e sistemit operativ të jetë dhënë me kohë, për të mundësuar kryerjen e rishqyrtimeve adekuate para vetë ndryshimit; 3. Gjatë ndryshime të pakove softuerike të merren parasysh: 3.1. Rrezikimi i kontrolleve të sendërtuara dhe i integritetit; 3.2. Mundësia e sigurimit të ndryshimeve të nevojshme si përditësime të rregullta programore; 3.3. Pasojat nga ndryshimet për institucionet; 3.4. Të gjitha ndryshimet testohen dhe dokumentohen, ashtu që ato të mund të përdoren për përditësimet e softuerit në të ardhmen. **Neni 44** **Kopjimi i softuerit** 1. Kriteret për kopjime të softuerit janë:	operating system; 2.2. Ensure that the information on changing the operating system is given due time in order to enable appropriate reviews prior to the change itself; 3. During the changes of software packages the following shall be taken into account: 3.1. the risk of realized controls and integrity; 3.2. Possibility of providing required changes as a regular program updates; 3.3. The effects of changes in institutions; 3.4. All changes are tested and documented, so that they can be used for software updates in the future. **Article 44** **Software copy** 1. Criteria to copy the software are:	staranje koja one koje nisu rezikovana od izmena doživele izmene operativnog sistema; 2.2. Obezbediti da se predaje izmene operativnog sistema blagovremeno da bih se moglo intervenisati na vreme, pored same izmene; 3. Tokom izmena softuerskih paketa treba imati u vidu: 3.1. Opasnost učinjenih kontroll i integriteta; 3.2. Mogučnost bezbednosti za potrebne izmene i redovno ažuriranja programa; 3.3. Posledice od izmena za institucije; 3.4. Izmene se testiraju i dokumentiraju, tako da u budućem one mogu da se koriste za ažuriranje softuera. **Član 44** **Kopiranje softuera** 1. Kriterjumi za kopiranje softuera su:

1.1. Njohja mbi të drejtat në kopjim të softuerit, blerjes së tyre dhe ndërmarrja e masave disiplinore kundër stafit që i shkel këto; 1.2. Ruajtja e dëshmisë mbi pronësinë e licencave; 1.3. Zbatimi i kritereve për t'u përkujdesur që të mos tejkalohet numri maksimal i lejuar i shfrytëzuesve; 1.4. Kontrollimi përkatës për të parë nëse janë instaluar vetëm produkte dhe softuerë të licencuar; 1.5. Përmbushja e kushteve adekuate të licencës; 1.6. Shfrytëzimi i veglave përkatëse për revizion.	1.1. Knowledge on the rights to copy the software, purchasing and undertaking disciplinary measures against staff that violate these rights; 1.2. Preservation of proof of ownership and licenses; 1.3. Application of criteria to ensure not to exceed the maximum allowed number of users; 1.4. Respective checks to see if only licensed products and software are installed; 1.5. Adequately meeting the conditions of the license; 1.6. Use of appropriate tools for auditing.	1.1. poznavanje prava za kopiranje softuera, njihova kupovina i preduzimanje diciplinskih mera protiv onih individa koji ne poštuju isto; 1.2. očuvanje dokaza o vlasništvu licencoja; 1.3. Sprovodjenje kriterijuma o staranju da ne prevazidje dozvoljeni maksimalni broj korisnika; 1.4.dotična Kontrola koja utvrdjuje da li su instalirani ili su samo produkti i të licencirani softueri; 1.5. Dopuna adekuatnih uslova licencije; 1.6. Korišćenje dotičnih alata za reviziju.
Neni 45 **Rishqyrtimet e politikës së sigurisë**	**Article 45** **Reviews of security policy**	**Član 45** **Ponovno razmatranje bezbednosne politike**
1. Siguria e sistemeve informative duhet të rishqyrtohet rregullisht. 2. Rishqyrtimet e tilla duhet të kryhen kundrejt politikave përkatëse të sigurisë dhe platformave teknike, ndërsa sistemet informative duhet të kontrollohen për të parë nëse janë në përputhje me standardet	1. Security of information systems should be reviewed regularly. 2. Such reviews should be conducted against the relevant security policies and technical platforms, while information systems should be checked to see if they are in compliance with applicable safety	1. Bezbednost sistema informacija treba redovno da se ponovo razmatra. 2. Ponovno razmatranje treba da se obavljaju u skladu sa dotičnim politikama bezbednosti i tekničke platforme, zatim informativni sistem treba da se kontroliše da se vidi da li su u skladu sa

për zbatim të sigurisë.	standards.	standardima za sprovodjenje bezbednosti.
Neni 46 **Kontrollimi i harmonizimit teknik**	**Article 46** **Control of technical harmonization**	**Član 46** **Kontrola teknikčkog uskladjivanja**
1. Sistemet informative duhet rregullisht të kontrollohen për të parë nëse janë në përputhje me standardet për implementim të sigurisë.	1. Information systems should be checked regularly to see if they are in compliance with security implementation standards.	1. informativnom sistemu treba redovna kontrola da bih videli da li se uskladjuju standardima implementiranja bezbednosti.
2. Kontrolli mbi harmonizimin teknik kryhet nga persona kompetent të autorizuar apo të mbikëqyret nga ata.	2. The control on technical harmonization shall be carried out by competent authorized persons or shall be supervised by them.	2. Kontrola o tekničkom uskladjivanju obavljaju kompetena lica ili se nadgleda od njih.
Neni 47 **Revizioni i sistemit**	**Article 47** **System Audit**	**Ćlan 47** **Revizija sistema**
Revizioni i sistemit duhet të planifikohen për të minimizuar rrezikun e çrregullimit në procesin e punës.	The system audit should be planned in order to minimize the risk of disruption in the work process.	Revizija sistema treba da se plandra da bih minimizirali rizik nereda u procesu rada.
Neni 48 **Hyrja në fuqi**	**Article 48** **Enforcement**	**Član 48** **Stupanje na snagu**
Ky Udhëzim Administrativ hynë në fuqi ditë e nënshkrimit.	This Administrative Instruction shall enter into force on the day is signed.	Ovo Administrativno upustvo nastupa na snagu, dana potpisivanja.

Edita Tahiri, Ministre Ministria e Administratës Publike, Prishtinë, më 26. 05. 2010.	Edita Tahiri, Minister Ministry of Public Administration, Prishtina, on 26-05. 2010.	Edita Tahiri, Ministarka Ministarstvo Javne Uprave, Priština, dana 26. 05. 2010