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

PROJEKTLIGJI PËR SIGURINË KIBERNETIKE[1]

DRAFT LAW ON CYBER SECURITY[2]

NACRT ZAKONA O KIBERNETIČKOJ BEZBEDNOSTI[3]

[1] Projektligji per Sigurine Kibernetike eshte aprovuar ne mbledhjen e 96 te Qeverise se Kosoves, me Vendimin Nr. 07/96, date 14.09.2022
[2] Draft Law on Cyber Security was approved on the 96 meeting of the Government of Kosovo, with the Decision No. 07/96, date 14.09.2022
[3] Nacrt Zakona o Kibernetickoj Bezbednosti, usvojen je na 96 sednicu Vlade Kosova, sa Odlukom Br. 07/96, datum 14.09.2022

Kuvendi i Republikës së Kosovës, Në pajtim me nenin 65 (1) të Kushtetutës së Republikës së Kosovës, Miraton: **LIGJ PËR SIGURINË KIBERNETIKE** **KAPITULLI I** **DISPOZITAT E PËRGJITHSHME** **Neni 1** **Qëllimi** 1. Ky ligj përcakton parimet e sigurisë kibernetike, institucionet që zhvillojnë dhe zbatojnë politikën e sigurisë kibernetike, përgjegjësitë e autoriteteve në fushën e sigurisë kibernetike, detyrat e subjekteve të sigurisë kibernetike, bashkëpunimin ndërinstitucional, parandalimin e sulmeve kibernetike në Republikën e Kosovës, si dhe themelon Agjencinë për Siguri Kibernetike. 2. Ky ligj transpozon pjesërisht Direktivën (BE) 2013/40 të Parlamentit Evropian dhe Këshillit të datës 12 gusht 2013 për Sulmet kundër Sistemeve të Informacionit, që zëvendëson Vendimin Kornizë të Këshillit 2005/222/JHA, si dhe	Assembly of the Republic of Kosovo, Pursuant to Article 65 (1) of the Constitution of the Republic of Kosovo, Adopts: **LAW ON CYBER SECURITY** **CHAPTER I** **GENERAL PROVISIONS** **Article 1** **Purpose** 1. This law establishes the principles of cyber security, the institutions that develop and implement cyber security policy, the responsibilities of the authorities in the field of cyber security, the duties of cyber security entities, inter-institutional cooperation, the prevention and combating of cybercrime in the Republic of Kosovo against any threat or attack and establishes the Cyber Security Agency. 2. This law partially transposes Directive (EU) 2013/40 of the European Parliament and of the Council of 12 August 2013 on attacks against information systems replacing Council Framework Decision 2005/222 / JHA as well as Directive (EU)	Skupština Republike Kosovo, U skladu sa članom 65 (1) Ustava Republike Kosovo, Usvaja: **ZAKON O SAJBER BEZBEDNOSTI** **POGLAVLJE I** **OPŠTE ODREDBE** **Član 1** **Cilj** 1. Ovim zakonom se utvrđuju principi sajber bezbednosti, institucije koje razvijaju i sprovode politiku sajber bezbednosti, odgovornosti organa u oblasti sajber bezbednosti, dužnosti subjekata za sajber bezbednost, međuinstitucionalna saradnja, sprečavanje i suzbijanje sajber napada u Republici Kosovo, i takođe se osnuje Agencija za sajber bezbednost. 2. Ovim zakonom se delimično transponuje Direktiva (EU) 2013/40 Evropskog parlamenta i Saveta od 12. avgusta 2013. o napadima na informacione sisteme, koja zamenjuje Okvirnu odluku Saveta 2005/222/JHA, kao i Direktivu (EU)

Direktivën (BE) 2016/1148 të Parlamentit Evropian dhe Këshillit të datës 6 korrik 2016 për Masat e Sigurisë së Sistemeve të Rrjetit dhe Informacionit.	2016/1148 of the European Parliament and of the Council of 6 July 2016 on security measures for network and information systems.	2016/1148 Evropskog parlamenta i Saveta od 6. jula 2016. o merama bezbednosti mreža i informacionih sistema.
Neni 2 **Fushëveprimi**	**Article 2** **Scope**	**Član 2** **Delokrug**
Ky ligj rregullon standardet dhe kriteret minimale për mirëmbajtjen e sistemeve të rrjetit dhe informacionit të domosdoshme për funksionimin e shoqërisë, sistemeve të rrjetit dhe informacionit, përgjegjësitë dhe mbikëqyrjen, si dhe bazat për parandalimin, trajtimin dhe zgjidhjen e incidenteve kibernetike.	This Law regulates minimum standards and criteria for the maintenance of network systems and information essentialfor the functioning of society, network and information systems of state authorities, responsibilities and supervision, and the bases for the prevention, handling and resolution of cyber-incidents.	Ovim zakonom se uređuju minimalni standardi i kriterijumi za održavanje mrežnih i informacionih sistema neophodnih za funkcionisanje društva, mrežnih i informacionih sistema, odgovornosti i nadzor, kao i osnove za sprečavanje i postupanje sa sajber incidentima.
Neni 3 **Përkufizimet**	**Article 3** **Definitions**	**Član 3** **Definicije**
1. Shprehjet, termet dhe shkurtesat e përdorura në këtë ligj kanë këto kuptime:	1. The terms and abreviations used in this law shall have the following meaning:	1. Izrazi korišćeni u ovom zakonu imaju sledeća značenje:
1.1. **kibernetika -** nënkupton aktivitete që ndërlidhen me përfshirjen e kompjuterëve ose rrjeteve kompjuterike, siç është interneti;	1.1. **cybernetics -** means activities related to involvement of computers or computer networks, such as internet;	1.1. **kibernetika -** podrazumeva povezane aktivnosti sa uključivanjem računara i računarskih mera, kao što je internet;
1.2. **hapësirë kibernetike -** nënkupton mjedisi kompleks që rezulton nga ndërveprimi i njerëzve, softuerëve dhe shërbimeve në internet me anë të pajisjeve teknologjike dhe rrjeteve të	1.2. **cyberspace -** means the complex environment that results from interaction of people, software and services on the Internet through technological devices and networks connected to it, which does	1.2. **sajber prostor –** podrazumeva je složeno okruženje koje proizilazi iz interakcije ljudi, softvera i usluga na internetu, pomoću tehnološke opreme i mreža koje su povezane sa njim, koje ne

lidhura me të, i cili nuk ekziston në ndonjë formë fizike;	not exist in any physical form**;**	postoji u na bilo kom fizičkom obliku;
1.3. **siguria kibernetike -** nënkupton aktivitetet e nevojshme për të mbrojtur sistemet e rrjetit dhe informacionit, përdoruesit e këtyre sistemeve dhe personave të tjerë të prekur nga incidenti kibernetik;	1.3. **cyber Security** - means necessary activities to protect network and information systems, users of such systems and other persons affected by a cyber incident;	1.3. **sajber bezbednost** - podrazumeva neophodne aktivnosti za zaštitu mrežnih i informacionih sistema, korisnika ovih sistema i drugih lica pogođenih sajber incidentom;
1.4. **sistem kompjuterik -** nënkupton një pajisje apo grup pajisjesh të ndërlidhura, një ose më shumë prej të cilave, në bazë të një programi, kryejnë përpunim automatik të të dhënave;	1.4. **computer system** - means a device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data;	1.4. **kompjuterski sistem -** podrazumeva uređaj ili grupu međusobno povezanih uređaja, od kojih jedan ili više, na osnovu programa, obavljaju automatsku obradu podataka;
1.5. **incident kibernetik -** nënkupton çdo ngjarje që ka efekt negativ real në sigurinë e sistemeve të rrjetit dhe informacionit;	1.5. **cyber incident -** means any event that has a real adverse effect on the security of network and information systems;	1.5. **sajber incident -** podrazumeva svaki događaj koji ima stvarni negativni uticaj na bezbednost mrežnih i informacionih sistema;
1.6. **trajtimi i incidentit kibernetik -** nënkupton të gjitha procedurat që mbështesin zbulimin, analizën dhe mbajtjen nën kontroll të incidentit kibernetik dhe reagimin ndaj tij;	1.6. **cyber incident handling** - means all procedures supporting the detection, analysis and containment of an incident and the response thereto;	1.6. **tretman sajber incidenata -** podrazumeva sve postupke koji podržavaju otkrivanje, analizu i držanje pod kontrolom sajber incidenta i reagovanje na njega;
1.7. **sistem informacioni -** nënkupton një pajisje ose grup pajisjesh të ndërlidhura, ku një ose më shumë prej tyre në bazë të një programi, përpunojnë në mënyrë automatike të	1.7. **information system** - means a device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data, or digital data	1.7. **informacioni sistem -** podrazumeva bilo koju vrstu uređaja ili sklop međusobno povezanih ili sličnih uređaja, od kojih jedan ili više njih na osnovu programa, vrše automatsku obradu

dhëna kompjuterike, po ashtu të dhëna kompjuterike të ruajtura, përpunuara, të marra ose transmetuara nga ajo pajisje ose grup i pajisjeve për qëllime të operimit, përdorimit, mbrojtjes dhe mirëmbajtjes së tyre;	stored, processed, retrieved or transmitted by aforesaid device or group of devices for the purposes of their operation, use, protection and maintenance;	računarskih podataka, kao i računarske podatke koje taj uređaj ili grupa uređaja čuva, obrađuje, prima ili prenosi u cilju njihovog rada, korišćenja, zaštite i održavanja;
1.8. **të dhëna kompjuterike -** nënkupton një paraqitje të fakteve, informatave ose koncepteve në një formë të përshtatshme për përpunim në një sistem informacioni, përfshirë një program të përshtatshëm i cili mundëson që një sistem informacioni të kryejë një funksion. Të dhënat kompjuterike përfshijnë por nuk kufizohen në dokumente të shkruara, fotografi, audio dhe video materiale, programet softuerike dhe materialet tjera që ruhen në formë digjitale;	1.8. **computer data** - means the presentation of facts, information or concepts in a form suitable for processing in an information system, including a suitable program that causes an information system to perform a function. Computer data includes, but is not limited to written documents, pictures, audio and video materials, software programs and other digitally stored materials;	1.8. **računarski podaci -** podrazumevaju predstavljanje činjenica, informacija ili koncepata u obliku pogodnom za obradu u informacionom sistemu, uključujući odgovarajući program koji omogućava da informacioni sistem obavlja funkciju. Računarski podaci uključuju, ali nisu ograničeni na, pisane dokumente, fotografije, audio i video materijale, softverske programe i drugi materijal koji se čuva i digitalnom obliku;
1.9. **trafiku i të dhënave -** nënkupton çdo lloj të dhënash kompjuterike që janë pjesë e një komunikimi nëpërmjet një sistemi kompjuterik, të prodhuara nga një sistem kompjuterik që formojnë një pjesë në zinxhirin e komunikimit, që tregojnë origjinën e komunikimit, destinacionin, rrugën, kohën, datën, madhësinë, kohëzgjatjen, apo llojin e shërbimit përkatës;	1.9. **data traffic -** means any kind of computer data, related to communication through a computer system, produced by a computer system representing a part of the communication chain, indicating the origin of the communication, destination, route, time, date, size, duration, or the type of service concerned;	1.9. **podaci o saobraćaju -** podrazumevaju bilo koje računarske podatke koji su deo komunikacije putem računarskog sistema, proizvedeni od računarskog sistema, koji predstavljaju deo komunikacionog lanca, naznačujući poreklo komunikacije, odredište, rutu, vreme, datum, veličinu, vreme, ili vrstu dotične usluge;
1.10. **rrjeti i komunikimeve**	1.10. **electronic communications**	1.10. **mreža elektronskih komunikacija**

elektronike - nënkupton sistemin e transmetimit dhe nëse ekzistojnë, pajisjet e komutimit ose rutinimit dhe resurset tjera, duke përfshirë elementet e rrjetit që nuk janë aktive, të cilat lejojnë përcjelljen e sinjaleve nëpërmjet përcjellësve, radios, mjeteve optike ose mjeteve të tjera elektromagnetike, duke përfshirë rrjetet satelitore, rrjetet fikse (me komutim të qarqeve ose me komutim të paketave, përfshirë internetin), rrjetet mobile tokësore, sistemet e kabllove elektrike në raste kur ato përdoren për transmetimin e sinjaleve, rrjetet e përdorura për transmetimet radiotelevizive dhe të televizionit kabllor, pavarësisht nga tipi i informacionit të bartur;	**network -** means the transmission system and, if any, switching or routing equipment and other resources, including non-active network elements, which allow the transmission of signals through conductors, radio, optical or other electromagnetic means, including networks satellite, fixed networks (circuit switching or packet switching, including Internet), mobile terrestrial networks, electrical cable systems where they are used for signal transmission, networks used for radio and television broadcasting, regardless of type of information transmitted;	**-** podrazumeva sistem prenosa i, ako postoje, uređaji za komutaciju ili rutiniranje, i druge resurse, uključujući neaktivne mrežne elemente, koji omogućavaju praćenje signala putem provodnika, radija, optičkih ili drugih elektromagnetnih sredstava, uključujući satelitske mreže, fiksne mreže (komutacijom kola ili komutacijom paketa, uključujući internet), mobilne zemaljske mreže, električni kablovski sistemi u slučajevima kada se oni koriste za prenos signala, mreže koje se koriste za radio i televizijsko emitovanje, bez obzira na vrstu prenesenih informacija;
1.11**. sistemi i rrjetit dhe informacionit -** nënkupton:	1.11**. network and information system -** means:	1.11**. mrežni i informacioni sistem -** podrazumeva:
1.11.1. një rrjet komunikimi elektronik, siç definohet në paragrafin 1.10 të këtij neni;	1.11.1. an electronic communication network, as defined in paragraph 1.10 of this article;	1.11.1. elektronsku komunikacionu mrežu, kao što je definisano u stavu 1.10 ovog člana;
1.11.2. çdo sistem informacioni, siç definohet në paragrafin 1.7 të këtij neni;	1.11.2. any information system as defined in paragraph 1.7 of this article;	1.11.2. svaki informacioni sistem (kao što je definisano u stavu 1.7 ovog člana;
1.11.3. të dhënat digjitale të ruajtura, përpunuara, pranuara ose transmetuara nga elementet e	1.11.3. digital data stored, processed, received or transmitted from the elements covered in pragaraph	1.11.3. digitalni podaci koji se čuvaju, obrađuju, primaju ili prenose iz elemenata obuhvaćenim tačkama

mbuluara në pragrafin 1.11.1. dhe 1.11.2. të këtij neni për qëllimet e operimit, përdorimit, mbrojtjes dhe mirëmbajtjes së tyre;	1.11.1. and 1.11.2. of this article for the purpose of their operation, use, protection and maintenance;	1.11.1. i 1.11.2. u cilju njihovog rada, korišćenja, zaštite i održavanja;
1.12. **siguria e sistemeve të rrjetit dhe informacionit -** nënkupton aftësinë e sistemeve të rrjetit dhe informacionit për të rezistuar, në një nivel të caktuar besueshmërie, çdo veprimi që komprometon disponueshmërinë, origjinalitetin, integritetin ose konfidencialitetin e të dhënave të ruajtura ose të transmetuara ose të përpunuara ose shërbimet përkatëse të ofruara nga, apo të qasshme nëpërmjet këtyre sistemeve të rrjetit dhe informacionit;	1.12. **network and information systems security -** means the ability of network and information systems to withstand, at a certain level of reliability, any action that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted, processed data or related services provided by, or accessible through, these network and information systems;	1.12. **bezbednost mrežnih i informacionih sistema -** podrazumeva sposobnost mrežnih i informacionih sistema da se odupru, do određenog stepena pouzdanosti, bilo kojoj radnji koja kompromituje raspoloživost, originalnost, integritet ili poverljivost podataka koji se čuvaju, prenose ili obrađuju; ili relevantne usluge koje pruža, ili čine dostupnim ovi mrežni i informacioni sistemi;
1.13. **operatori i shërbimeve esenciale -** nënkupton një subjekt publik ose privat i cili posedon infrastrukturë kritike kombëtare sipas Ligjit përkatës për Infrastrukturën Kritike;	1.13. **operator of essential services** – means a public or private entity that possesses national critical infrastructure according to the law on critical infrastructure;	1.13. **operater osnovnih usluga -** javni ili privatni subjekt koji poseduje nacionalnu kritičnu infrastrukturu u skladu prema relevantnom Zakonu o kritičnoj infrastrukturi;
1.14. **ofruesi i shërbimit digjital -** nënkupton personin juridik me seli kryesore ose me një degë, të regjistruar në Republikën e Kosovës, i cili ofron shërbime digjitale;	1.14. **digital service provider -** means a legal person with a base or branch registered in the Republic of Kosovo, which provides digital services;	1.14. **provajder digitalnih usluga -** podrazumeva pravno lice sa glavnim sedištem ili jednim ogrankom registrovanim u Republici Kosovo, koji pruža digitalne usluge;
1.15. **shërbimet digjitale -**	1.15. **digital services -** means a set of	1.15. **digitalne usluge -**podrazumevaju

nënkuptojnë një grup shërbimesh të bazuara në teknologji të informacionit dhe komunikimeve ku përfshin: shërbimet e tregut online, kërkimit në internet dhe shërbimet e cloud-computing;	information and communication technology-based services including, online marketplace, Internet search and cloud computing services;	grupu usluga zasnovanih na informacione i komunikacione tehnologije, koje uključuje usluge internet tržišta, internet pretraživanje i cloud-computing usluge;
1.16. **treg online** - nënkupton një shërbim digjital që i mundëson konsumatorëve dhe tregtarëve, siç përcaktohen në pikën (a) dhe në pikën (b) të nenit 4 (1) të Direktivës 2013/11/BE të Parlamentit Evropian dhe të Këshillit (18) apo direktivave pasuese, të shesin në internet ose të lidhin kontrata të shërbimit në ueb-faqen e tregut online ose në ueb-faqen e një tregtari që përdor shërbime kompjuterike të ofruara nga tregu online;	1.16. **online markerplace** - means a digital service enabling consumers and traders, as defined in item (a) and item (b) of Article 4 (1) of Directive 2013/11 / EU of the European Parliament and of the Council (18), to conclude online sales or service contracts either on the online marketplace's website or on the website of a trader using computer services provided by the online marketplace;	1.16. **internet tržište** - podrazumeva digitalnu usluga koja omogućava potrošačima i/ili trgovcima kao što je definisano u tački (a) i u tački (b) člana 4 (1) Direktive 2013/11/EU Evropskog Parlamenta i Saveta (18) ili u sledećim direktivama, da prodaju na internetu ili sklapaju ugovore o usluzi sa trgovcima na internet stranici internet tržišta ili na internet stranici trgovca koji koristi računarske usluge koje pruža onlajn tržište;
1.17. **motor kërkimi në internet** - nënkupton një shërbim digjital që i mundëson përdoruesve të kryejnë kërkime, në parim, në të gjitha ueb-faqet, ose në të gjitha ueb-faqet në një gjuhë të caktuar, në bazë të një kërkese për çfarëdo teme në formën e një fjale, fraze ose të dhëne tjetër, dhe kthen linqe në të cilat mund të gjenden informatat lidhur me përmbajtjen e kërkuar;	1.17. **online search engine** - means a digital service that enables users to perform searches, in principle, on all websites, or on all websites in a particular language, on basis of a query for any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found;	1.17. **internet pretraživač** - podrazumeva digitalnu uslugu koja omogućava korisnicima izvrše pretragu, u principu, na svim internet stranicama, ili na svim internet stranicama na određenom jeziku, na osnovu bilo kog zahteva za bilo koju temu u obliku reči, fraze ili drugih podatak, vraća veze na kojima se mogu pronaći informacije o traženom sadržaju;
1.18. **shërbimi i cloud computing** -	1.18. **cloud computing service** - means	1.18. **cloud computing usluga** -

nënkupton një shërbim digjital që mundëson qasje në një pako të shkallëzuar dhe elastike të burimeve/resurseve kompjuterike të shpërndara. Burimet kompjuterike përfshijnë burime të tilla si rrjetet, serverët ose infrastruktura tjetër, hapësira ruajtëse, aplikacionet dhe shërbimet;	a digital service that enables access to a scalable and elastic pool of distributed computing resources. Computer resources include resources such are networks, servers or other infrastructure, storage spaces, applications and services;	podrazumeva digitalnu uslugu koja omogućava pristup skalabilnom i elastičnom paketu za deljenje internet izvora/resursa. Računarski resursi uključuju resurse kao što su mreže, serveri ili druga infrastruktura, prostor za skladištenje, aplikacije i usluge;
1.19. **i shkallëzuar** - i referohet burimeve kompjuterike që shpërndahen në mënyrë fleksibile nga ofruesi i shërbimit cloud, pavarësisht nga vendndodhja gjeografike e burimeve, në mënyrë që të trajtojë luhatjet e kërkesës;	1.19 **scalable** - refers to computer resources that are flexibly distributed by the cloud service provider, regardless from the geographical location of the resources, in order to handle demand fluctuations;	1.19. **skalabilan** - se odnosi na internet resurse koje fleksibilno deli provajder cloud usluge, bez obzira na geografsku lokaciju izvora, kako bi se nosili sa fluktuacijama potražnje;
1.20. **elastike** - përdoret për të përshkruar ato burime kompjuterike që sigurohen dhe lëshohen sipas kërkesës në mënyrë që të rriten dhe zvogëlohen me shpejtësi burimet e disponueshme në dispozicion;	1.20. **elastic** - is used to describe those computer resources that are provided and released on demand in order to rapidly increase and decrease the available resources;	1.20. **elastičan** - koristi se da opiše one internet resurse koji se obezbeđuju i puštaju na zahtev, u cilju brzog povećanja i smanjenja raspoloživih resursa;
1.21. **regjistri** – nënkupton regjistrin e incidenteve kibernetike;	1.21. **registry** – means the Cyber Incident Registry;	1.21. **registar** - podrazumeva Registar sajber incidenata;
1.22. **ASK** – nënkupton Agjencinë për Siguri Kibernetike;	1.22. **CSA** - means the Cyber Security Agency;	1.22. **ASB** – podrazumeva Agenciju za sajber bezbednost;
1.23. **CERT kombëtar** – nënkupton Ekipi i Republikës së Kosovës për	1.23. **national CERT** – means the team of the Republic of Kosovo for response	1.23. **nacionalni CERT** – podrazumeva Tim Republike Kosovo za reagovanje u

reagim ndaj emergjencave kompjuterike në nivel kombëtar;	to computer emergencies at the national level;	računarskim vanrednim situacijama na nacionalnom nivou;
1.24. **CSIRT-at sektorial kombëtar**– nënkupton ekipet për reagim ndaj incidenteve të sigurisë kompjuterike ose të sigurisë kibernetike që prekin një sektor specifik në nivel kombëtar. CSIRT-at sektorial kombëtar mund të themelohen në sektorë të tillë siç janë: shëndetësia, energjia, transporti, etj.;	1.24. **national sectoral CSIRTs** - means cyber security or cyber security incident response teams that affect a specific sector at the national level. National sectoral CSIRTs may be established in sectors such are Health, Energy, Transport, etc;	1.24. **nacionalni sektorski CSIRT-ovi** – podrazumevaju timove za reagovanje na incidente računarske bezbednosti ili sajber bezbednosti, koji pogađaju određeni sektor na nacionalnom nivou. Nacionalni sektorski CSIRT-ovi se mogu osnovati u sektorima kao što su zdravstvo, energija, transport itd;
1.25. **CSIRT-at e OShE** - nënkupton ekipet për reagim ndaj incidenteve të sigurisë kompjuterike ose të sigurisë kibernetike që prekin një operator të shërbimeve esenciale;	1.25. **CSIRTs of OES-** means teams for responding to computer security or cyber security incidents affecting an operator of essential services;	1.25. **CSIRT-ovi OOU-a** – podrazumeva timove za reagovanje na incidente računarske bezbednosti ili sajber bezbednosti, koji pogađaju jednog operatera osnovnih usluga;
1.26. **CSIRT-at e OShD** - nënkupton ekipet për reagim ndaj incidenteve të sigurisë kompjuterike ose të sigurisë kibernetike që prekin një ofrues të shërbimeve digjitale;	1.26. **CSIRTs of DSP** - means computer security or cyber security incident response teams affecting a digital service provider;	1.26. **CSIRT-ovi PDU-a** – podrazumeva timove za reagovanje na incidente računarske bezbednosti ili sajber bezbednosti, koji pogađaju jednog provajdera digitalnih usluga;
1.27. **KSHSK** – nënkupton Këshilli Shtetëror për Siguri Kibernetike;	1.27. **NCSC** – means The National Cyber Security Council;	1.27. **DSSB** - podrazumeva Državni savet za sajber bezbednost;
1.28. **MPB –** nënkupton Ministrinë e Punëve të Brendshme;	1.28. **MIA –** means Ministry of Internal Affairs;	1.28. **MUP –** podrazumeva Ministarstvo unutrašnjih poslova;
1.29. **MM** – nënkupton Ministrinë e Mbrojtjes;	1.29. **MD** - means Ministry of Defence;	1.29. **MO** - podrazumeva Ministarstvo Odbrane;
1.30. **FSK –** nënkupton Forcën e	1.30. **KSF** – means Kosovo Security	1.30. **KBS** – podrazumeva Kosovske

Sigurisë së Kosovës. **Neni 4** **Parimet e garantimit të Sigurisë Kibernetike** 1. Parimet e mëposhtme do të merren parasysh në garantimin e sigurisë kibernetike: 1.1. Parimi i personalitetit – që nënkupton se garantimi i sigurisë së një sistemi do të organizohet nga ofruesi i shërbimit; 1.2. Parimi i mbrojtjes integrale - që nënkupton se ofruesi i shërbimit do të konstatojë rreziqet e mundshme që paraqiten në sistem të rrjetit dhe informacionit dhe do të zbatojë masat e duhura organizative dhe teknike për mbrojtjen e sistemit të rrjetit dhe informacionit; 1.3. Parimi i minimizimit të efektit negativ - që nënkupton se në rastin e incidentit kibernetik, ofruesi i shërbimeve duhet të zbatojë kujdesin e duhur dhe masat për të shmangur përshkallëzimin e efektit të incidentit kibernetik dhe përhapjen e saj të mundshme në një sistem tjetër, dhe njofton autoritetin mbikëqyrës të	Force. **Article 4** **Principles of Guaranteeing Cyber Security** 1. The following principles shall be taken into account in ensuring cyber security: 1.1. The principle of personality – which means that ensuring the security of a system will be arranged by the service provider; 1.2. The principle of integral protection - which means that the service provider will ascertain the potential risks posed to the system and apply appropriate organizational and technical measures for protection of the network and information system; 1.3. The principle of minimizing the adverse effect - which means that in the case of a cyberincident, the service provider shall implement due care and measures to avoid the escalation of the effect of the cyber incident and its possible spread to another system, and notify the supervisory authority provided under this cyber incident law;	Bezbednosti Snage. **Član 4** **Principi garantovanja sajber bezbednosti** 1. Sledeći principi će se uzeti u obzir u garantovanju sajber bezbednosti: 1.1. Princip ličnosti – što znači da će garantovanje bezbednosti sistema organizovati pružalac usluge;; 1.2. Princip integrisanezaštite – što znači da provajder usluga će utvrditi moguće rizike koji nastaju u mrežni i informacioni sistem i primeniće odgovarajuće organizacione i tehničke mere za zaštitu mrežnog i informacionog sistema; 1.3. Princip minimiziranja negativnog efekta - što znači da u slučaju sajber incidenta, provajder usluga mora primeniti dužan oprez i mere kako bi izbegao eskalaciju efekta sajber incidenta i njegovo moguće širenje na drugi sistem, i obaveštava nadzorno telo predviđeno u skladu sa ovim zakonom o sajber incidentu;

paraparë sipas këtij ligji për incidentin kibernetik;		
1.4. Parimi i bashkëpunimit - që nënkupton se në garantimin e sigurisë kibernetike dhe zgjidhjen e incidentit kibernetik, palët do të bashkëpunojnë dhe nëse është e nevojshme, të marrin parasysh lidhjen e ndërsjellë dhe varësinë e sistemeve dhe shërbimeve.	1.4. The principle of cooperation - which means that in ensuring cyber security and resolving cyber incidents, the parties will cooperate and, if necessary, take into mutual connection between and dependence of the systems and services.	1.4. Princip saradnje - što znači da u obezbeđivanju sajber bezbednosti i rešavanje sajber incidenata, strane će sarađivati i, ako je potrebno, uzeti u obzir uzajamno povezivanje i zavisnosti sistema i usluga.
KAPITULLI II **OBLIGIMET PËR GARANTIMIN E SIGURISË KIBERNETIKE**	**CHAPTER II** **OBLIGATIONS FOR ENSURING CYBER SECURITY**	**POGLAVLJE II** **OBAVEZE ZA GARANTOVANJE SAJBER BEZBEDNOSTI**
Neni 5 **Masat e sigurisë së sistemit të operatorëve të shërbimeve esenciale**	**Article 5** **Security measures of the operator of essential services' system**	**Član 5** **Bezbednosne mere za sistem operatera osnovnih usluga**
1. Operatori i shërbimeve esenciale në mënyrë të përhershme duhet të zbatojë masa të sigurisë organizative, fizike dhe të teknologjisë së informacionit për:	1. The operator of essential services shall permanently apply organizational, physical and information technology security measures for:	1. Operater osnovnih usluga mora trajno primeniti fizičke i bezbednosne mere informacionih tehnologija za:
1.1. parandalimin e incidentit kibernetik;	1.1. preventing cyber incidents;	1.1. za sprečavanje sajber incidenta;
1.2. zgjidhjen e incidentit kibernetik;	1.2. resolving cyber incidents;	1.2. rešavanje sajber incidenta;
1.3. parandalimin dhe zbutjen e ndikimit në vazhdimësinë e shërbimit ose sigurinë e sistemit për shkak të	1.3. preventing and mitigating an impact on the continuity of the service or the security of the system due to a cyber	1.3. sprečavanje i ublažavanje uticaja na kontinuiteta usluge ili bezbednosti sistema zbog sajber incidenta ili za

incidentit kibernetik ose për parandalimin dhe zbutjen e një ndikimi të mundshëm mbi vazhdimësinë e një shërbimi tjetër të varur ose sigurisë së një sistemi.	incident or for preventing and mitigating a possible impact on the continuity of another dependent service or the security of a system.	sprečavanje i ublažavanje potencijalnog uticaja na kontinuitet druge zavisne usluge ili bezbednosti sistema.
2. Me zbatimin e masave të sigurisë, operatori i shërbimeve esenciale duhet të:	2. Upon the implementation of security measures, the operator of essential services is required to:	2. Primenom bezbednosnih mera, operater osnovnih usluga treba:
2.1. përgatis një vlerësim të rrezikut të sistemit që duhet të:	2.1. prepare a system risk assessment that should:	2.1. pripremiti procenu rizika sistema koja treba da:
2.1.1 përmbaj një listë të rreziqeve të cilat ndikojnë në sigurinë e sistemit dhe vazhdimësinë e shërbimit dhe që mund të shkaktojnë paraqitjen e incidenteve kibernetike;	2.1.1 set out a list of risks affecting security of the system and continuity of the service and causing the occurrence of cyberincidents,	2.1.1 sadrži listu sa rizicima koji utiču na bezbednost sistema i kontinuitet usluge, a koji mogu prouzrokovati pojavu sajber incidenta,
2.1.2 përcaktoj ashpërsinë e pasojave të një incidenti kibernetik nëse jetësohen rreziqet, në bazë të parametrave në vijim:	2.1.2 determine the severity of consquences of a cyberincident occurring upon the realization of risks, based on the following parameters:	2.1.2 odrediti nivo štete prouzrokovane sajber incidentom ako se pojave rizici, na osnovu sledećih parametara*:*
2.1.2.1 numri i përdoruesve të prekur nga ndërprerja e shërbimit esencial;	2.1.2.1 the number of users affected by the interruption of essential services;	2.1.2.1 broj pogođenih korisnika prekidom osnovnih usluga;
2.1.2.2 kohëzgjatja e incidentit kibernetik;	2.1.2.2 duration of the incident;	2.1.2.2 trajanje sajber incidenta;
2.1.2.3 shtrirjen gjeografike në lidhje me zonën e prekur nga	2.1.2.3 geographical extent in relation to the area affected by the incident.	2.1.2.3 geografska rasprostranjenost u odnosu na područje koje je pogođeno

incidenti kibernetik.		incidentom.
2.2. përshkruaj masat për zgjidhjen e incidentit kibernetik;	2.2. describe the measures for resolving a cyber incident;	2.2. opisuje mere za rešavanje sajber incidenta;
2.3. të garantoj ekzistimin e dokumentimit të vlerësimit të rrezikut të sistemit, rregulloreve të sigurisë dhe përshkrimit të masave të sigurisë që duhet të zbatohen në kohen e duhur;	2.3. ensure the existence and timeliness of a documented system risk assessment, security regulations and description of the application of security measures;	2.3. garantuje postojanje i dokumentovanje blagovremene procene rizika sistema, uredbi o bezbednosti i opisa bezbednosnih mera koje treba primeniti;
2.4. të garantoj monitorimin e sistemit për zbulimin e veprimeve ose softuerit që komprometon sigurinë e tij, dhe përcjell informacionet për veprimet ose softuerin që komprometon sigurinë e sistemit tek ASK;	2.4. ensure the monitoring of the system for detecting actions or software compromising its security and communicate information about the actions or software compromising the security of the system to the CSA;	2.4. garantuje nadgledanje sistema za otkrivanje radnji ili softvera koji ugrožavaju njegovu bezbednost, i prosleđuje obaveštenje sa informacijama o radnjama ili softveru koji kompromituje bezbednost sistema, kod ASB-a:
2.5. ndërmerr masa për reduktimin e ndikimit dhe përhapjes së një incidenti kibernetik, duke përfshirë kufizimin e përdorimit ose qasjen në sistem, nëse është e domosdoshme;	2.5. take measures for reducing the impact and spread of a cyber incident, including restriction of the use of or access to the system, if neccessary;	2.5. preduzme mere za smanjenje uticaja i širenja sajber incidenta, uključujući ograničavanje pristupa ili pristup sistemu, po potrebi;
2.6. kontrollon mjaftueshmërinë, efektshmërinë dhe pajtueshmërinë e zbatimit të masave të sigurisë dhe dokumenton rezultatet;	2.6. check the sufficiency, effectiveness and compliance of the application of security measures and document the results;	2.6. proverava efikasnost i usaglašenost primene bezbednosnih mera i dokumentuje rezultate;
2.7. ruajnë dokumentet e parashikuara në nënparagrafin 2.6 të	2.7. retain the documents envisaged in the paragraph 2.6 of this Article for at	2.7. čuva dokumente predviđene tačkom 2.3 ovog člana, najmanje tri

këtij neni, së paku tri vite nga krijimi i tyre.	least three years from their creation.	godine nakon njihovog stvaranja.
3. Nëse operatori i shërbimeve esenciale autorizon një palë tjetër për të administruar sistemin ose përdor një palë tjetër për të hostuar sistemin, operatori i shërbimeve esenciale është përgjegjës për zbatimin e masave të sigurisë të sistemit nga pala tjetër.	3. If the operator of essential services authorizes another party to administer the system or uses another party to host the system, the operator of essential services shall be responsible for the application of the security measures of the system by the other party.	3. Ako operater osnovnih usluga ovlasti drugu stranu da upravlja sistemom ili koristi drugu stranku za hostiranje sistema, operater osnovnih usluga je odgovoran za primenu bezbednosnih mera za sistem od druge strane.
4. Operatori i shërbimeve esenciale e ka për obligim themelimin e CSIRT të OShE apo së paku caktimin e një zyrtari i cili do të jetë përgjegjës për sigurinë e sistemeve të rrjetit dhe informacionit.	4. The essential service operator is obliged to establish the CSIRT of OES or at least to appoint an official who will be in charge for network and information systems and security.	4. Operater osnovnih usluga ima obavezu da osnuje CSIRT OOU-a ili najmanje da imenuje službenika koji će biti odgovoran za bezbednost informacionih sistema i mreže.
5. Operatori i shërbimeve esenciale mund të jetë pjesë e CSIRT sektorial kombëtar, por kjo nuk e liron nga obligimi i përcaktuar në paragrafin 4 të këtij neni.	5. The operator of essential services may be part of the national sectoral CSIRT, but this does not release it from the obligation set out in the paragraph 4 of this Article.	5. Operater osnovnih usluga može biti deo nacionalnog sektorskog CSIRT-a, ali ga to ne oslobađa obaveze iz stava 4. ovog člana.
6. Përshkrimi i masave të sigurisë për sistemin e rrjetit dhe informacionit, të përdorur për ofrimin e një shërbimi esencial dhe kërkesat për përgatitjen e vlerësimit të rrezikut, përcaktohen me akt nënligjor të miratuar nga Ministri i ministrisë përgjegjëse për punë të brendshme.	6. The description of the security measures for the network and information system, used for the provision of an essential service and requirements for the preparation of the risk assessment, shall be determined by a bylaw approved by the Minister of the Ministry responsible for internal affairs.	6. Opis bezbednosnih mera za mrežni i informacioni sistem, koji se koristi za pružanje osnovnih usluga i uslovi za pripremu procene rizika, utvrđuju se podzakonskim aktom koji daje ministar Ministarstva nadležnog za unutrašnje poslove.
7. Mos zbatimi i paragrafëve 1 deri 4 të këtij neni nga operatorët e shërbimeve	7. Failure by the operators of essential services to comply with paragraphs 1 to 4 of	7. Nesprovođenje stavova od 1. do 4. ovog člana od strane operatera osnovnih usluga,

esenciale, përbën vepër të kundërvajtjes. 8. Procedurat dhe masat reaguese në rastin e incidentit kibernetik përcaktohen me akt nënligjor të miratuar nga Ministri i ministrisë përgjegjëse për punë të brendshme.	this Article, constitutes a misdemeanour. 8. The procedures and response measures in case of a cyber incident, are determined by a bylaw approved by the Minister of the Ministry responsible for internal affairs.	predstavlja prekršajno delo. 8. U slučaju sajber incidenta, procedure i mere reagovanja utvrđuju se podzakonskim aktom koji daje ministar Ministarstva nadležnog za unutrašnje poslove.
Neni 6 **Detyrimi i operatorit të shërbimeve esenciale për të njoftuar për incidentin kibernetik**	**Article 6** **Obligation of the operator of essential service to report a cyber incident**	**Član 6** **Obaveza operatera osnovnih usluga da prijavi sajber incident**
1. Operatori i shërbimeve esenciale duhet të informojë ASK-në menjëherë, por jo më vonë se njëzetë e katër (24) orë pasi që të jetë vënë në dijeni të incidentit kibernetik: 1.1. i cili ka një ndikim të konsiderueshëm në sigurinë e sistemit ose vazhdimësinë e shërbimit; 1.2. ndikimi i konsiderueshëm i të cilit për sigurinë e sistemit apo vazhdimësinë e shërbimit nuk është i qartë por mund të supozohet në mënyrë të arsyeshme. 2. Një incident kibernetik ka një ndikim të konsiderueshëm nëse plotësohet të paktën një nga kushtet e mëposhtme:	1. An operator of essential services shall inform the CSA immediately, but not later than 24 hours after becoming aware of a cyber incident: 1.1. which has a significant impact on the security of the system or the continuity of the service; 1.2. a significant impact of which on the security of the system or the continuity of the service is not obvious but can be reasonably presumed. 2. A cyber incident has a significant impact if at least one of the following conditions is met:	1. Operator osnovnih usluga treba da odmah obavesti ASB, ali najkasnije u roku od 24 sata nakon što je upoznat sa sajber incidentom: 1.1. koji ima značajan uticaj na bezbednost sistema ili kontinuitet usluga; 1.2. čiji značajan uticaj na bezbednost sistema ili kontinuitet usluga nije jasan, ali se može razumno pretpostaviti. 2. Sajber incident ima značajan uticaj ako se ispuni najmanje jedan od sledećih uslova:

2.1. ndikimi i incidentit kibernetik është së paku i nivelit të lartë sipas shkallës së pasojave të përcaktuara në vlerësimin e rrezikut të sistemit të përgatitur në bazë të nenit 5, paragrafin 2 të këtij ligji;	2.1. tthe impact of the cyber incident is at least high according to the degree of consequences determined in the system risk assessment prepared on the basis of Article 5, paragraph 2 of this Law;	2.1. uticaj sajber incidenta je najmanje visokog nivoa u odnosu na stepen posledica utvrđenih procenom rizika sistema pripremljenom u skladu sa članom 5. stav 2. ovog zakona;
2.2. për shkak të incidentit kibernetik, ofrimi i shërbimit nuk mund të vazhdohet pas kalimit të kohës maksimale të lejuar të ndërprerjes së shërbimit, të paraparë në marrëveshjen përkatëse të nivelit të shërbimit ose kërkesat për vazhdimësinë e shërbimit;	2.2. due to a cyber-incident, the provision of the service cannot be continued after the passing of the maximum permitted time of disruption of the service provided by the relevant service level agreement or requirements for thr continuity of the service;	2.2. zbog sajber incidenta, pružanje usluge se ne može nastaviti nakon prolaska maksimalnog vremena dozvoljenog za prekid usluge, koji je predviđen relevantnim ugovorom o nivou usluge ili zahtevima za kontinuitet usluge;
2.3. vazhdimësia e shërbimit të ofruesit të një shërbimi tjetër është ndërprerë për shkak të incidentit kibernetik;	2.3. the continuity of the service of the provider of another service is disrupted due to the cyber incident;	2.3. kontinuitet pružanja drugih usluga od strane provajdera je prekinut zbog sajber incidenta;
2.4. masat e jashtëzakonshme të përcaktuara në vlerësimin e rrezikut të sistemit të përgatitur sipas nenit 5, paragrafin 2 të këtij ligji, ose ndonjë dokument tjetër, të cilat përshkruajnë rivendosjen e vazhdimësisë së shërbimit ose sigurisë së sistemit duhet të aplikohen për zgjidhjen e incidentit kibernetik;	2.4. extraordinary measures set out in the system risk assessment prepared under Article 5 paragraph 2 of this Law or in any other document, if any, which desscribing the restoration of the continuity of the service or the security of the system need to be applied for resolving the cyber incident;	2.4. vanredne mere utvrđene u proceni rizika za sistem pripremljene u skladu sa članom 5. stav 2. ovog zakona, ili u bilo kojem drugom dokumentu, koji opisuju ponovno uspostavljanje kontinuiteta usluge ili bezbednosnih mera koje treba primeniti za rešavanje sajber incidenta;
2.5. ofruesi i shërbimit, ofruesi i një shërbimi tjetër ose përdoruesit e	2.5. the service provider, the provider of another service, or service users	2.5. provajder usluga, provajder drugih usluga ili korisnik usluga trpi ili može

shërbimeve pësojnë ose mund të pësojnë dëme të konsiderueshme për shkak të incidentit kibernetik.	suffer or may suffer significant damage due to the cyber-incident.	pretrpeti značajnu štetu zbog sajber incidenta.
3. Obligimi i përcaktuar në paragrafin 1 të këtij neni nuk e kufizon të drejtën e operatorit të shërbimeve esenciale për të njoftuar ASK-në për një incident kibernetik që nuk ka një ndikim të konsiderueshëm siç është definuar në paragrafin 2 të këtij neni.	3. The obligation set forth in paragraph 1 of this Article shall not limit the right of the operators of essential services to notify the CSA of a cyber-incident that does not have a significant impact as defined in paragraph 2 of this Article.	3. Obaveza utvrđena u stavu 1 ovog člana ne ograničava pravo operatora osnovnih usluga da obavesti ASB o sajber incidentu koji nema značajan uticaj kao što je utvrđeno u tački 2ovog člana.
4. Brenda një periudhe të arsyeshme kohore, operatori i shërbimeve esenciale është i detyruar të njoftojë personat potencialisht të prekur nga incidenti kibernetik me një ndikim të konsiderueshëm, ose publikun, kur personat e prekur nuk mund të njoftohen individualisht.	4. Within a reasonable period of time, the operator of essential service is obliged to notify persons possibly affected by the cyber-incident with a significant impact, or the public, if the persons affected persons cannot be notified individually.	4. U razumnom vremenskom periodu, operater osnovnih usluga je dužan da obavesti lica potencijalno pogođenim sajber incidentom sa značajnim uticajem, ili javnost, kad pogođene strane ne mogu biti pojedinačno obavešteni.
5. Në bazë të informacionit të dhënë në njoftimin nga ana e operatorit të shërbimeve esenciale, ASK do të informojë të gjithë operatorët e shërbimeve esenciale të prekur, nëse incidenti kibernetik ka një ndikim të rëndësishëm në vazhdimësinë e shërbimeve esenciale. ASK, në përputhje me legjislacionin në fuqi, ruajnë interesat e sigurisë dhe interesat komerciale të operatorit të shërbimeve esenciale, si dhe konfidencialitetin e informacionit të dhënë	5. Based on the information provided in the notification by the operator of essential services, the CSA shall inform all affected operators of essential services if the incident has a significant impact on the continuity of the essential services. The CSA, in accordance with the legislation in force, safeguards the security and commercial interests of the operator of essential services, as well as the confidentiality of the information provided in the notification.	5. Na osnovu informacija dobijenih u obaveštenju od strane operatera osnovnih usluga, ASB će obavestiti sve pogođene operatere osnovnih usluga, ako sajber incident ima značajan uticaj na kontinuitet osnovnih usluga. ASB, u skladu sa važećim zakonodavstvom, štiti bezbednosne i komercijalne interese operatera osnovnih usluga, kao i poverljivost informacija navedenih u obaveštenju.

në njoftim.		
6. Nëse operatori i shërbimit esencial nuk kryen detyrimin e njoftimit të përcaktuar në paragrafin 4 të këtij neni brenda një periudhe të arsyeshme kohore, ASK mund të njoftojë personin e prekur apo vetë publikun, duke njoftuar gjithashtu operatorin e shërbimit esencial për njoftimin e tillë.	6. If the operator of essential services fails to comply with the notification obligation provided for in paragraph 4 of this Article within a reasonable period of time, the CSA may notify the person affected or the public itself, also informing the operator of essential services of such notification.	6. Ako operater osnovnih usluga ne ispuni obavezu obaveštavanja iz stava 4. ovog člana u razumnom vremenskom roku, ASB bezbednost može da obavesti pogođenu osobu ili samu javnost, takođe obaveštavajući operatera osnovnih usluga o takvom obaveštenju.
7. Për zgjidhjen e një incidenti kibernetik me ndikim të konsiderueshëm, operatori i shërbimit esencial duhet t'i dërgojë ASK-së raport i cili përfshin informacione për shkaqet e incidentit kibernetik, kohën e kaluar në zgjidhjen e tij, masat e zbatuara dhe ndikimin e incidentit kibernetik.	7. In resolving a cyber incident with significant impact, the operator of essential services is required to submit to the CSA a report which includes information on the causes of the cyber incident, the time spent in its resolution, the measures applied and the impact of the cyber incident.	7. Za rešavanje sajber incidenta sa značajnim uticajem, operater osnovnih usluga mora poslati ASB-u izveštaj koji sadrži informacije o uzrocima sajber incidenta, vreme provedeno za njegovo rešenje, primenjene mere i uticaj sajber incidenta.
8. Operatori i shërbimeve esenciale duhet të ruajë të dhënat e përdoruesve në pajtim me legjislacionin në fuqi.	8. The Operator of Essential services must maintain user data in accordance with applicable legislation.	8. Operater osnovnih usluga trebaju čuvati korisničke podatke u skladu sa važećim zakonodavstvom.
9. Kur rrethanat lejojnë, ASK do t'i ofroj operatorit njoftues të shërbimeve esenciale, informacionin përkatës në lidhje me veprimet e ndërmarra pas njoftimit të tij, siç janë informacionet që mund të mbështesin trajtimin efektiv të incidenteve kibernetike.	9. When circumstances permit, the CSA shall provide the operator of essential services that has reported the incident with relevant information on the actions taken following its notification, such as information that may support effective incident handling.	9. Kada okolnosti to dozvoljavaju, ASB će osnovnom operateru izveštavanja o uslugama, pružiti relevantne informacije o preduzetim radnjama nakon obaveštavanja, kao što su informacije koje podržavaju efikasan tretman sajber incidenata.
10. Për të gjitha sistemet e informacionit, në të cilat qasja është e kufizuar ose	10. For all information systems, to which access is restricted or completely prohibited,	10. Za sve informacione sisteme, u kojima je pristup ograničen ili u potpunosti

plotësisht e ndaluar, operatorët e shërbimeve esenciale detyrohen ta rregullojnë që në mënyrë të qartë dhe automatike të paralajmërohet përdoruesi me informacion, si dhe në çfarë kushtesh mund ta përdorë, ose se është i ndaluar përdorimi i këtij sistemi informacioni dhe për pasojat ligjore për qasje të paautorizuar.	the operators of essential services are obliged to make sure that the user is clearly and automatically warned with information, as well as under what conditions the user can use the information system, or that the use of this information system is prohibited, and the legal consequences of the unauthorized access.	zabranjen, operatori osnovnih usluga dužni su da regulišu na taj način, da korisnik bude jasno i automatski upozoren informacijama, kao i o tome pod kojim uslovima može da ih koristi, odnosno da je korišćenje ovog informacionog sistema zabranjen, kao i o pravnim posledicama neovlašćenog pristupa.
11. Mos zbatimi i detyrimeve të përcaktuara në këtë nen nga operatori i shërbimeve esenciale, përbën vepër të kundërvajtjes.	11. Failure to comply with the obligations set out in this Article by the operator of essential services constitutes a misdemeanor.	11. Nesprovođenje obaveza utvrđenih ovim članom od strane operatera osnovnih usluga predstavlja prekršaj.
12. Procedura për njoftimin e incidentit kibernetik dhe formati i raportit do të përcaktohet me një akt nënligjor të miratuar nga Ministri i ministrisë përgjegjëse për punë të brendshme.	12. The procedure for notification of the cyber incident and the format of the report will be determined by bylaw approved by the Minister of the Ministry responsible for internal affairs.	12. Postupak za obaveštavanje o sajber incidentu i format izveštaja biće utvrđeni podzakonskim aktom koji daje ministar Ministarstva nadležnog za unutrašnje poslove.
Neni 7 **Masat e sigurisë për sistemin e ofruesit të shërbimeve digjitale**	**Article 7** **Security measures of digital service providers's system**	**Član 7** **Bezbednosne mere sistema za provajdere digitalnih usluga**
1. Ofruesi i shërbimeve digjitale kërkohet të konstatojë rreziqet që cenojnë sigurinë e sistemit të tyre, t'i analizojë ato dhe të marrë masa adekuate organizative dhe teknike për menaxhimin e rrezikut.	1. A digital service provider is required to identify the risks posed to the security of their system, analyse them, and take appropriate organizational and technical measures for risk management.	1. Od provajdera digitalnih usluga traži se da utvrdi rizike koji utiču na bezbednost njihovog sistema, da ih analizira ih i preduzima odgovarajuće organizacione i tehničke mere upravljanja rizikom.
2. Në përzgjedhjen e masave për	2. In choosing the measures for ensuring the	2. U izboru mera za garantovanje

garantimin e sigurisë së një sistemi duhet të merren parasysh:	security of a system the following shall be taken into account:	bezbednosti sistema treba uzeti u obzir:
2.1. siguria e infrastrukturës teknike;	2.1. the security of the technical infrastructure;	2.1. bezbednost tehničke infrastrukture;
2.2. parandalimi, zbulimi dhe zgjidhja e incidentit kibernetik;	2.2. the prevention, detection and resolution of a cyber incident;	2.2. sprečavanje, otkrivanje i rešavanje sajber incidenta;
2.3. menaxhimi i vazhdimësisë;	2.3. continuity management;	2.3. upravljanje kontinuitetom;
2.4. monitorimi, auditimi dhe testimi;	2.4. monitoring, auditing and testing;	2.4. praćenje, revizija i testiranje;
2.5. pajtueshmëria me standardet ndërkombëtare.	2.5. compliance with international standards.	2.5. usaglašenost sa međunarodnim standardima.
3. Ofruesi i shërbimeve digjitale duhet të marrë masat e duhura për të minimizuar ndikimin e incidentit kibernetik në vazhdimësinë e shërbimit të ofruar.	3. The digital service provider shall take appropriate measures to minimize the impact of a cyber incident on the continuity of the service provided.	3. Provajder digitalnih usluga mora preduzeti odgovarajuće mere da minimizira uticaj sajber incidenta na kontinuitet pružene usluge.
4. Ofruesi i shërbimeve digjitale e ka për obligim themelimin e CSIRT të OShD apo së paku caktimin e një zyrtari i cili do të jetë përgjegjës për sigurinë e sistemeve të rrjetit dhe informacionit.	4. The digital service provider has the obligation to establish the CSIRT of the DSP or at least to appoint an official who will be in-charge for the security of network and information systems.	4. Provajder digitalnih usluga ima obavezu da osnuje CSIRT PDS-a ili najmanje da imenuje službenika koji će biti odgovoran za bezbednost informacionih sistema i mreže.
5. Ofruesi i shërbimeve digjitale mund të jetë pjesë e CSIRT sektorial kombëtar, por kjo nuk e liron nga obligimi i përcaktuar në paragrafin 4 të këtij neni.	5. The digital service provider may be part of the national sectoral CSIRT, but this does not release it from the obligation set out in paragraph 4 of this Article.	5. Provajder digitalnih usluga može biti deo nacionalnog sektorskog CSIRT-a, ali ga to ne oslobađa obaveze utvrđene u stavu 4. ovog člana.
6. Mos zbatimi i paragrafëve 1 deri 4 të	6. Failure to comply with paragraphs 1 to 4	6. Nesprovođenje stava od 1. do 4. ovog

këtij neni nga ofruesit e shërbimeve digjitale, përbën vepër të kundërvajtjes.	of this Article by digital service providers constitutes a misdemeanor.	člana od strane provajdera digitalnih usluga predstavlja prekršaj.
Neni 8 **Detyrimi i ofruesit të shërbimeve digjitale për të njoftuar për incidentin kibernetik**	**Article 8** **Obligation of the digital service providers to report a cyber incident**	**Član 8** **Obaveza provajdera digitalnih usluga da prijavi sajber incident**
1. Ofruesi i shërbimeve digjitale duhet të njoftojë ASK–në për një incident kibernetik që ka një ndikim të konsiderueshëm në shërbimin digjital të ofruar, menjëherë pasi që të jetë në dijeni të incidentit kibernetik.	1. A digital service provider shall notify the CSA of a cyber incident that has a significant impact on the digital service provided, immediately after becoming aware of the cyber incident.	1. Provajder digitalnih usluga mora obavestiti ASB o sajber incidentu koji ima značajan uticaj na pruženu digitalnu uslugu, odmah nakon što saznaje za sajber incident.
2. Për të përcaktuar nëse ndikimi i një incidenti kibernetik është i konsiderueshëm, do të merren në konsideratë parametrat e mëposhtëm:	2. To determine whether the impact of an incident is significant, the following criteria shall be considered:	2. Da bi se utvrdilo da li je uticaj sajber incidenta značajan, uzeće se u obzir sledeći parametri:
2.1. numri i përdoruesve të prekur nga incidenti kibernetik, në veçanti përdoruesit që mbështeten në shërbimin, për ofrimin e shërbimeve të tyre;	2.1. the number of users affected by the incident, in particular users relying on the service for the provision of their services;	2.1. broj pogođenih korisnika sajber incidentom, posebno korisnici koji se oslanjaju na uslugu za pružanje svojih usluga;
2.2. kohëzgjatjen e incidentit kibernetik;	2.2. duration of the incident;	2.2. trajanja sajber incidenta;
2.3. shtrirjen gjeografike në lidhje me zonën e prekur nga incidenti kibernetik;	2.3. geographical spread in terms of the area affected by the incident;	2.3. geografska rasprostranjenost u odnosu na pogođeno područje sajber incidentom;

2.4. shtrirja e ndërprerjes së funksionimit të shërbimit;	2.4 the extent of the interruption the service;	2.4. rasprostranjenost prekida funkcionisanja usluge;
2.5. shtrirja e ndikimit në aktivitetet ekonomike dhe shoqërore.	2.5. the extent of the impact on economic and social activities.	2.5. rasprostranjenost uticaja na ekonomske i društvene aktivnosti.
3. Njoftimi duhet t'i dorëzohet autoritetit kompetent ose ekipit të reagimit të incidenteve të sigurisë kompjuterike - CERT të shtetit ku:	3. The notification shall be submitted to the competent authority or computer security incident response team - CERT of the State where:	3. Obaveštenje se mora dostaviti nadležnom organu ili timu za odgovor na incidente računarske bezbednosti - CERT države u kojoj je:
3.1. është themeluar ofruesi i shërbimit digjital;	3.1. the digital service operator has been established;	3.1. osnovan operater digitalne usluge;
3.2. kompania amë e grupit është e themeluar, në rastin e një grupi;	3.2. the parent company of the group is established in the case of a group;	3.2. matična kompanija grupe osnovana u slučaju grupe;
3.3. është vendosur përfaqësuesi i emëruar nga operatori ekonomik i vendit të tretë.	3.3. the representative appointed by an economic operator from a third country economic operator is located.	3.3. postavljen predstavnik koga je imenovao ekonomski operater treće zemlje.
4. Njoftimi duhet të përfshijë informacione që i mundësojnë autoritetit kompetent ose ekipit të reagimit të incidenteve të sigurisë kompjuterike - CERT që të përcaktojnë çdo ndikim ndërkufitar të incidentit kibernetik.	4. The notification shall include information enabling the competent authority or computer security incident response team - CERT to determine any cross-border impact of the cyber incident.	4. Obaveštenje uključuje informacije koje omogućavaju nadležnom organu ili timu za odgovor na incidente računarske bezbednosti - CERT da utvrde bilo kakav preko prekogranični uticaj sajber incidenta.
5. Nëse incidenti kibernetik ka ndikim të konsiderueshëm në vazhdimësinë e shërbimit digjital në një Shtet tjetër, ASK njofton Shtetin e prekur në bazë të	5. If a cyber incident has a significant impact on the continuity of a digital service in another State, the CSA shall notify the affected State on the basis of information	5. Ako sajber slučaj ima značajan uticaj na kontinuitet digitalne usluge u drugoj državi, ASB obavesti pogođenu državu na osnovu informacija dobijenih od strane provajdera

informacionit të paraqitur nga ofruesi i shërbimit digjital.	provided by the digital service provider.	digitalne usluge.
6. Nëse me qëllim të parandalimit të incidentit kibernetik ose zgjidhjes së incidentit kibernetik në zhvillim e sipër dhe në interes të publikut është e nevojshme të njoftohet publiku, ASK mund që pas njoftimit të ofruesit të shërbimit digjital të njoftoj publikun për incidentin kibernetik ose të kërkoj nga ofruesi i shërbimit digjital ta bëjë këtë.	6. If for the purpose of preventing a cyber incident or resolving an ongoing cyber incident and in the public interest, it is necessary to notify the public, the CSA may, after informing he digital service provider, notify the public of the cyber incident or request the digital service provider to do so.	6. Ako je u cilju sprečavanja sajber incidenta ili rešavanja sajber incidenta u toku, i u javnom interesu, potrebno da se informiše javnost, ASB može, nakon obaveštavanja provajdera digitalne usluge, da obavesti javnost o sajber incidentu ili da traži od provajdera digitalne usluge da to uradi.
7. Paragrafi 1 i këtij neni nuk zbatohet nëse ofruesi i shërbimit digjital nuk ka informacion për identifikimin e rëndësisë së ndikimit të incidentit kibernetik.	7. Paragraph 1 of this Article shall not apply if the digital service provider lacks information for identifying the significance of the impact of the cyber incident.	7. Stav 1 ovog člana se ne sprovodi ako provajder digitalne usluge nema informacije za identifikaciju značaja uticaja sajber incidenta.
8. Kur operatori i shërbimeve esenciale mbështetet në një ofrues të shërbimeve digjitale si palë e tretë për ofrimin e një shërbimi që është esencial për mirëmbajtjen e aktiviteteve kritike shoqërore dhe ekonomike, për çdo ndikim të rëndësishëm në vazhdimësinë e shërbimeve esenciale për shkak të një incidenti kibernetik që ndikon tek ofruesi i shërbimit digjital, do të njoftohet nga ky ofrues i shërbimit.	8. When an operator of essential service relies on a digital service operator as a third party to provide a service that is essential for the maintenance of critical social and economic activities, for any significant impact on the continuity of the essential services due to an incident affecting the digital service provider will be notified by this service provider.	8. Kada se operater osnovnih usluga oslanja na provajdera digitalnih usluga kao treća stranka da pruži uslugu koja je od suštinskog značaja za održavanje kritičnih društvenih i ekonomskih aktivnosti, za svakog značajan uticaj na kontinuitet osnovnih usluga zbog sajber incidenta koji utiče na provajdera digitalne usluge, biće prijavljeni od strane ovog operatera.
9. Për të gjitha sistemet e informacionit, në të cilat qasja është e kufizuar ose plotësisht e ndaluar, ofruesit e shërbimeve	9. For all information systems, to which access is restricted or completely restricted, the digital service providers are obliged to	9. Za sve informacione sisteme, u kojima je pristup ograničen ili u potpunosti zabranjen, provajderi digitalnih usluga dužni su da

digjitale, detyrohen ta rregullojnë që në mënyrë të qartë dhe automatike të paralajmërohet përdoruesi me informacion, si dhe në çfarë kushtesh mund ta përdorë, ose se është i ndaluar përdorimi i këtij sistemi informacioni dhe për pasojat ligjore për qasje të paautorizuar.	make sure that the user is clearly and automatically warned with information, as well as under what conditions the user can use the information system, or that the use of this information system is prohibited, and the legal consequences of the unauthorized access.	regulišu na taj način, da korisnik bude jasno i automatski upozoren informacijama, kao i o tome pod kojim uslovima može da ih koristi, odnosno da je korišćenje ovog informacionog sistema zabranjen, kao i o pravnim posledicama neovlašćenog pristupa.
10. Mos zbatimi i detyrimeve të përcaktuara në këtë nen nga ofruesi i shërbimeve digjitale, përbën vepër të kundërvajtjes.	10. Failure to comply with the obligations set out in this article by the digital service provider, constitutes a misdemeanor.	10. Nesprovođenje obaveza utvrđenih ovim članom od strane provajdera digitalnih usluga predstavlja prekršaj.
11. Njoftimi i incidentit kibernetik do të bazohet në kriteret e përcaktuara me me akt nënligjor të miratuar nga Ministri i ministrisë përgjegjëse për punë të brendshme.	11. The notification of a cyber-incident shall be based on the criteria provided for by a bylaw approved by the Minister of the Ministry responsible for internal affairs.	11. Obaveštavanje o sajber incidentu zasnivaće se na kriterijumima utvrđenim u podzakonskim aktom koji daje ministar Ministarstva nadležnog za unutrašnje poslove.
KAPITULLI III **GARANTIMI I SIGURISË KIBERNETIKE**	**CHARTER III** **ENSURING CYBER SECURITY**	**POTPOGLAVLJE III** **GARANTOVANJE SAJBER BEZBEDNOSTI**
Neni 9 **Parandalimi dhe zgjidhja e incidentit kibernetik**	**Article 9** **Prevention and resolution of a cyber incident**	**Član 9** **Sprečavanje i rešavanje sajber incidenta**
1. Grarantimi i sigurisë kibernetike dhe parandalimi dhe zgjidhja e një incidenti kibernetik në masën e parashikuar nga ky ligj, koordinohen nga ASK.	1. Ensuring cyber security, prevention and resolution of a cyber incident to the extent provided by this law shall be coordinated by the CSA.	1. Pružanje sajber bezbednosti, sprečavanje i rešavanje sajber incidenta u meri u kojoj je propisana ovim zakonom, koordinira ASB.

2. Me qëllim të garantimit të sigurisë kibernetike, ASK në koordinim me Ministrinë e Mbrojtjes, Autoritetin Rregullativ të Komunikimeve Elektronike dhe Postare dhe institucionet tjera të sigurisë, analizon rreziqet që cenojnë sigurinë e sistemeve dhe ndikimin e tyre në shtet, shoqëri dhe sigurinë e sistemeve.	2. For the purpose of ensuring cyber security, the CSA in coordination with the Ministry of Defence, the Regulatory Authority of Electronic and Postal Communications and other security institutions, analyses the risks posed to the security of systems and their impact on the state, society and security the of systems.	2. U cilju garantovanja sajber bezbednost, ASB, u koordinaciji sa Ministarstvom odbrane, Regulatornim autoritetom za elektronske i poštanske komunikacije i drugim bezbednosnim institucijama, analizira rizike koji ugrožavaju bezbednost sistema i njihov uticaj na državu, društvo i bezbednost informacionih sistema.
3. ASK do të krijojë dhe mirëmbajë një regjistër elektronik të rreziqeve të sigurisë kibernetike për vendin.	3. CSA will establish and maintain an electronic register of cyber security risks for the country.	3. ASB će uspostaviti i održavati elektronski registar rizika sajber bezbednosti za zemlju.
4. Me qëllim të parandalimit të incidenteve kibernetike, ASK në bashkëpunim me Qendrën Shtetërore Trajnuese për Siguri Kibernetike në MM\FSK, organizon ushtrime me operatorët e shërbimeve esenciale dhe ofruesit e shërbimeve digjitale.	4. For thr purpose of preventing and resolving a cyber-incident, the CSA in cooperation with the State Cyber Security Training Centre in MD\KSF organizes exercises with operators of essential service and digital service providers.,	4. U cilju sprečavanja sajber incidenata, ASB u saradnji sa Državnim centrom za obuku o sajber bezbednosti u MO\KSB organizuje vežbe sa operaterima osnovnih usluga i provajderima digitalnih usluga.
5.ASK dërgon alarme tek operatorët e shërbimeve esenciale dhe ofruesit e shërbimeve digjitale që u mundësojnë atyre të marrin masa për të shmangur ose zvogëluar ndikimin e incidentit.	5.CSA sends alerts to operators of essential service and digital service providers to enable them to take measures to avoid or reduce the impact of a cyber incident.	5.KAS šalje upozorenja operaterima osnovnih usluga i provajderima digitalnih usluga koje omogućavaju njima da preduzmu mere da izbegnu ili smanje uticaj incidenta.
6. ASK ka të drejtën që të shkëmbej informacione me një shtet tjetër ose me Agjencinë e Bashkimit Evropian për Sigurinë Kibernetike ose me një organizatë tjetër, me qëllim të parandalimit dhe zgjidhjen e një incidenti	6. CSA has the right to exchange information with a foreign state or with the European Union Cyber Security Agency or with another organization regarding the prevention and resolution of a cyber incident for the performance of the	6. ASB ima pravo na razmenu informacija sa drugom državom ili sa Agencijom Evropske unije za sajber bezbednost ili sa nekom drugom organizacijom, u cilju sprečavanja i rešavanja sajber incidenta za obavljanje funkcija utvrđenih ovim

kibernetik për kryerjen e funksioneve të përcaktuara në këtë ligj ose një detyrimi që rrjedh nga legjislacioni i Bashkimit Evropian ose në rastet sipas procedurës së përcaktuar në një marrëveshje ndërkombëtare, me kusht që informacioni i dërguar nuk dëmton sigurinë kombëtare apo procedurat penale.	functions set out in this Law or an obligation arising from European Union legislation or in cases as provided for in an international agreement, provided that the information exchanged does not harm national security or criminal proceedings.	zakonom ili obaveze prema zakonodavstvu Evropske unije, ili u slučajevima prema proceduri utvrđene međunarodnim sporazumom, pod uslovom da date informacije ne oštete nacionalnu bezbednost ili krivične postupke.
7. Me rastin e shkëmbimit të informacionit, ASK do të marrë parasysh interesat e biznesit të operatorit të shërbimeve esenciale ose ofruesit të shërbimeve digjitale dhe do të respektojë detyrimin për të ruajtur sekretet e biznesit.	7. When exchanging information, the CSA shall take into account the business interests of the operator of essential service or digital service provider and shall abide by the obligation to keep business secrets.	7. Prilikom razmene informacija, ASB će uzeti u obzir poslovne interese operatera osnovnih usluga ili provajdera digitalnih usluga i poštovaće obavezu da čuva poslovne tajne.
8. Në mënyrë që të sigurohen sistemet e informacionit dhe mbrojtja e të dhënave personale, ASK koordinon dhe bashkëpunon me institucionet publike me kompetenca në këtë fushë, me ofruesit e shërbimeve, organizatat joqeveritare dhe përfaqësuesit e shoqërisë civile, për zhvillimin e aktiviteteve dhe programeve për parandalimin e incidenteve kibernetike.	8. In order to ensure security of information systems and protection of personal data, CSA coordinates and cooperates with public institutions with competences in this field, with service providers, non-governmental organizations and civil society representatives to develop activities and programs for prevention of cyber incidents.	8. Da bi se osigurali informacioni sistemi i zaštita ličnih podataka, ASB koordinira i sarađuje sa javnim institucijama sa nadležnostima u ovoj oblasti, sa provajderima usluga, nevladinim organizacijama i predstavnicima civilnog društva u sprovođenju aktivnosti i programa za sprečavanje sajber incidenata.
9. Mënyra e regjistrimit të të dhënave dhe zbulimit të informacionit të përfshirë në këtë regjistër, do të përcaktohen me akt nënligjor të miratuar nga Ministri i ministrisë përgjegjëse për punë të brendshme.	9. The manner of data registration and disclosure of information included in this register will be provided in a bylaw approved by the Minister of the Ministry responsible for internal affairs.	9. Način evidencije podataka i otkrivanja informacija uključenih u ovaj registar, biće utvrđeni podzakonskim aktom koji daje ministar Ministarstva nadležnog za unutrašnje poslove.

Neni 10 **Regjistri i incidenteve kibernetike**	**Article 10** **Cyber incident Registry**	**Član 10** **Registar sajber incidenata**
1. Regjistri i incidenteve kibernetike është një bazë të dhënash që ruhet nga ASK, ku regjistrohen të dhënat për paraqitjen e incidentit me qëllim të mbajtjes së shënimeve të incidenteve kibernetike, analizimit të incidenteve kibernetike me qëllim zgjidhjen e tyre, dërgimin e njoftimeve alarmuese dhe kryerjen e operacioneve mbikëqyrëse.	1. The Cyber Incident Registry is a database maintained by the CSA, where data describing the occurrence of a cyber incident is entered for the purpose of keeping record of cyber incidents, analysing cyber incidents for resolving them, sending alerts and performing supervisory operations.	1. Registar sajber incidenata je baza podataka koja se čuva od strane ASB-a, gde se evidentiraju podaci o prijavljivanju incidenta u cilju vođenja evidencije o sajber incidentima, analizama sajber incidenata u cilju njihovog rešavanja, slanja upozoravajućih obaveštenja i sprovođenja nadzornih operacija.
2. Qasja në regjistër është e kufizuar dhe të dhënat e regjistrit janë të destinuara për përdorim të brendshëm, përveç nëse përcaktohet ndryshe me legjislacionin në fuqi.	2. Access to the registry is restricted and the registry data is intended for internal use, unless otherwise provided by applicable legislation.	2. Pristup registru je ograničen, a podaci registra namenjeni su za unutrašnju upotrebu, osim ako važećim zakonodavstvom nije drugačije određeno.
3. Përmbajtja e regjistrit përcaktohet me akt nënligjor të miratuar nga Ministri i ministrisë përgjegjëse për punë të brendshme.	3. The contents of the Registry shall be determined by a bylaw approved by the Minister of the Ministry responsible for internal affairs.	3. Sadržaj registra se utvrđuje posebnim podzakonskim aktom koji daje ministar Ministarstva nadležnog za unutrašnje poslove.
Neni 11 **Mbikëqyrja dhe monitorimi**	**Article 11** **Supervision and monitoring**	**Član 11** **Nadzor i praćenje**
1. Mbikëqyrja shtetërore dhe administrative mbi pajtueshmërinë me kërkesat e parashikuara në këtë ligj dhe në legjislacionin e përcaktuar në bazë të këtij ligji, ushtrohen nga ASK.	1. State and administrative supervision over the compliance with the requirements set forth in this law and in the legislation established on the basis of this law are exercised by the CSA.	1. Državni i upravni nadzor nad usaglašavanjem sa uslovima utvrđenih ovim zakonom i zakonodavstvom predviđanim ovim zakonom vršiće se od strane ASB-a.

2. Gjatë ushtrimit të mbikëqyrjes shtetërore, ASK, me qëllim të parandalimit të një kërcënimi të menjëhershëm serioz ose eliminimit të ndonjë çrregullimi në rast të një incidenti kibernetik mund të kufizoj ose ndërpres përkohësisht përdorimin ose qasjen në një rrjet apo sistem, me përjashtim të sistemeve ushtarake, me kusht që plotësohen të gjitha kriteret e mëposhtme:	2. Upon exercising state supervision, the CSA, for the purpose of preventing an imminent serious threat or the elimination of any disturbance in the event of a cyber incident, may temporarily restrict or discontinue the use or access to a network or system, with the exception of military systems, provided all of following conditions are met:	2. Vršenjem državnog nadzora, ASB, izuzev vojnih sistema, može da privremeno ograniči ili prekine korišćenje ili pristup mreži ili sistemu da spreči trenutnu ozbiljnu pretnju ili otkloni bilo kakve smetnje u slučaju sajber incidenta, pod uslovom da se ispunjavaju svi navedeni parametri u nastavku:
2.1. incidenti kibernetik komprometon ose dëmton sigurinë e një sistemi tjetër;	2.1. a cyber incident compromises or harms the security of another system;	2.1. sajber incident kompromituje ili narušava bezbednost drugog sistema;
2.2. administratori i sistemit nuk është në gjendje fare ose nuk është në gjendje në kohën e duhur për të reaguar ndaj kërcënimit serioz ose për të eliminuar çrregullimin që mund të vij si pasojë e incidentit kibernetik;	2.2. the system administrator is either unable or unable in a timely manner to respond to the serious threat or eliminate the consequences that resulting from a cyber incident;	2.2. administrator sistema nije uopšte u stanju ili nije u stanju u pravo vreme da odgovori na ozbiljnu pretnju ili da otkloni smetnje koje mogu nastati kao posledica sajber incidenta;
2.3. nuk është e mundur për t'iu përgjigjur kërcënimit serioz ose për të eliminuar çrregullimet që mund të vijnë nga incidenti kibernetik duke përdorur një masë më të lehtë reaguese;	2.3. it is not possible to respond to the serious threat or to eliminate the consequences that may come from a cyber-incident using a less infringing response measure;	2.3. nije moguće odgovoriti na ozbiljnu pretnju ili otkloniti smetnje koje mogu nastati od sajber incidenta korišćenjem blagih mera reagovanja;
2.4. si rezultat i reagimit nga ASK ndaj rrezikut serioz ose eliminimit të çrregullimit që rrjedh nga incidenti	2.4. a disproportional damage to a person is not caused by responding to the threat originating from the cyber	2.4. kao rezultat reagovanja ASB-a na ozbiljnu pretnju ili otklanjanje smetnje koje nastaje od sajber incidenta, licu nije

kibernetik, personit nuk i shkaktohet dëm disproporcional.	incidentor by eliminating the conseqeunces of the cyber incident.	prouzrokovana nesrazmerna šteta.
3. Procedura e marrjes së masave sipas paragrafit 2, dokumentimi i masave të ndërmarra dhe njoftimi ndaj subjektit të prekur, rregullohen me akt nënligjor të miratuar nga Ministri i ministrisë përgjegjëse për punë të brendshme.	3. The procedure for taking the measures referred to in paragraph 2, the documentation of the measures taken and the notification sent to the affected entity shall be regulated by a bylaw approved by the Minister of the Ministry responsible for internal affairs.	3. Postupak preduzimanja mera iz stava 2, dokumentovanje preduzetih mera i obaveštavanje pogođenog subjekta, uređuje se podzakonskim aktom koji daje ministar Ministarstva nadležnog za unutrašnje poslove.
Neni 12 **Trajnimet dhe programet e specializuara**	**Article 12** **Specialized trainings and programs**	**Član 12** **Specijalizovane obuke i programi**
Qendra Shtetërore Trajnuese për Siguri Kibernetike në Ministrinë e Mbrojtjes/Forca e Sigurisë së Kosovës, në bashkëpunim me ASK-në, përcakton procedurën dhe formatin e programeve të specializuara për trajnime dhe certifikime të personelit të angazhuar në fushën e sigurisë kibernetike në përputhje me kompetencat që ushtrojnë.	The State Cyber Security Training Centre at the Ministry of Defence / Kosovo Security Force, in cooperation with CSA, determines the procedure and format of specialized programs for training and certification of the personnel engaged in the field of cyber security in accordance with the competencies that they exercise.	Državni centar za obuke o sajber bezbednosti u Ministarstvu odbrane/Kosovske snage bezbednosti u saradnji sa ASB-om utvrđuje postupak i format specijalizovanih programa za obuke i sertifikaciju osoblja angažovanog u oblasti sajber bezbednosti u skladu sa nadležnostima koje imaju.

KAPITULLI IV INSTITUCIONET PËRGJEGJËSE PËR SIGURI KIBERNETIKE	CHAPTER IV INSTITUTIONS RESPONSIBLE FOR CYBER SECURITY	POGLAVLJE IV ODGOVORNE INSTITUCIJE ZA SAJBER BEZBEDNOST
Neni 13 **Themelimi dhe Statusi i Agjencisë për Siguri Kibernetike**	**Article 13** **Establishment and Status of the Cyber Security Agency**	**Član 13** **Osnivanje i status Agencije za sajber bezbednost**
1. Me këtë ligj themelohet Agjencia për Siguri Kibernetike.	1. This law establishes the Agency for Cyber Security.	1. Ovim zakonom se osniva Agencija za sajber bezbednost.
2. Agjencia ka statusin e Agjencisë Ekzekutive në pajtim me Ligjin përkatës për organizimin dhe funksionimin e administratës shtetërore dhe Agjencive të Pavarura.	2. The Agency has the status of an Executive Agency in accordance with the relevant Law on the organization and functioning of the state administration and Independent Agencies.	2. Agencija ima status izvršne agencije u skladu sa odgovarajućim Zakonom o organizaciji i funkcionisanju državne uprave i nezavisnih agencija.
3. Agjencia është pjesë e Ministrisë përgjegjëse për punë të brendshme.	3. The agency is part of the Ministry responsible for internal affairs	3. Agencija je u sastavu Ministarstva nadležnog za unutrašnje poslove
4. ASK është person juridik me seli qendrore në Prishtinë.	4. CSA is a legal entity based in Prishtina.	4. ASB je pravno lice sa sedištem u Prištini.
5. Brenda Agjencisë për Siguri Kibernetike do të funksionalizohet CERT Kombëtar.	5. National CERT will be operational within the Cyber Security Agency.	5. U okviru Agencije za sajber bezbednost biće funkcionalizovan Nacionalni CERT.
Neni 14 **Simbolet e ASK-së**	**Article 14** **Symbols of the CSA**	**Član 14** **Simboli ASB-a**
ASK e ka stemën e cila propozohet nga Drejtori Ekzekutiv dhe miratohet nga	CSA has the coat of arms which is proposed by the Executive Director and approved by	ASB ima grb koji predlaže izvršni direktor i usvaja ministar MUP-a.

Ministri i MPB-së.	the Minister of MIA.	
Neni 15 **Drejtimi dhe mbikëqyrja e ASK-së**	**Article 15** **Management and Supervision of the CSA**	**Član 15** **Upravljanje i nadzor ASB-a**
1. ASK udhëhiqet nga Drejtori Ekzekutiv i cili është përgjegjës për administrimin, funksionimin dhe menaxhimin e Agjencisë.	1. CSA is lead by the Executive Director, who is who is responsible for the administration, funcioning and management of the Agency.	1. ASB vodi Izvršni direktor, koji je odgovoran za administraciju, funkcionisanje i upravljanje Agencijom.
2. Drejtori i agjencisë është nëpunës civil i kategorisë së lartë drejtuese, emërimi, shkarkimi, statusi, mandati dhe kohëzgjatja e mandatit, si dhe elementet tjera të marrëdhënies së punës i së cilit rregullohen me Ligjin përkatës për zyrtarët publikë.	2. The director of the agency is a civil servant of the senior management category, whose appointment, dismissal, status, mandate and duration of the mandate, as well as other elements of the employment relationship, are regulated by the relevant Law on public officials.	2. Direktor agencije je državni službenik kategorije višeg rukovodstva, čije imenovanje, razrešenje, status, mandat i trajanje mandata, kao i drugi elementi radnog odnosa, uređuju se odgovarajućim Zakonom o državnim funkcionerima.
3. Drejtori Ekzekutiv për performancën dhe veprimtarinë e ASK-së, i përgjigjet Ministrit të MPB-së si dhe e informon Sekretarin e Përgjithshëm të MPB-së.	3. The Executive Director for the performance and activity of CSA, answers to the Minister of MIA and informs the General Secretary of MIA.	3. Izvršni direktor za rad i rad ASB-a, odgovara ministru MUP-a i obaveštava generalnog sekretara MUP-a.
Neni 16 **Funksionet e Drejtorit Ekzekutiv të ASK-së**	**Article 16** **Functions of the Director General**	**Član 16** **Funkcije Generalnog direktora**
1. Drejtori Ekzekutiv i ASK-së është përgjegjës për:	1. The Executive Director of the CSA is responsible for:	1. Izvršni direktor ASB-a je odgovoran za:

1.1. menaxhimin dhe administrimin e përgjithshëm të ASK-së;	1.1. general management and administration of the CSA;	1.1. opšte rukovođenje i upravljanje ASB-om;
1.2. menaxhimin e burimeve njerëzore në pajtim me Ligjin për Zyrtarët Publik;	1.2. human resource management in accordance with the Law on Public Officials;	1.2. upravljanje ljudskim resursima u skladu sa zakonom o javnim službenicima;
1.3. menaxhimin efektiv dhe efikas të resurseve që i janë besuar ASK-së;	1.3. effective and efficient management of the resources entrusted to the CSA;	1.3. efektivno i efikasno upravljanje resursima koji su povereni ASB-u;
1.4. propozimin e planit dhe raportit vjetor të performancës të Agjencisë;	1.4. proposing the annual plan and performance report of the Agency;	1.4. . predlaganje godišnjeg plana i izveštaja o radu Agencije;
1.5. lidh marrëveshje bashkëpunimi nga fushëveprimtaria e ASK-së në përputhje me legjislacionin relevant në fuqi;	1.5. Reaches cooperation agreements within the scope of the CSA in accordance with the relevant legislation in force;	1.5. zaključivanje sporazuma o saradnji iz delokruga ASB-a u skladu sa relevantnim zakonodavstvom na snazi;
1.6. zhvillimin e planit vjetor dhe planit strategjik afatgjatë për administrimin efektiv dhe efikas të ASK-së;	1.6. developing the annual plan and long-term strategic plan for the effective and efficient administration of the CSA.	1.6. sprovođenje godišnjeg i dugoročnog strateškog plana za efektivno i efikasno upravljanje ASB-om.
1.7. çdo përgjegjësi tjetër që i caktohet me legjislacion tjetër.	1.7. any other responsibilities assigned to it by other legislation.	1.7. sve druge odgovornosti koje su mu dodeljene drugim zakonodavstvom.
2. Drejtori Ekzekutiv nxjerr vendime, më qëllim të ushtrimit të detyrave dhe përgjegjësive nga paragrafi 1 i këtij neni.	2. In order to exercise the duties and responsibilities under paragraph 1 of this article, the Executive Director shall issue decisions.	2. Izvršni direktor donosi odluke radi vršenja dužnosti i odgovornosti iz stava 1 ovog člana.

Neni 17 Detyrat dhe përgjegjësitë	Article 17 Duties and responsibilities	Član 17 Dužnosti i odgovornosti
1. ASK është institucion përgjegjës për propozim dhe zbatimin e masave për siguri kibernetike në Republikën e Kosovës.	1. CSA is the institution responsible for proposing and implementing cyber security measures in the Republic of Kosovo.	1. ASB je odgovorna institucija za predlaganje i sprovođenje mera sajber bezbednosti u Republici Kosovo.
2. ASK ka për detyrë të monitoroj, inspektoj dhe koordinoj aktivitetet e institucioneve përgjegjëse për siguri kibernetike në Republikën e Kosovës, si dhe të ndërmerr masa në rast të moszbatimit, në pajtim me këtë ligj.	2. CSA is responsible to monitor, inspect and coordinate the activities of the institutions responsible for cyber security in the Republic of Kosovo, as well as to take measures in case of non-implementation, pursuant to this Law.	2. ASB je dužna da prati, vrši inspekcijski nadzor i koordinira aktivnosti institucija odgovornih za sajber bezbednost u Republici Kosovo, kao i da preduzima mere u slučaju nesprovođenja, u skladu sa ovim zakonom.
3. ASK në bashkëpunim me Qendrën Shtetërore Trajnuese për Siguri Kiberentike ka për detyrë realizimin e testimeve dhe ushtrimeve të përbashkëta me operatorët e shërbimeve esenciale dhe ofruesit e shërbimeve digjitale, me qëllim evidentimin e cenueshmërisë.	3. In order to identify the vulnerabilities, CSA in cooperation with the State Training Centre for Cyber Security is obliged to conduct joint tests and exercises with operators of essential service and digital service providers.	3. ASB u saradnji sa Državnim centrom za obuke o sajber bezbednosti, dužna je da sprovodi zajedničko testiranje i vežbe sa operaterima osnovnih usluga i provajderima digitalnih usluga, u cilju evidentiranja ugroženosti.
4. ASK ka për detyrë reagimin ndaj kërcënimeve dhe incidenteve në hapësirën kibernetike të Republikës së Kosovës.	4. CSA is responsible for responding to threats and incidents in the cyber space of the Republic of Kosovo.	4. ASB je dužna da reaguje na pretnje i incidente u sajber prostoru Republike Kosovo.
5. ASK administron me regjistrin e incidenteve kibernetike dhe regjistrin e kërcënimeve kibernetike.	5. CSA administers the cyber incident register and the cyber threat register.	5. ASB upravlja registrom sajber incidenata i registrom sajber pretnji.
6. ASK bën hulumtime dhe analiza, si dhe nxjerr rekomandime për zbatim nga	6. CSA shall conduct research and analysis and issues recommendations for	6. ASB sprovodi istraživanja i analize, i takođe daje preporuke za sprovođenje

institucionet e tjera.	implementation by other institutions.	drugim institucijama.
7. ASK krijon platformë elektronike për shkëmbim të informatave në kohë reale. Shfrytëzues të kësaj platforme do të jenë operatorët e shërbimeve esenciale dhe ofruesit e shërbimeve digjitale.	7. CSA shall create an electronic platform for real-time information exchange. Users of this platform will be operators of essential services and digital service providers.	7. ASB uspostavlja elektronsku platformu za razmenu informacija u realnom vremenu. Korisnici ove platforme biće operateri osnovnih usluga i provajderi digitalnih usluga.
8. Bashkëpunon me autoritetet e shteteve të huaja dhe organizatat ndërkombëtare në lidhje me aspektet që janë nën përgjegjësinë e ASK-së.	8. CSA shall cooperate with the authorities of foreign countries and international organizations regarding the aspects that are under the responsibility of the CSA	8. Saradnja sa organima stranih država i međunarodnim organizacijama u vezi sa aspektima koji su u nadležnosti ASB-a.
9. ASK ka kompetencat dhe mjetet për të kërkuar nga operatorët e shërbimeve esenciale dhe ofruesit e shërbimeve digjitale që të ofrojnë:	9. CSA has the power and the means to require from the operator of essential services and digital service providers to provide:	9. ASB ima nadležnosti i sredstva da zahteva od operatora osnovnih usluga provajdera digitalnih usluga da obezbede:
9.1. informacionin e nevojshëm për të vlerësuar sigurinë e rrjetit të tyre dhe sistemeve të informacionit, duke përfshirë politikat e dokumentuara të sigurisë;	9.1. information needed to assess the security of their network and information systems, including documented security policies;	9.1. informacije potrebne za procenu bezbednosti njihovih mreža i informacionih sistema, uključujući i dokumentovane politike bezbednosti;
9.2. dëshmitë e zbatimit efektiv të politikave të sigurisë, të tilla si rezultatet e një auditimi të sigurisë të kryer nga institucionet kompetente, duke përfshirë dëshmitë themelore, të cilat duhet të jenë në dispozicion të ASK-së.	9.2. evidence of effective implementation of security policies, such as the results of a security audit conducted by the competent institutions, including basic evidence, which should be available to CSA.	9.2. dokaze o efikasnoj primeni bezbednosnih politika, kao što su rezultati revizije bezbednosti koju su izvršili nadležne institucije, uključujući osnovne dokaze, koji bi trebala da budu raspoloživi ASB-u.
10. Pas vlerësimit të informacionit ose	10. After evaluating the information or	10. Nakon procene informacija ili rezultata

rezultateve të auditimeve të sigurisë të referuara në paragrafin 9 të këtij neni, ASK mund të lëshojë udhëzime detyruese për operatorët e shërbimeve esenciale për të korrigjuar mangësitë e identifikuara.	results of the security audits referred to in paragraph 2, CSA may issue binding instructions to essential service providers to correct the deficiencies identified.	revizije bezbednosti iz stava 9.2 ovog člana, ASB može izdati obavezujuća uputstva operaterima osnovnih usluga da isprave identifikovane nedostatke.
11. ASK bashkëpunon ngushtë me Agjencinë Shtetërore për Mbrojtjen e të Dhënave Personale kur adreson incidente që rezultojnë në shkelje të të dhënave personale.	11. CSA shall closely cooperate with the state agency for the protection of personal data when addressing incidents resulting in personal data breaches.	11. ASB blisko sarađuje s državnom agencijom za zaštitu ličnih podataka prilikom rešavanja incidenata koji rezultiraju povredom ličnih podataka.
12. ASK koordinon aktivitetet e saj me institucionet e sigurisë dhe mbrojtjes, bashkëpunon me CSIRT-at sektorial kombëtar, CSIRT-at e OShE, CSIRT-at e OShD, zyrtarët e sigurisë së informacionit të caktuar dhe autoritetet ndërkombëtare.	12. CSA shall coordinate its activities with security and defence institutions and cooperates with sectorial CERTs of ESO, CSIRTs of DSP, certain information security officers and international authorities.	12. ASB koordinira svoje aktivnosti sa institucijama za bezbednost i odbranu, sarađuje sa nacionalnim sektorskim CSIRT-ovima OOU-a, CSIRT-ovima PDU-a, službenicima za bezbednost informacija i međunarodnim telima.
13. ASK bën certifikimin e sigurisë për pajisjet dhe shërbimet e teknologjisë së informacionit dhe komunikimeve, në rastet kur kërkohet nga institucionet publike. Ky certifikim i sigurisë nënkupton se pajisjet dhe shërbimet janë nga ofrues të besueshëm, dhe kryejnë vetëm funksionet e përcaktuara nga prodhuesi në karakteristikat e pajisjes, dhe jo ndonjë funksion shtesë të paligjshëm siç mund të jetë përgjimi, marrja e informatave, etj.	13. CSA carries out security certification for equipment and services of information and communication technology, in the cases when required by public institutions. This security certification means that equipment and services are from the reliable providers, and carry out only the functions specified by the manufacturer in the specifications of the equipment, and not any additional unlawful function such as interception, obtaining information, etc.	13. ASB vrši sertifikaciju bezbednosti za uređaje i usluge informacione i komunikacione tehnologije, u slučajevima kada to zahtevaju javne institucije. Ova sertifikacija bezbednosti podrazumeva da su uređaji i usluge od proverenih provajdera, i da obavljaju samo funkcije koje je proizvođač naveo u specifikacijama opreme, a ne bilo kakve dodatne nezakonite funkcije kao što su prisluškivanje, dobijanje informacija itd.
14. Rregullat dhe procedurat për procesin	14. Rules and procedures for the	14. Pravila i procedure za proces

e certifikimit do të definohen me akt nënligjor të miratuar nga Ministri i ministrisë përgjegjëse për punë të brendshme.	certification process shall be defined by a sub-legal act approved by the Minister of MIA.	sertifikacije biće utvrđene podzakonskim aktom usvojenim od strane ministra MUP-a.
15. Qeveria e Republikës së Kosovës me propozim të Ministrit të Ministrisë përgjegjëse për punë të brendshme me akt nënligjor, miraton rregullat dhe masat e sigurisë së qasjes së fëmijëve në internet, të cilin do të obligohen ta zbatojnë të gjithë ofruesit e shërbimeve të internetit në Republikën e Kosovës. Gjatë hartimit të aktit nënligjor MPB bashkëpunon me ASK-në dhe Autoritetin Rregullativ të Komunikimeve Elektronike dhe Postare.	15.The Government of the Republic of Kosovo, on the proposal of the Minister of the Ministry responsible for internal affairs, by a by-law, approves the rules and safety measures for children's access to the Internet, which all Internet service providers in the Republic of Kosovo will be obliged to implement. Kosovo. During the drafting of the by-law, the Ministry of Internal Affairs cooperates with CSA and the Regulatory Authority of Electronic and Postal Communications.	15.Vlada Republike Kosovo, na predlog ministra nadležnog za unutrašnje poslove, podzakonskim aktom, usvaja pravila i mere bezbednosti za pristup dece Internetu, koje svi provajderi Internet usluga u Republici Kosovo će biti u obavezi da sprovede. Kosovo. Prilikom izrade podzakonskog akta, Ministarstvo unutrašnjih poslova sarađuje sa ASB-om i Regulatornim organom za elektronske i poštanske komunikacije.
16. ASK do të krijoj platformë komunikuese me qytetarë dhe biznese që do të jetë në shërbim 24/7 për raportim të incidenteve kibernetike.	16. CSA will create a communication platform 24/7 with citizens and businesses, for reporting of cyber incidents.	16. ASB će kreirati komunikacionu platformu sa građanima i preduzećima koja će biti dostupna 24/7 za prijavljivanje sajber incidenata.
Neni 18 **Organizimi i brendshëm dhe personeli**	**Article 18** **Internal Organization and Personnel**	**Član 18** **Unutrašnja organizacija i osoblje**
1. Personeli i ASK-së përbëhet nga nëpunësit civil dhe nëpunësit administrativ dhe mbështetës dhe marrëdhënia e tyre e punës rregullohet legjislacionin në fuqi për zyrtarët publikë.	1. CSA staff shall be composed of civil servants and administrative and support staff, in accordance with applicable Law on Public Officials.	1. Osoblje ASB se sastoji od državnih službenika i administrativnog i pomoćnog osoblja u skladu sa važećim zakonom o javnim službenicima
2. Struktura dhe organizimi i brendshëm i	2. Structure and internal in CSA shall be	2. Strukturu i unutrašnje u ASB, vrši se

ASK-së bëhet me akt nën ligjor, i cili miratohet në pajtim me ligjin në fuqi për Organizimin dhe Funksionimin e Administratës Shtetërore dhe të Agjencive të Pavarura.	done by a bylaw act approved in accordance with the applicable Law on the Organization and Functioning of State Administration and Independent Agencies.	propisom, koji se usvaja u skladu sa važećim zakonom o organizaciji i funkcionisanju državne administracije i samostalnih organa.
Neni 19 **Pagat, shpërblimet dhe kompensimet**	**Article 19** **Salaries, Bonuses and Remunerations**	**Član 19** **Plate, bonusi i naknade**
Pagat, shpërblimet dhe kompensimet për personelin e ASK-së, rregullohen me ligjin përkatës për Pagat në Sektorin Publik.	Salaries, bonuses and remunerations for CSA staff shall be regulated by the relevant Law on Salaries in the Public Sector.	Plate, bonusi i naknade za osoblje ASB-a regulisani su važećim zakonom o platama u javnom sektoru.
Neni 20 **Buxheti i ASK-së**	**Article 20** **Budget of CSA**	**Član 20** **Budžet ASB-a**
1. Buxheti i ASK-së është vijë buxhetore në kuadër të buxhetit të MPB-së, të miratuar në pajtim me Ligjin përkatës për Menaxhimin e Financave Publike dhe Përgjegjësitë.	1. CSA budget is a budget line within the budget of MIA, approved in accordance with the relevant Law on Public Financial Management and Accountability.	1. Budžet ASB-a je budžetska stavka u okviru budžeta MUP-a, koji je odobren u skladu sa relevantnim Zakonom o upravljanju javnim finansijama i odgovornostima.
2. Drejtori Ekzekutiv përgatit buxhetin e ASK-së, dhe e përcjell tek Ministri për shqyrtim dhe procedim të mëtutjeshëm, në përputhshmëri me procedurat e parapara me ligj.	2. The Executive Director shall prepare the budget of CSA and shall forward it to the Minister for further review and proceeding, in accordance with the procedures foreseen by the law.	2. Izvršni direktor priprema budžet ASB-a i prosleđuje ga ministru na dalje razmatranje i obradu, u skladu sa zakonom predviđenim procedurama.
3. Drejtori Ekzekutiv është përgjegjës për menaxhimin efektiv dhe efikas të buxhetit të ASK-së, në pajtim me ligjin dhe me rregullat e brendshme buxhetore të MPB-së.	3. The Executive Director shall be responsible for the effective and efficient management of the CSA budget, in accordance with the Law and the internal budgetary rules of the Ministry.	3. Izvršni direktor je odgovoran za efektivno i efikasno upravljanje budžetom ASB-a, u skladu sa zakonom i internim budžetskim pravilima Ministarstva.

4. Të hyrat buxhetore që krijohen nga veprimtaria e ASK-së, derdhen në Buxhetin e Republikës së Kosovës.	4. Budget revenues generated by the activity of CSA are deposited in the Budget of the Republic of Kosovo.	4. Budžetski prihodi ostvareni delatnošću ASB-a prilivaju se u budžet Republike Kosovo.
Neni 21 **Këshilli Shtetëror për Siguri Kibernetike**	**Article 21** **National Cyber Security Council**	**Član 21** **Državni savet za sajber bezbednost**
1. Këshilli Shtetëror për Siguri Kibernetike është organ këshillimor i pavarur në nivel shtetëror i Qeverisë së Republikës së Kosovës dhe komunitetit të biznesit , përmes Qeverisë, i përbërë nga përfaqësues të nivelit të lartë nga institucionet qeveritare, institucionet e zbatimit të ligjit, organizatat publike, ato private dhe komunitetit shkencor.	1. The National Cyber Security Council is an independent state-level advisory body to the Government of the Republic of Kosovo and the business community, through government composed of high-level representatives from government institutions, public and private organizations and scientific community.	1. Državni savet za sajber bezbednost je nezavisni savetodavni organ na državnom nivou Vlade Republike Kosovo i poslovne zajednice, preko vlade, sastavljen od visokih predstavnika vladinih institucija, institucija za sprovođenje zakona, javni i privatnih organizacije i naučne zajednice.
2. KSHSK ndërmerr masa në nivel strategjik për të rritur nivelin e sigurisë kibernetike në Republikën e Kosovës.	2. The NCSC should take measures at a strategic level to increase the level of cyber security in the Republic of Kosovo.	2. DSSB preduzima mere na strateškom nivou za povećanje nivoa sajber bezbednosti u Republici Kosovo.
2. KSHSK ka qëllim të vendos një mbulueshmëri sa më të gjerë të aspekteve të ndryshme të fushës së sigurisë kibernetike.	3. The NCSC intends to establish a wide coverage of various aspects of the cyber security field.	3. DSSB ima za cilj da uspostavi što širu pokrivenost različitih aspekata iz oblasti sajber bezbednosti.
4. KSHSK është përgjegjës për forcimin e koordinimit dhe bashkëpunimit midis institucioneve të ndryshme publike me kompetencat në çështjet e sigurisë kibernetike, si dhe ndërmjet sektorit	4. The NCSC is responsible for strengthening coordination and cooperation between various public institutions with competencies in cyber security issues, as well as between the public and private	4. DSSB je odgovoran za jačanje koordinacije i saradnje između različitih javnih institucija sa nadležnostima u pitanjima sajber bezbednosti, kao i između javnog i privatnog sektora. Takođe, ovaj

publik dhe atij privat. Gjithashtu, ky këshill do e lehtësoj procesin e vendimmarrjes nëpërmjet analizës, studimit dhe propozimit të nismave në nivel kombëtar dhe ndërkombëtar.	sectors. It will also facilitate the decision-making process by analysing, studying and proposing initiatives at national and international level.	savet će olakšati proces donošenja odluka kroz analizu, proučavanje i predlaganje inicijativa na nacionalnom i međunarodnom nivou.
5. KSHSK ka detyra që kontribuojnë në arritjen e misionit të saj përmes:	5. The NCSC has tasks that contribute to achieving its mission through:	5. DSSB ima dužnosti koje doprinose ostvarivanju njegove misije kroz:
5.1. sigurimit të këshillave strategjike të kërkuara për sigurinë kibernetike për Qeverinë e Kosovës dhe komunitetin e biznesit (përmes Qeverisë);	5.1. Providing the required strategic advice on cyber security to the government of Kosovo and the business community (through government).	5.1. Pružanje potrebnih strateških saveta o sajber bezbednosti vladi Kosova i poslovnoj zajednici (preko vlade).
5.2. monitorimit të tendencave dhe zhvillimeve të reja teknologjike dhe, aty ku është e nevojshme, marrjen e masave për të reduktuar rreziqet e sigurisë kibernetike, për të rritur mundësitë ekonomike;	5.2. Monitoring new technological trends and developments and, where necessary, taking measures to reduce cyber security risks, to increase economic opportunities.	5.2. Praćenje novih tehnoloških trendova i razvoja i, tamo gde je potrebno, preduzimanje mera za smanjenje rizika sajber bezbednosti, za povećanje ekonomskih prilika.
5.3. inicimit dhe përshpejtimit të iniciativave relevante që kontribuojnë dukshëm në ngritjen e nivelit të sigurisë kibernetike në Kosovë;	5.3. Initiating and accelerating relevant initiatives that significantly contribute to increase the level of cyber security in Kosovo.	5.3. Pokretanje i ubrzanje relevantnih inicijativa koje značajno doprinose podizanju nivoa sajber bezbednosti na Kosovu.
5.4. mbajtja e diskutimeve për të garantuar që siguria kibernetike arrin agjendën deri në nivel strategjik;	5.4. Holding discussions to ensure that cyber security reaches the agenda up to the strategic level.	5.4. Održavanje rasprava kako bi se osiguralo da sajber bezbednost dostigne agendu strateškog nivoa.
5.5. monitorimi sistematik dhe koordinimi i zbatimit të Strategjisë	5.5. Systematic monitoring and coordination of the implementation of	5.5. Sistematsko praćenje i koordinaciju sprovođenja Nacionalne strategije za

Kombëtare të Sigurisë Kibernetike, duke marrë parasysh të gjitha sfidat ekzistuese dhe të ardhshme në fushën e sigurisë kibernetike;	the National Cyber Security Strategy taking into account all existing and future challenges in the field of cyber security.	sajber bezbednost, uzimajući u obzir sve postojeće i buduće izazove u oblasti sajber bezbednosti.
5.6. sugjerimi i masave të sakta për përmirësimin e zbatimit të Strategjisë Kombëtare të Sigurisë Kibernetike dhe Planit të Veprimit;	5.6. Suggestion of precise measures to improve the implementation of the National Cyber Security Strategy and Action Plan.	5.6. Predlaganje preciznih mera za unapređenje sprovođenja Nacionalne strategije za sajber bezbednost i Akcionog plana.
5.7. identifikimi i sfidave për menaxhimin e krizës kibernetike dhe sugjerimi i masave adekuate për efikasitet më të madh;	5.7. Identify challenges for cyber crisis management and suggest appropriate measures for greater efficiency.	5.7. Identifikacija izazova za upravljanje sajber krizama i predlaganje adekvatnih mera za veću efikasnost.
5.8. zhvillimi i programeve dhe planeve të veprimit për aktivitetet në fushën e sigurisë kibernetike që duhet të zbatohen nga ASK me kapacitete operacionale të sigurisë kibernetike;	5.8. Development of programs and action plans for cyber security activities to be implemented by the CSA with operational cyber security capabilities.	5.8. Razvoj programa i akcionih planova za aktivnosti iz oblasti sajber bezbednosti koje će sprovoditi ASB sa radnim kapacitetima za sajber bezbednost.
6. Udhëheqësi i KSHSK-së është Ministri i MPB-së apo i deleguari i tij i cili *ex officio* është Koordinator Nacional për Siguri Kibernetike.	6. The head of NCSC is the National Coordinator for cyber security, who is the Minister of MIA or his delegate.	6. Rukovodilac Državnog saveta za sajber bezbednost je ministar unutrašnjih poslova ili njegov izaslanik, koji je po službenoj dužnosti državni koordinator za sajber bezbednost.
7. Përbërja e KSHSK-së përcaktohet me vendim nga Koordinatori Nacional për Siguri Kibernetike.	7. Composition of NCSC is defined upon a decision of the National Coordinator for cyber security.	7. Sastav DSSB-a utvrđuje se odlukom Nacionalnog koordinatora za sajber bezbednost.

Neni 22 **Qendra Shtetërore Trajnuese për Sigurinë Kibernetike**	**Article 22** **State Cyber Security Training Centre**	**Član 22** **Državni centar za obuke o sajber bezbednosti**
1. Në kuadër të Ministrisë së Mbrojtjes dhe Forcës së Sigurisë së Kosovës themelohet Qendra Shtetërore Trajnuese për Sigurinë Kibernetike, e cila ofron trajnime për të gjitha institucionet e Republikës së Kosovës në fushën e sigurisë kibernetike.	1. Within the Ministry of Defence and Kosovo Security Force, the State Cyber Security Training Centre is established, which provides training for all institutions of the Republic of Kosovo in the field of cyber security.	1. U okviru Ministarstva odbrane i Kosovskih bezbednosnih snaga osniva se Državni centar za obuke o sajber bezbednosti, koji pruža obuku za sve institucije Republike Kosovo u oblasti sajber bezbednosti.
2. Detyrat dhe përgjegjësitë e Qendrës Shtetërore Trajnuese për Sigurinë Kibernetike përcaktohen më akt nënligjor nga Qeveria e Kosovës, ku përfshihen edhe detyrat e përcaktuara në nenin 12 të këtij ligji.	2. Duties and responsibilities of the State Cyber Security Training Centre are defined by a sub-legal act of the Government of Kosovo, which includes the duties set out in Article 12.	2. Dužnosti i odgovornosti Državnog centra za obuke o sajber bezbednosti biće utvrđene podzakonskim aktom Vlade Kosova, u kojem će biti uključene dužnosti iz člana 12.
Neni 23 **Koordinimi dhe bashkëpunimi i mekanizmave shtetëror për siguri kibernetike**	**Article 23** **Coordination and cooperation of state mechanisms for cyber security**	**Član 23** **Koordinacija i saradnja državnih mehanizama za sajber bezbednost**
Koordinimi dhe bashkëpunimi i mekanizmave shtetëror për parandalimin e sulmeve kibernetike dhe mbrojtjen kibernetike në Republikën e Kosovës, do të rregullohet me një akt të nënligjor të propozuar nga Ministri i ministrisë përgjegjëse për punë të brendshme dhe të miratuar nga Qeveria e Kosovës.	Coordination and cooperation of state mechanisms for the prevention of cyber-attacks and cyber protection in the Republic of Kosovo shall be regulated by a bylaw proposed by the Minister of the Ministry responsible for internal affairs and approved by the Government of Kosovo.	Koordinacija i saradnja državnih mehanizama za sprečavanje sajber-napada i sajber zaštitu u Republici Kosovo uređuje se podzakonskim aktom koji predlaže ministar nadležnog za unutrašnje poslove ministarstva, a usvaja Vlada Kosova.

KAPITULLI V DISPOZITAT PËRFUNDIMTARE	CHAPTER V FINAL PROVISIONS	POTPOGLAVLJE V ZAVRŠNE ODREDBE
Neni 24 **Masat ndëshkuese**	**Article 24** **Punitive Measures**	**Član 24** **Kaznene mere**
1. Kur operatorët e shërbimeve esenciale dhe ofruesit e shërbimeve digjitale nuk marrin masat e përcaktuara në nenet 5, 6, 7 dhe 8 të këtij ligji, ASK do të urdhëroj marrjen e masave korrigjuese dhe do të dërgoj paralajmërime me shkrim.	1. When the operators of essential services fail to take the system security measures provided for in Articles 5, 6, 8 and 8 of this Law, the CSA shall order the taking of corrective measures and shall send warnings.	1. Ukoliko operateri osnovnih usluga i provajderi digitalnih usluga ne preduzmu mere utvrđene u članovima 5, 6, 7. i 8. ovog zakona, ASB će naložiti preduzimanje korektivnih mere i poslaće upozorenja;
2. Nëse operatorët e shërbimeve esenciale dhe ofruesit e shërbimeve digjitale nuk i zbatojnë masat e përcaktuara sipas paragrafit 1 të këtij neni, ASK për shkeljen e detyrimeve të përcaktuara me këtë ligj, shqipton gjobën për personin juridik nga pesëmbedhjetë mijë (15.000) euro deri në tridhjetë mijë (30.000) euro.	2. When operators of essential services and digital service providers fail to implement the measures specified in the paragraph 1 of this Article, CSA imposes fines from fifteen thousand (15,000) euros to thirty thousand (30,000) euros to legal entities violating obligations set out in this law.	2. Ukoliko operateri osnovnih usluga i provajderi digitalnih usluga ne primenjuju mere utvrđene u skladu sa stavom 1. ovog zakona, za kršenje obaveza utvrđene ovim zakonom, ASB će pravnom licu izricati Novčana kazna od petnaest hiljada (15.000) evra do trideset hiljada (30.000) evra.
3. Gjoba prej e njëmijë (1.000) euro deri në njëmijë e pesëqind (1.500) euro i shqiptohet personit përgjegjës në personin juridik, për mos zbatimin e obligimeve të përcaktuara me këtë ligj.	3. Fines from 1,000 - 1,500 Euro will be imposed on the responsible person in the legal entity for non-implementation of obligations defined by this law.	3. Novčana kazna deset hiljada (10.000) evra do petnaest hiljada (15.000) evra.izricaće se odgovornom licu pravnog lica za nesprovođenje obaveza utvrđenim ovim zakonom.
Neni 25 **Aktet nënligjore**	**Article 25** **Bylaws**	**Član 25** **Podzakonski akti**
Aktet nënligjore të parapara me këtë ligj miratohen brenda një (1) viti pas hyrjes në	The by-laws provided for by this law should be approved within one (1) year after the	Podzakonski akti predviđeni ovim zakonom usvajaju se u roku od jedne (1) godine od

fuqi të këtij ligji.	entry into force of this law.	dana stupanja na snagu ovog zakona.
Neni 26 **Dispozitat shfuqizuese**	**Article 26** **Abrogation Provisions**	**Član 26** **Ukidajuće odredbe**
1. Më hyrjen në fuqi të këtij ligji shfuqizohet: 1.1. Neni 5, 6, 7 dhe 8 i Ligjit Nr. 03/L-166 për Parandalimin dhe Luftimin e Krimit Kibernetik; 1.2. Paragrafi 21 i nenit 10 të Ligjit Nr. 04/L-109 për Komunikime Elektronike.	1. Upon entry into force of this law, the following articles are abrogated: 1.1. Articles 5, 6, 7, 8, of law No. 03/L-166 on Prevention and Fight of the Cyber Crime; 1.2. Paragraph 21 of Article 10 of the Law no. 04 / L-109 on Electronic Communications.	1. Stupanjem na snagu ovog zakona, stavljaju se van snage: 1.1. Člana 5, 6, 7, 8, zakon br. 03/L-166 sprečavanju i suzbijanju kibernetičkog zločina; 1.2. Stav 21. člana 10. Zakona br. 04/L-109 o elektronskim komunikacijama.
2. Të gjitha asetet e krijuara bazuar në paragrafin 1.2 të këtij neni, transferohen tek ASK.	2. All assets created based on this paragraph are transferred to CSA.	2. Sva sredstva stvorena na osnovu stava 1.2 ovog člana se prenose na ASB-u.
Neni 27 **Hyrja në fuqi**	**Article 27** **Entry into force**	**Član 27** **Stupanje na snagu**
Ky ligj hyn në fuqi pesëmbëdhjetë (15) ditë pas publikimit në Gazetën Zyrtare të Republikës së Kosovës. **Glauk KONJUFCA** **Kryetar i Kuvendit të Republikës së Kosovës**	This Law shall enter into force fifteen (15) days after its publication in the Official Gazette of the Republic of Kosovo. **Glauk KONJUFCA** **President of the Assembly of the Republic of Kosovo**	Ovaj zakon stupa na snagu petnaest (15) nakon objavljivanja u Službenom listu Republike Kosovo. **Glauk KONJUFCA** **Predsednik Skupštine Republike Kosovo**