



REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Politika e Bashkëpunimi Ndërkombëtar

Përmbajtja

1. Qëllimi	3
2. Fusha e zbatimit.....	3
3. Parimet Themelore	3
4. Rolet dhe Përgjegjësitë	3
5. Elementët e Politikës për Bashkëpunimin Ndërkombëtar	4
6. Referencat.....	5
7. Frekuenca e Rishikimit.....	5

1. Qëllimi

Qëllimi i kësaj politike është që të theksojë bashkëpunimin ndërkombëtar duke adresuar në mënyrë efektive kërcënimet ndërkombëtare dhe sfidat kibernetike.

Qëllimi i kësaj politike është të krijojë një kuadër të qartë, të strukturuar dhe të zbatueshëm për mënyrën se si Republika e Shqipërisë ndërton dhe zhvillon bashkëpunimin ndërkombëtar në fushën e sigurisë kibernetike për të adresuar në mënyrë efektive kërcënimet ndërkombëtare dhe sfidat kibernetike.

2. Fusha e zbatimit

Kjo politikë zbatohet në kuadër të strategjisë kombëtare të sigurisë kibernetike 2025-2030 dhe rregullon parimet e bashkëpunimit ndërkombëtar ndërmjet institucioneve përgjegjëse kombëtare të sigurisë dhe mbrojtjes dhe partnerëve ndërkombëtarë, me qëllim ndërtimin dhe ruajtjen e një hapësire kibernetike të sigurt, të qëndrueshme dhe reziliente.

Politika synon të nxisë shkëmbimin e informacionit, koordinimin e veprimeve dhe harmonizimin e praktikave për përballimin e kërcënimeve kibernetike gjithnjë e më komplekse dhe me shtrirje ndërkufitare.

3. Parimet Themelore

Zbatimi i kësaj politike mbështetet në disa parime themelore që përfshin çdo formë bashkëpunimi ndërkombëtar. Së pari, respektohet sovraniteti kombëtar dhe interesat strategjike të Republikës së Shqipërisë. Bashkëpunimi zhvillohet mbi bazën e besimit të ndërsjellë, transparencës dhe përfitimit të përbashkët me partnerët ndërkombëtarë.

Një rëndësi e veçantë i kushtohet ruajtjes së konfidencialitetit të informacionit që shkëmbehet, veçanërisht kur bëhet fjalë për të dhëna sensitive apo informacione që lidhen me sigurinë kombëtare. Çdo bashkëpunim realizohet në përputhje të plotë me legjislacionin kombëtar dhe detyrimet ndërkombëtare të Shqipërisë, duke u mbështetur në parimet e reciprocitetit, transparencës dhe përmirësimit të vazhdueshëm të kapaciteteve institucionale.

4. Rolet dhe Përgjegjësitë

4.1 Roli i Autoriteti Kombëtar për Sigurinë

Autoriteti Kombëtar për Sigurinë Kibernetike ka rolin qendror në koordinimin e bashkëpunimit ndërkombëtar në fushën e sigurisë kibernetike. AKSK është institucioni që identifikon nevojat strategjike të vendit në këtë fushë, propozon nisma bashkëpunimi me partnerët ndërkombëtarë dhe mbikëqyr zbatimin e marrëveshjeve të lidhura. Po ashtu, AKSK përfaqëson Shqipërinë në rrjete, forume dhe mekanizma ndërkombëtarë të sigurisë kibernetike dhe ka përgjegjësi për të monitoruar zbatimin e kësaj politike dhe për të raportuar mbi progresin e arritur.

4.2 Roli i CSIRT Kombëtar

CSIRT-i Kombëtar luan një rol kryesisht operacional në bashkëpunimin ndërkombëtar duke u angazhuar në mënyrë aktive në rrjetet ndërkombëtare të CSIRT-eve, duke shkëmbyer informacion teknik mbi incidente, dobësi dhe kërcënime. Përmes këtij bashkëpunimi, CSIRT-i kontribuon në rritjen e kapaciteteve teknike kombëtare dhe siguron që Shqipëria të përfitojë nga përvojat dhe praktikat më të mira të vendeve partnere. Gjithashtu, CSIRT-i merr pjesë në ushtrime ndërkombëtare që simulojnë incidente kibernetike, me qëllim përmirësimin e gatishmërisë për reagim.

4.3 Roli i Ministrisë për Evropën dhe Punët e Jashtme

Ministria për Evropën dhe Punët e Jashtme kontribuon në këtë politikë përmes dimensionit të diplomacisë kibernetike. Ajo mbështet përfaqësimin e Shqipërisë në organizata dhe struktura ndërkombëtare, si dhe ndihmon në koordinimin e marrëdhënieve diplomatike që lidhen me marrëveshjet ndërkombëtare në fushën e sigurisë kibernetike. Në këtë mënyrë sigurohet që bashkëpunimi teknik të jetë i harmonizuar me politikën e jashtme të vendit.

4.4 Roli i institucioneve të tjera publike

Institucionet e tjera publike, në varësi të fushës së tyre të përgjegjësisë, marrin pjesë në zbatimin e kësaj politike duke kontribuar në projekte, iniciativa apo mekanizma ndërkombëtarë. Ato kanë detyrimin të raportojnë periodikisht mbi aktivitetet që zhvillojnë në kuadër të bashkëpunimit ndërkombëtar për sigurinë kibernetike.

5. Elementët e Politikës për Bashkëpunimin Ndërkombëtar

Marrëveshje Bilaterale dhe Multilaterale:

Nxitja dhe zhvillimi i marrëveshjeve bilaterale dhe multilaterale me shtete, organizata dhe struktura ndërkombëtare, me qëllim bashkëpunimin në fushën e sigurisë kibernetike, shkëmbimin e informacionit mbi kërcënimet kibernetike, zhvillimin e ushtrimeve të përbashkëta dhe koordinimin e reagimit ndaj incidenteve kibernetike.

Pjesëmarrja në Forume Ndërkombëtare:

Pjesëmarrje aktive në forume, organizata dhe konferenca ndërkombëtare të lidhura me sigurinë kibernetike, siç janë Kombet e Bashkuara, INTERPOL, Qendra e Bashkëpunimit për Mbrojtjen Kibernetike e NATO-s (CCDCOE), dhe Forumi Global për Ekspertizë Kibernetike (GFCE), Forumi për Menaxhimin e Incidenteve, etj.

Rregullat dhe Standardet Globale të Sigurisë Kibernetike:

Harmonizimi i politikave, kuadrit rregullator dhe praktikave kombëtare me rregullat dhe standardet ndërkombëtare të sigurisë kibernetike, përfshirë standardet ISO/IEC dhe kornizën NIST për menaxhimin e rrezikut dhe sigurisë së informacionit.

Legjislacioni dhe Zbatimi i Ligjit për Krimet Kibernetike Ndërkufitare:

Bashkëpunimi ndërkombëtar për zhvillimin dhe harmonizimin e legjislacionit për krimet kibernetike, përfshirë mekanizmat e ndihmës juridike ndërkombëtare, me qëllim parandalimin, hetimin dhe ndjekjen penale të veprave penale kibernetike me karakter ndërkufitar.

Në këtë kuadër, mbështeten iniciativat për asistencë teknike dhe ngritje kapacitetesh, veçanërisht për shtetet në zhvillim, në funksion të rritjes së sigurisë kibernetike globale.

Shkëmbimi i Informacionit të Sigurisë Kibernetike, Threat Intel dhe Koordinimi Operacional

Marrja pjesë në mekanizma dhe rrjete ndërkombëtare për shkëmbimin e informacionit mbi kërcënimet, cenueshmëritë dhe incidentet kibernetike realizohet në përputhje me legjislacionin në fuqi për mbrojtjen e informacionit dhe të dhënave.

Promovohet koordinimi operacional me homologët ndërkombëtarë për reagimin e përbashkët dhe të koordinuar ndaj incidenteve kibernetike, si dhe zhvillimi i projekteve të përbashkëta kërkimore dhe zhvillimore në fushën e sigurisë kibernetike.

Diplomacia kibernetike është instrument për adresimin e çështjeve që lidhen me sigurinë dhe stabilitetin kibernetik në nivel ndërkombëtar.

Trajnimet dhe Shkëmbimet Akademike:

Pjesëmarrja në programe ndërkombëtare të trajnimit, edukimit dhe shkëmbimeve akademike, me qëllim rritjen e kapaciteteve profesionale dhe institucionale në fushën e sigurisë kibernetike. Mbështetja e Iniciativave Ndërkombëtare të Sigurisë Kibernetike: Mbështetja dhe inkurajimi i iniciativave ndërkombëtare të cilat ynojnë forcimin e stabilitetit kibernetik dhe mbrojtjen e infrastrukturave kritike të informacionit në nivel global.

6. Referencat

Kjo politikë mbështetet në legjislacionin kombëtar për sigurinë kibernetike, Strategjinë Kombëtare për Sigurinë Kibernetike, si dhe në praktikat dhe standardet ndërkombëtare të njohura në fushën e bashkëpunimit ndërkombëtar për sigurinë kibernetike.

7. Frekuenca e Rishikimit

Ky dokument duhet të rishikohet të paktën një herë në vit ose kur ka ndryshime të rëndësishme në sistemin e menaxhimit të sigurisë së informacionit në institucion.