



REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Politika e Partneritetit Publik-Privat

Përmbajtja

1. Qëllimi	3
2. Fusha e zbatimit	3
3. Parimet Themelore	3
4. Rolet dhe përgjegjësitë	3
5. Elementët e Politikës për Partneritetin Publik-Privat.....	4
6. Referencat.....	5
7. Frekuenca e Rishikimit	5

1. Qëllimi

Qëllimi i kësaj politike është të ofrojë një qasje strategjike për lehtësimin dhe forcimin e bashkëpunimit ndërmjet entiteteve qeveritare dhe organizatave të sektorit privat, me synim rritjen e nivelit të sigurisë kibernetike kombëtare dhe mbrojtjen e infrastrukturave dhe shërbimeve kritike.

2. Fusha e zbatimit

Kjo politikë forcon bashkëpunimin publik-privat dhe kontribuon në rritjen e kapaciteteve për parandalimin, mbrojtjen dhe reagimin ndaj incidenteve kibernetike. Në këtë kuadër, politika synon:

1. Të minimizojë rreziqet kibernetike dhe të garantojë integritetin, disponueshmërinë dhe qëndrueshmërinë e shërbimeve të infrastrukturave kritike;
2. Të mbështesë zhvillimin dhe zbatimin e standardeve të larta të sigurisë kibernetike;
3. Të promovojë një qasje të koordinuar, të qëndrueshme dhe gjithëpërfshirëse ndaj sigurisë kibernetike.

3. Parimet Themelore

Politika për Partneritetin Publik-Privat bazohet në parimin e mbrojtjes së interesit publik dhe sigurisë kombëtare, përgjegjësinë e përbashkët të sektorit publik dhe privat, si dhe në ndërtimin e besimit dhe transparencës ndërmjet palëve. Bashkëpunimi zhvillohet në përputhje me legjislacionin në fuqi duke garantuar proporcionalitet, efikasitet dhe mbrojtjen e konfidencialitetit të informacionit. Politika nxit përfshirjen e aktorëve relevantë, qëndrueshmërinë afatgjatë dhe përmirësimin e vazhdueshëm të mekanizmave të bashkëpunimit, me synim krijimin e vlerës së shtuar dhe forcimin e kapaciteteve kombëtare.

4. Rolet dhe përgjegjësitë

• Roli i AKSK

Autoriteti Kombëtar për Sigurinë Kibernetike ka rol koordinues në zbatimin e kësaj politike për Partneritetin Publik-Privat. AKSK përcakton prioritetet kombëtare të bashkëpunimit, lehtëson krijimin dhe funksionimin e mekanizmave të partneritetit ndërmjet institucioneve publike dhe aktorëve të sektorit privat, mbikëqyr zbatimin e masave të sigurisë kibernetike, promovon ndarjen e sigurt të informacionit dhe mbështet iniciativat e përbashkëta në nivel kombëtar

• Roli i institucioneve publike

Institucionet publike kanë përgjegjësi për të marrë pjesë aktive në zbatimin e kësaj politike për Partneritetin Publik-Privat, në përputhje me kërkesat ligjore, si dhe duke respektuar gjithmonë kërkesat e qarta të sigurisë. Institucionet publike bashkëpunojnë me AKSK dhe aktorët e sektorit privat për forcimin e kapaciteteve, menaxhimin e rrezikut dhe përmirësimin e aftësive për parandalimin, zbulimin dhe reagimin ndaj kërcënimeve kibernetike në nivel kombëtar.

• Roli i sektorit privat dhe shoqërisë civile

Sektori privat dhe organizatat e shoqërisë civile janë partnerë kyç në zbatimin e kësaj politike, duke kontribuar me ekspertizë teknike dhe inovacion. Në bashkëpunim me AKSK dhe institucionet publike, këta aktorë marrin pjesë në iniciativa të përbashkëta, ndajnë praktika të mira dhe mbështesin zhvillimin e kapaciteteve kombëtare për parandalimin, zbulimin dhe reagimin ndaj kërcënimeve kibernetike.

5. Elementët e Politikës për Partneritetin Publik-Privat

i. Struktura për Bashkëpunim

Vendosja e një strukture apo platforme formale për komunikim dhe bashkëpunim të vazhdueshëm midis sektorëve publik dhe privat në fushën e sigurisë kibernetike. Kjo mund të përfshijë komitete të përbashkëta, grupe pune, ose task forca.

ii. Mekanizma të Ndarjes së Informacionit

Krijimi dhe zbatimi i protokolleve për ndarjen e informacionit mbi kërcënimet kibernetike, cënueshmëritë dhe praktikatat më të mira ndërmjet entiteteve publike dhe private, duke siguruar respektimin e kërkesave për privatësi, konfidencialitet dhe mbrojtje të informacionit.

iii. Nisma të Përbashkëta të Sigurisë Kibernetike

Zhvillimi i projekteve dhe programeve bashkëpunuese që shfrytëzojnë kapacitetet dhe ekspertizën e sektorëve publik dhe privat, me fokus në mbrojtjen e infrastrukturave kritike, kërkimin dhe zhvillimin, si dhe ndërgjegjësimin për sigurinë kibernetike.

iv. Ngritja dhe zhvillimi kapaciteteve njerëzore

Zbatimi i programeve të përbashkëta të trajnimit dhe stërvitjeve për ekspertët e sigurisë kibernetike, me qëllim forcimin e aftësive profesionale dhe adresimin e mungesës së kapaciteteve dhe talenteve në këtë fushë.

v. Mbështetje Ligjore dhe Rregullatore

Sigurimi i mbështetjes ligjore dhe zhvillimi i një kuadri rregullator që nxit pjesëmarrjen e sektorit privat në iniciativat e sigurisë kibernetike dhe ofron mbrojtje ligjore për ndarjen e informacionit në përputhje me legjislacionin në fuqi.

vi. Standardet dhe Praktikatat më të Mira të Sigurisë Kibernetike

Inkurajimi i adoptimit dhe zbatimit të standardeve kombëtare dhe ndërkombëtare të sigurisë kibernetike, si dhe praktikave më të mira, veçanërisht brenda sektorit privat.

vii. Planifikimi i Përgjigjes ndaj Incidenteve dhe Rikuperimit

Bashkëpunimi në zhvillimin dhe zbatimin e strategjive të përbashkëta për përgjigjen ndaj incidenteve kibernetike dhe planet e rikuperimit, me qëllim menaxhimin dhe zbutjen e ndikimit të incidenteve.

viii. Financimi dhe Burimet

Alokimi i burimeve qeveritare dhe ofrimi i nxitjeve për të mbështetur iniciativat e sigurisë kibernetike në sektorin privat, duke përfshirë grante, nxitje fiskale dhe financim për projekte të përbashkëta kërkimi dhe zhvillimi.

ix. Bashkëpunimi në Menaxhimin e Rrezikut

Bashkëpunimi për identifikimin, vlerësimin dhe zbutjen e rreziqeve të sigurisë kibernetike, veçanërisht atyre që prekin njëkohësisht sektorët publik dhe privat.

x. Zhvillimi i Politikave dhe Planifikimi Strategjik

Përfshirja e ekspertizës dhe perspektivave të sektorit privat në proceset e zhvillimit të politikave kombëtare dhe planeve strategjike për sigurinë kibernetike, me qëllim ndërtimin e një qasjeje të koordinuar dhe gjithëpërfshirëse ndaj kërcënimeve kibernetike.

6. Referencat

Kjo politikë mbështetet në legjislacionin kombëtar për sigurinë kibernetike, Strategjinë Kombëtare për Sigurinë Kibernetike, si dhe në praktikën dhe standardet ndërkombëtare të njohura në fushën e partneritetit publik-privat në siguri 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.