



REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Politika e Komunikimit

Përmbajtja

1.	Hyrje	3
2.	Qëllimi	3
3.	Fusha e zbatimit	3
4.	Parimet Themelore të Komunikimit	4
5.	Rolet dhe Përgjegjësitë.....	4
6.	Elementët e Politikës për Komunikim	4
7.	Menaxhimi i klasifikimit të informacionit	5
8.	Komunikimi dhe Bashkëpunimi Ndërinstitucional dhe Ndërkombëtar	5
9.	Trajnimi dhe ndërgjegjësimi mbi Komunikimin efektiv	6
10.	Përdorimi i Teknologjisë për Komunikim	6
11.	Mekanizmat e Reagimit	6
12.	Referenca	6
13.	Frekuenca e rishikimit.....	6

1. Hyrje

Politika për Komunikim përbën një komponent thelbësor të strategjisë kombëtare për të adresuar sfidat në rritje të sigurisë kibernetike. Kjo politikë përcakton kornizën e komunikimit dhe koordinimit ndërmjet institucioneve publike, sektorit privat dhe publikut, me qëllim adresimin e kërcënimeve kibernetike, menaxhimin e incidenteve dhe rritjen e ndërgjegjësimit për sigurinë kibernetike.

Përmes përcaktimit të protokolleve të komunikimit, planeve të komunikimit në situata krize dhe mekanizmave të bashkëpunimit, politika synon të forcojë reagimin kombëtar ndaj rreziqeve kibernetike, të mbrojë interesat kombëtare dhe të ruajë besimin e publikut në shërbimet dhe mjedisin digjital.

Komunikimi efektiv në fushën e sigurisë kibernetike përbën një komponent thelbësor të mbrojtjes së interesit kombëtar, ruajtjes së besimit të publikut dhe garantimit të një reagimi të koordinuar ndaj incidenteve kibernetike. Në një mjedis digjital gjithnjë e më kompleks dhe të ekspozuar ndaj kërcënimeve hibride, mungesa e një komunikimi të strukturuar mund të çojë në keqinformim, panik publik, cenim të reputacionit institucional dhe dëm të drejtpërdrejtë ndaj sigurisë kombëtare.

Kjo politikë përcakton kornizën kombëtare të komunikimit për çështjet e sigurisë kibernetike duke vendosur parime udhëheqëse, role të qarta, përgjegjësi institucionale dhe mekanizma koordinimi ndërmjet institucioneve publike, sektorit privat, aktorëve akademikë dhe publikut të gjerë.

2. Qëllimi

Qëllimi i kësaj politike është të sigurojë që të gjitha palët e interesit si agjencitë qeveritare deri te sektori privat dhe publiku, të jenë të informuara, të koordinuara dhe të përgatitura për t'u përballur me kërcënimet kibernetike. Kjo do të arrihet përmes vendosjes së protokolleve të qarta të komunikimit, trajnimit të duhur dhe përdorimit të teknologjive të avancuara, me qëllim ruajtjen e sigurisë kombëtare dhe besimit të publikut.

Gjithashtu kjo politike synon të krijojë dhe të konsolidojë një sistem të standardizuar, të koordinuar dhe të besueshëm komunikimi në fushën e sigurisë kibernetike. Politika synon të sigurojë që komunikimi institucional të mbështesë parandalimin dhe menaxhimin efektiv të incidenteve kibernetike, të mundësojë informimin korrekt dhe në kohë të publikut, të ruajë besimin në institucionet shtetërore dhe të kontribuojë në forcimin e kapaciteteve kombëtare për reagim ndaj kërcënimeve kibernetike. Njëkohësisht, kjo politikë synon të garantojë përputhshmërinë e plotë me kuadrin ligjor dhe rregullator në fuqi.

3. Fusha e zbatimit

Kjo politikë zbatohet për Autoritetin Kombëtar për Sigurinë Kibernetike dhe të gjitha strukturat e tij përbërëse, për institucionet publike të administratës qendrore dhe vendore, për operatorët e Infrastrukturave Kritike dhe të Rëndësishme të Informacionit, si dhe për

subjektet private që përfshihen në incidente me 0ndikim të gjerë kombëtar. Politika shtrihet gjithashtu në marrëdhëniet e komunikimit me partnerët kombëtarë dhe ndërkombëtarë të fushës së sigurisë kibernetike.

4. Parimet Themelore të Komunikimit

Komunikimi kombëtar për çështjet e sigurisë kibernetike udhëhiqet nga parimi i saktësisë mbi shpejtësinë, duke garantuar që çdo informacion që publikohet të jetë i verifikuar dhe i bazuar në fakte të konfirmuara. Transparenca konsiderohet element kyç i besimit publik, zbatohet në mënyrë të kontrolluar për të shmangur cenimin e sigurisë operationale dhe komprometimin e hetimeve apo masave mbrojtëse.

Politika mbështetet në parimin “need-to-know”, sipas të cilit informacioni ndahet vetëm me palët që kanë nevojë legjitime për tu njohur. Komunikimi për incidente me ndikim të gjerë duhet të jetë i koordinuar në nivel qendror dhe të realizohet vetëm përmes autoriteteve të autorizuar, duke shmangur deklaratat e pakontrolluara që mund të krijojnë konfuzion apo dëm institucional.

5. Rolet dhe Përgjegjësitë

Autoriteti Kombëtar për Sigurinë Kibernetike mban rolin qendror të koordinimit të komunikimit kombëtar për incidentet kibernetike me ndikim të lartë. AKSK është përgjegjës për nxjerrjen e njoftimeve zyrtare, për garantimin e koherencës së mesazhit institucional dhe për veprimin si pikë kontakti me autoritetet ndërkombëtare homologe.

CERT-i Kombëtar luan një rol teknik mbështetës, duke përgatitur analizat profesionale që shërbejnë si bazë për komunikimin publik dhe institucional, si dhe duke publikuar njoftime teknike dhe këshilla profesionale për komunitetin e sigurisë.

Institucionet publike kanë detyrimin të raportojnë në kohë pranë AKSK çdo incident të sigurisë, si dhe të mos ndërmarrin komunikim publik të pakoordinuar. Ato duhet të caktojnë pika kontakti të dedikuara për çështjet e komunikimit në fushën e sigurisë kibernetike.

6. Elementët e Politikës për Komunikim

I. Protokollet e Komunikimit të Brendshëm

Përcaktimi i kanaleve dhe rregullave të komunikimit brenda institucioneve publike dhe ndërmjet sektorëve publik dhe privat, për shkëmbimin e informacionit mbi kërcënimet kibernetike, cënueshmëritë dhe incidentet.

Institucionet janë të detyruara të përdorin kanale të sigurta për komunikimin e informacionit të lidhur me incidentet kibernetike, të respektojnë klasifikimin e informacionit dhe të dokumentojnë çdo vendimarrje të rëndësishme gjatë menaxhimit të situatave të krizës. Gjurmueshmëria e komunikimit përbën element thelbësor për llogaridhënie dhe për përmirësim të vazhdueshëm institucional.

II. Strategjitë e Komunikimit Publik

Hartimi i protokolleve për komunikimin me publikun lidhur me kërcënimet dhe incidentet kibernetike, si dhe me çështjet e ndërgjegjësimit. Në këtë kuadër përcaktohen lloji i informacionit që publikohet, mënyra e publikimit dhe autoritetet e autorizuar për komunikim zyrtar.

Komunikimi me publikun duhet të jetë i qartë, profesional dhe i bazuar në fakte të verifikuara. Informacioni i shpërndarë nuk duhet të krijojë panik, as të minimizojë rrezikun real, por të ruajë një balancë që nxit besimin dhe përgjegjësinë qytetare. Çdo komunikim publik duhet të respektojë parimet e mbrojtjes së të dhënave personale dhe interesin publik.

III. Planet e Komunikimit të Krizës

Hartimi i planeve për komunikim gjatë dhe pas incidenteve ose krizave të sigurisë kibernetike, duke garantuar shpërndarjen e informacionit të saktë dhe në kohë të publiku, media dhe palët e tjera të interesit.

Në rast të incidenteve kibernetike me ndikim të gjerë, komunikimi institucional duhet të ndjekë një strukturë të qartë të ndarë me faza. Fillimisht publikohet një deklaratë paraprake për të informuar publikun mbi situatën. Më pas, realizohen përditësime periodike mbi zhvillimin e incidentit dhe masat e marra. Pas përfundimit të menaxhimit të situatës, institucionet janë të detyruara të ofrojnë një komunikim përmbledhës që përfshin mësimet e nxjerra dhe masat përmirësuese të ndërmarra. Gjatë gjithë procesit duhet të respektohet parimi i pikës së vetme të komunikimit.

7. Menaxhimi i klasifikimit të informacionit

Nuk lejohet publikimi i informacionit që përmban detaje teknike të cilat mund të shfrytëzohen për sulme të mëtejshme, të dhëna sensitive operacionale, të dhëna personale pa bazë ligjore, si dhe informacion që mund të cenojë proceset hetimore ose procedurat e reagimit ndaj incidenteve. Çdo vendim për publikimin e informacionit duhet të marrë në konsideratë balancën midis transparencës dhe sigurisë.

8. Komunikimi dhe Bashkëpunimi Ndërinstitucional dhe Ndërkombëtar

AKSK nxit dhe promovon shkëmbimin e informacionit me autoritete homologe ndërkombëtare, organizata partnere, operatorë të infrastrukturave kritike dhe aktorë të tjerë strategjikë, me qëllim shkëmbimin e informacionit, praktikave më të mira dhe koordinimin e reagimit ndaj kërcënimeve kibernetike me karakter ndërkombëtar.

Lehtësimi i komunikimit dhe bashkëpunimit me organizata ndërkombëtare dhe qeveri të huaja, për shkëmbimin e informacionit, praktikave më të mira dhe koordinimin e reagimit ndaj kërcënimeve kibernetike me karakter ndërkombëtar.

9. Trajnimi dhe ndërgjegjësimi mbi Komunikimin efektiv

Zhvillimi i trajnimeve për personelin përkatës mbi komunikimin efektiv, përfshirë trajtimin e informacionit të ndjeshëm dhe menaxhimin e komunikimit në situata krize, të organizojnë ushtrime simulimi për incidente dhe të promovojnë një kulturë institucionale që e konsideron komunikimin e përgjegjshëm si pjesë integrale të sigurisë kibernetike.

10.Përdorimi i Teknologjisë për Komunikim

Përdorimi i mjeteve dhe teknologjive të përshtatshme për të garantuar komunikim të shpejtë, të sigurt dhe të qëndrueshëm në kanale të ndryshme.

11.Mekanizmat e Reagimit

Krijimi i kanaleve të komunikimit për të marrë reagime nga publiku dhe palët e interesit mbi politikat dhe incidentet e sigurisë kibernetike, duke mundësuar një rrjedhë të vazhdueshme dhe efektive komunikimi dypalëshe.

12.Referenca

Të gjitha aktivitetet e komunikimit të parashikuara në këtë politikë realizohen në përputhje të plotë me legjislacionin kombëtar për sigurinë kibernetike, legjislacionin për mbrojtjen e të dhënave personale, si dhe me detyrimet ndërkombëtare të Republikës së Shqipërisë.

13.Frekuenca e rishikimit

Kjo politikë rishikohet të paktën një herë në vit dhe gjithashtu pas çdo incidenti madhor që evidenton nevojën për përmirësim të mekanizmave të komunikimit ose të koordinimit institucional.