Politika për Monitorimin dhe Vlerësimin e Performancës

1. Hyrje

Politika për Monitorimin dhe Vlerësimin e Performancës është themelore për të siguruar qëndrueshmërinë dhe mbrojtjen e infrastrukturave kritike dhe të rëndësishme të informacionit. Kjo politikë fokusohet në monitorimin e vazhdueshëm, vlerësimin sistematik të rrezikut dhe përmirësimin e vazhdueshëm të nivelit të qëndrueshmërisë kibernetike, me qëllim mbrojtjen e shërbimeve dhe aseteve kritike nga kërcënimet kibernetike aktuale dhe potenciale. Mungesa e një qasjeje të strukturuar dhe të koordinuar për monitorimin dhe vlerësimin e performancës do të ekspozonte sigurinë kombëtare, stabilitetin ekonomik dhe mirëqenien publike ndaj rreziqeve me pasoja serioze dhe afatgjata.

2. Qëllimi

Qëllimi i kësaj politike është të përcaktojë parimet dhe drejtimet kryesore për zhvillimin dhe zbatimin e një sistemi efektiv të monitorimit dhe vlerësimit të performancës së sigurisë kibernetike për infrastrukturat kritike dhe të rëndësishme të informacionit, me synim forcimin e mbrojtjes së tyre ndaj kërcënimeve kibernetike dhe ruajtjen e sigurisë kombëtare, stabilitetit ekonomik dhe interesit publik.

3. Parimet Themelore të Politikës

Politika bazohet në parimet e matshmërisë, objektivitetit dhe bazës së provave, si dhe në monitorimin e vazhdueshëm, duke siguruar vlerësim të saktë të performancës së infrastrukturave kritike dhe të rëndësishme të informacionit, transparencën e raporteve, bashkëpunimin midis institucioneve publike, sektorit privat dhe shoqërisë civile, si dhe përdorimin e teknologjive të avancuara për përmirësimin e vazhdueshëm të sigurisë kibernetike.

4. Rolet dhe Përgjegjësitë

- **Roli i AKSK**

AKSK koordinon në nivel kombëtar monitorimin dhe vlerësimin e performancës, përcakton standardet dhe metodologjitë që duhet të zbatojnë infrastrukturat kritike, dhe mbikëqyr përputhshmërinë me këto standarde.

- **Roli i Institucioneve publike**

Institucionet publike zbatojnë masat e politikës brenda organizatave të tyre, sigurojnë mbledhjen dhe raportimin e të dhënave për performancën dhe bashkëpunojnë me AKSK për përmirësimin e vazhdueshëm të sigurisë.

- **Roli i Sektorit privat dhe shoqërisë civile**

Sektori privat dhe shoqëria civile mbështesin monitorimin dhe vlerësimin e performancës duke ndarë informacion treguesit e performancës, si dhe duke kontribuar në përmirësimin e vazhdueshëm të sigurisë kibernetike.

5. Elementët e Politikës së Monitorimit dhe Vlerësimit të Performancës

- **Monitorimi i Vazhdueshëm**

Zbatimi i sistemeve, proceseve dhe mekanizmave për monitorimin e vazhdueshëm dhe në kohë reale të aktiviteteve, anomalive dhe kërcënimeve kibernetike që prekin infrastrukturat kritike dhe të rëndësishme.Treguesit e Vlerësimit të Performancës

Përcaktimi i treguesve dhe kritereve të qarta për vlerësimin e performancës së sigurisë kibernetike, përfshirë aftësinë për zbulimin e kërcënimeve, kohën e reagimit ndaj incidenteve dhe kapacitetin e rikuperimit të sistemeve, me qëllim matjen e vazhdueshme të nivelit të sigurisë dhe qëndrueshmërisë.

- **Vlerësimi dhe Menaxhimi i Rrezikut**

Kryerja periodike e vlerësimeve të rrezikut për të identifikuar cenueshmëritë dhe kërcënimet potenciale ndaj infrastrukturave, duke analizuar ndikimin dhe probabilitetin e materializimit të rreziqeve kibernetike.Kontrollet dhe Ri kontrollet e Përputhshmërisë

Zbatimi i kontrolleve dhe rikontrolleve periodike për të verifikuar përputhshmërinë e infrastrukturave kritike me politikat, standardet dhe kërkesat kombëtare të sigurisë kibernetike.

- **Raportimi dhe Analiza e Incidenteve**

Zhvillimi dhe zbatimi i protokolleve të standardizuara për raportimin, analizimin dhe dokumentimin e incidenteve kibernetike, përfshirë funksionalizimin e një sistemi qendror të raportimit për incidentet që prekin infrastrukturat kritike dhe të rëndësishme.Partneritetet Publike-Private Forcimi i bashkëpunimit me subjektet publike dhe private që zotërojnë ose operojnë infrastrukturë kritike, me qëllim përmirësimin e praktikave të monitorimit, raportimit dhe vlerësimit të performancës së sigurisë kibernetike.

- **Ngritja e Kapaciteteve dhe Trajnimi**

Investimi në programe të vazhdueshme trajnimi dhe zhvillimi profesional për personelin e përfshirë në monitorimin, analizën dhe vlerësimin e sigurisë kibernetike, për të garantuar aftësi dhe kompetenca të përshtatshme.

- **Përdorimi i Avancimeve Teknologjike**

Shfrytëzimi i zgjidhjeve teknologjike të avancuara, duke perfshireinteligjencen artificiale dhe machine learning, për të rritur efikasitetin e monitorimit, analizës dhe parashikimit të kërcënimeve kibernetike.

- **Platformat e Ndarjes së Informacionit**

Krijimi dhe funksionalizimi i platformave për ndarjen e informacionit, praktikave më të mira dhe përvojave në lidhje me kërcënimet, cenueshmëritë dhe incidentet e sigurisë kibernetike ndërmjet palëve të interesit.

- **Planet e Përgatitjes dhe Përgjigjes ndaj Emergjencave**

Zhvillimi dhe mirëmbajtja e planeve efektive të përgatitjes dhe reagimit ndaj emergjencave kibernetike, me qëllim adresimin në kohë dhe zbutjen e ndikimit të incidenteve të identifikuara.

- **Angazhimi dhe Ndërgjegjësimi i Palëve të Interesit**

Angazhimi i vazhdueshëm i institucioneve publike, sektorit privat dhe publikut për rritjen e ndërgjegjësimit mbi rëndësinë e monitorimit dhe vlerësimit të performancës së sigurisë kibernetike për infrastrukturat kritike.

- **Mekanizmat e Rishikimit dhe Përditësimit**

Rishikimi dhe përditësimi periodik i kësaj politike dhe mekanizmave të zbatimit të saj, në përputhje me zhvillimet e reja të kërcënimeve kibernetike, përparimet teknologjike dhe ndryshimet në kuadrin ligjor dhe rregullator.

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 monitorimit dhe vlerësimit të performancës.

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.