Nr. 93/ 25.03.2024

POLITICA DE EVALUARE A RISCURILOR DE SECURITATE CIBERNETICA

SCOP

Implementarea procesului de management al riscului de securitate cibernetica bazat pe standardul ISO 27001 facilitand identificarea riscurilor asociate cu pierderea confidentialitatii, integritatii si disponibilitatii datelor. Procesul de management al riscului de securitate cibernetica este aplicat in administrarea globala a datelor.

DOMENIU DE APLICARE

Aceasta politica se aplica retelei interne, componentelor de retea, sistemelor informatice, componentelor sistemelor informatice si dispozitivelor mobile detinute sau operate de CMV.

DEFINITII

Strategia de **transfer de risc** inseamna atribuirea unei terte parti a responsabilitatii pentru gestionarea unui eveniment / risc si a impactului acestuia. Strategia de transfer de risc este aplicabila numai amenintarilor.

Partajarea riscului presupune cooperarea cu o alta parte cu scopul de a imparti in mod convenabil acest risc. (exemplu: polite de asigurare sau clauze contractuale de despagubire).

Speak up se refera la incurajarea unei culturi pozitive, ca mijloc de imbunatatire a activitatii, prin care angajatii simt ca pot vorbi si ca vocile lor vor fi auzite, iar sugestiile lor vor fi puse in aplicare. Speak up inseamna sa poti vorbi liber despre orice lucru care crezi ca va conduce la un rezultat negativ/ o activitate incorecta.

DECLARATIE DE POLITICA

- LabCMV efectueaza permanent o evaluare a securitatii cibernetice identificand riscurile de securitate a informatiilor, probabilitatea si amploarea prejudiciului cauzat de accesul neautorizat, utilizarea, dezvaluirea, intreruperea, modificarea sau distrugerea sistemului si a informatiilor pe care le prelucreaza, le stocheaza sau le transmite.

- LabCMV documenteaza, revizuieste si prioritizeaza riscurile analizate in procesul de management al riscurilor. Tratarea riscului include acceptarea, evitarea, diminuarea si transferul sau partajarea riscului.

- LabCMV se consulta cu societatile care asigura furnizarea software-urilor utilizate, a echipamentelor de laborator si a calculatoarelor, impreuna constituind **Comisia pentru asigurarea securitatii cibernetice**, pentru a selecta optiunile adecvate de tratare a riscurilor de securitate, tinand cont de rezultatele evaluarii riscurilor. LabCMV determina toate controalele care sunt necesare pentru analizarea raspunsului la masurile implementate pentru tratarea riscul de securitate a informatiilor.

- Monitorizeaza sistemul informatic in mod continuu pentru a verifica conformitatea si pentru a determina eficacitatea masurilor de raspuns la risc.

- Efectueaza evaluarea riscurilor in mod periodic sau ori de cate ori apar modificari semnificative ale sistemului sau mediului de operare (inclusiv identificarea de noi amenintari si vulnerabilitati) sau alte conditii care pot afecta starea de securitate a sistemului;

- **Comisia pentru asigurarea securitatii cibernetice** realizeaza periodic evaluari ale amenintarilor si atacurilor asupra firewall-ului pentru a identifica potentialele vulnerabilitati ale sistemului. Remedierea vulnerabilitatilor este prioritizata de echipa de securitate cibernetica si atribuita proprietarului de proces/ utilizatorului corespunzator pentru implementare. Scanarile pentru identificarea vulnerabilitatilor sunt comparate pentru a se asigura ca acestea sunt remediate in timp util.

- LabCMV trebuie sa se informeze in mod continuu asupra alertelor/ directivelor de securitate ale sistemulor de informatii si sa ia masuri in timp util pentru a impiedica/ remedia orice noi amenintari.

- Evaluarea riscului de securitate a informatiilor, planul de tratare a riscurilor si acceptarea riscului rezidual de securitate a informatiilor trebuie sa fie aprobate de conducerea societatii.

CONFORMARE SI AVERTIZARE DE INTEGRITATE (WHISTLEBLOWING)

Nerespectarea acestei politici poate constitui un motiv pentru actiuni disciplinare, pana la si inclusiv reziliere contract individual de munca/ furnizare produse sau servicii.

Angajatii ar trebui sa vorbeasca despre orice comportament pe care il considera cu buna-credinta a fi o incalcare a acestei politici. Sesizarile/ ingrijorarile pot fi raportate prin oricare dintre resursele CMV Speak up. Rapoartele pot fi facute anonim si vor fi tratate in mod confidential in masura permisa de lege.

CMV interzice represaliile pentru rapoartele cu buna-credinta de suspiciune de incalcare a politicii.

Revizuirea acestui document: anual de catre **Comisia pentru asigurarea securitatii cibernetice**

Urmatoarea data de revizuire: 20.03.2025

Intocmit,
Manager Calitate,
Paraschiva Rodica

Aprobat,
Director General
Aionesei Silviu