Antibiotice

Politica de Securitate Cibernetică

2024

În contextul unei dezvoltări sustenabile, Antibiotice SA consideră securitatea cibernetică o componentă esențială a guvernanței corporative, a protecției drepturilor stakeholderilor și a continuității operaționale. Resursele informatice și de comunicații sunt gestionate în mod responsabil, în conformitate cu legislația, standardele internaționale și politicile interne, contribuind astfel la o activitate etică, sigură și sustenabilă.

1. Scopul politicii

Politica de Securitate Cibernetică stabilește cadrul care definește regulile și măsurile necesare pentru protejarea resurselor informatice și de comunicații ale Antibiotice SA. Politica asigura protejarea confidențialității, integrității și disponibilității informațiilor, contribuind la:
• Prevenirea riscurilor de natură digitală cu impact economic, social și reputațional;
• Protejarea drepturilor și datelor personale ale angajaților, clienților și partenerilor;
• Asigurarea unei infrastructuri informatice reziliente și sustenabile.

2. Principii ESG integrate

• **Confidențialitate:** Protejarea datelor cu caracter personal și a informațiilor comerciale sensibile;
• **Integritate:** Promovarea unui comportament etic în utilizarea tehnologiei. Prevenirea modificării sau distrugerii neautorizate a informațiilor;
• **Disponibilitate:** Asigurarea continuității activităților economice esențiale în condiții de transparență și responsabilitate.

3. Aplicabilitate și angajament

Politica se aplică tuturor angajaților, colaboratorilor și furnizorilor, care creează, stochează, accesează sau transmit date și informații utilizând infrastructura Antibiotice SA încurajând un comportament etic și responsabil în mediul digital.
Documentul este comunicat transparent și face parte din angajamentele noastre față de criteriile ESG (Environmental, Social, Governance).

4. Responsabilitate organizațională

• Echipa de Securitate Cibernetică: acționează proactiv pentru prevenirea riscurilor și asigurarea unei infrastructuri informatice sustenabile.
• Echipa de Răspuns la Incidente (IRT): intervine și gestionează în cazul incidentelor de securitate în mod eficient și transparent pentru asigurarea continuității activităților critice. Activează planul de continuitate operațională în situații de criză.

5. Protejarea drepturilor digitale, formare și conștientizare

Compania respectă legislația privind protecția datelo și asigură un mediu de lucru digital sigur, prin:
• Monitorizarea accesului la date și sisteme;
• Informarea angajaților privind drepturile și obligațiile lor digitale precum și respectarea politicilor și procedurilor de securitate;
• Instruiri periodice pentru angajați privind riscurile cibernetice, utilizarea responsabilă a tehnologiei și protecția datelor.

6. Utilizarea comunicațiilor electronice

Emailul și internetul sunt utilizate exclusiv în scopuri profesionale. Activitățile sunt monitorizate pentru prevenirea riscurilor cibernetice.

7. Raportarea incidentelor de securitate

Orice incident (tentativă de acces neautorizat, pierderi de date etc.) trebuie raportat imediat superiorului direct sau echipei de securitate IT.

8. Transferul de date confidențiale

• Datele confidențiale trebuie protejate și divulgate doar conform procedurilor interne.

9. Clasificarea informațiilor

Informațiile sunt clasificate astfel:
• Publice
• Interne
• Confidențiale
• Cu acces limitat.

10. Securitatea fizică

Accesul la echipamente IT și spații sensibile este controlat prin carduri de acces, sisteme de supraveghere video și autorizări stricte.

11.Lucrul de la distanță

Angajații care lucrează remote trebuie să respecte aceleași măsuri de securitate ca cei care lucrează din sediile companiei.

12. Managementul schimbărilor

Orice modificare adusă infrastructurii IT este documentată, testată și aprobată conform unui pro-ces controlat.

13. Auditarea sistemelor

Se efectuează audituri periodice pentru evaluarea conformității și identificarea vulnerabilităților.

14. Plan de urgență în caz de dezastru

Include proceduri de backup, testare a restaurării datelor și scenarii pentru menținerea activității în situații de criză.

15. Instruire și conștientizare

Angajații participă la sesiuni periodice de formare privind securitatea cibernetică și bunele practici.

16. Politica de sancțiuni

Încălcarea prevederilor politicii atrage sancțiuni disciplinare, care pot include și desfacerea contractului de muncă.

17. Managementul incidentelor
Se aplică proceduri clare pentru documentarea, investigarea și remedierea incidentelor de securitate, în scopul prevenirii reapariției acestora.

18. Lanțul valoric și furnizorii
Partenerii și furnizorii sunt încurajați să adopte standarde similare de securitate cibernetică și să respecte cerințele privind protecția datelor.

19. Revizuire și actualizare
Politica este revizuită anual și ori de câte ori apar schimbări legislative sau tehnologice relevante, pentru a reflecta angajamentul continuu față de sustenabilitate și conformitate.

20. Raportarea încălcărilor
Antibiotice SA încurajează raportarea oricăror situații care contravin principiilor și prevederilor prezentei Politici de Securitate Cibernetică. Orice sesizare referitoare la nerespectarea acestei politici poate fi transmisă prin următoarele canale:
• Direct **superiorului ierarhic**, în cazul angajaților.
• Către **Echipa de Răspuns la Incidente** prin acest formularul de contact de pe site.

Toate reclamațiile sunt analizate în conformitate cu procedurile interne de gestionare a incidentelor și sunt tratate cu promptitudine, echitate și profesionalism.

Antibiotice a+