Politica de securitate a informației

Scop și domeniu de aplicare	Prezenta politică stabilește angajamentul conducerii INFOtreat SRL și Infotreat Health-Services SRL de a proteja confidențialitatea, integritatea și disponibilitatea informațiilor pe care le deținem și le prelucrăm, în special datele cu caracter personal ale pacienților, inclusiv date privind sănătatea, prelucrate în cadrul serviciilor de raportare pe care le furnizăm. Informațiile sunt active ale afacerii cu o mare valoare pentru dezvoltarea durabilă a organizației, iar protejarea lor corespunzătoare asigură continuitatea afacerii și reduce riscul organizațional. Scopul politicii este protejarea bunurilor informaționale împotriva tuturor amenințărilor, interne sau externe, deliberate sau accidentale: acces neautorizat, modificare, divulgare sau distrugere. Politica se aplică tuturor activităților societăților, atât resursei umane, cât și celei materiale, în conformitate cu „Declarația de aplicabilitate” și cu domeniul de aplicare al SMSI, precum și angajaților, colaboratorilor, contractorilor și furnizorilor care au acces la informațiile organizației.
Context și obiective	INFOtreat SRL și Infotreat Health-Services SRL administrează raportarea tranzacțiilor farmaciilor privind reducerile acordate pacienților de producătorii de medicamente prin card. Având în vedere natura datelor prelucrate și contextul actual al pieței, securitatea informației este o prioritate a conducerii. **Obiectivul general** al securității informației este de a asigura continuitatea afacerii și de a minimiza daunele aduse acesteia, prin identificarea și tratarea riscurilor, prevenirea incidentelor de securitate și minimizarea impactului lor. Obiectivele specifice de securitate a informației sunt stabilite anual, sunt măsurabile, aliniate la strategia organizației și monitorizate în cadrul analizei efectuate de management.
Angajamentul conducerii	Politica este aprobată de management și reflectă angajamentul conducerii de a: • respecta cerințele legale, de reglementare și contractuale aplicabile, inclusiv Regulamentul (UE) 2016/679 („GDPR”); • implementa, menține și îmbunătăți continuu un Sistem de Management al Securității Informației (SMSI), certificat conform ISO/IEC 27001:2022 (inclusiv Amendamentul 1:2024), și a asigura resursele necesare funcționării acestuia; • gestiona riscurile de securitate a informației pe baza unei evaluări documentate a riscurilor.

Procese specifice	Evaluarea riscului a fost efectuată luând în considerare amenințările interne și externe, deliberate sau accidentale, precum și vulnerabilitățile care pot fi exploatate. Pentru securitatea informațiilor sunt implementate următoarele procese cheie: • identificarea și evaluarea resurselor organizației din punctul de vedere al importanței lor; • evaluarea riscului de pierdere a confidențialității, integrității și disponibilității informațiilor, pe baza amenințărilor și vulnerabilităților identificate; • tratarea și managementul riscurilor; • implementarea măsurilor de securitate pe baza controalelor din ISO/IEC 27002:2022 și a politicilor tematice aplicabile (control acces, criptare, copii de siguranță etc.); • aplicarea GDPR: legalitate, limitarea scopului, minimizarea datelor și securitatea prelucrării; • instruirea și conștientizarea personalului angajat; • evaluarea, măsurarea și stabilirea de acțiuni corective și de îmbunătățire continuă, inclusiv abordarea riscurilor și oportunităților; • gestionarea incidentelor de securitate și a încălcărilor securității datelor cu caracter personal; • planul de continuitate a afacerii.
Furnizori și terți	Cerințele de securitate se stabilesc contractual și se verifică periodic pentru furnizorii și partenerii care au acces la informațiile organizației sau le prelucrează, inclusiv furnizorii de servicii IT și cloud.
Schimbări climatice și reziliență	În cadrul analizei contextului organizației și al managementului riscurilor sunt evaluate efectele relevante ale schimbărilor climatice și ale fenomenelor meteorologice extreme asupra securității informației și continuității activității. Evaluarea are în vedere atât infrastructura și locațiile proprii, cât și serviciile și furnizorii critici, iar riscurile identificate sunt tratate, după caz, prin măsurile de securitate și planurile de continuitate și redresare aplicabile.
Incidente și continuitate	Incidentele de securitate și încălcările securității datelor cu caracter personal se raportează imediat Responsabilului SMSI și se gestionează conform procedurii dedicate, inclusiv cu respectarea termenelor legale de notificare. Planurile de continuitate a afacerii se testează periodic.
Responsabilități și autoritate	Responsabilul cu Sistemul de Management al Securității Informațiilor este investit cu autoritatea necesară conducerii SMSI, deciziile sale fiind luate cu sprijinul echipei de lucru SMSI, formată din personal special desemnat de Administrator. Administratorul INFOtreat SRL și Infotreat Health-Services SRL susține implementarea, funcționarea și îmbunătățirea SMSI și își asigură sprijinul personal în realizarea obiectivelor stabilite. Întregul personal trebuie să conștientizeze valoarea informațiilor din cadrul organizației, să le protejeze și să nu le folosească în scop personal sau în folosul unei terțe părți; în caz contrar, este pasibil de sancțiuni disciplinare și legale, după caz.

Comunicare și revizuire	Politica este comunicată, afișată și însușită de tot personalul, este disponibilă public pe site-ul www.infotreat.ro și este comunicată contractorilor cu ocazia semnării contractelor. Politica este revizuită cel puțin anual și ori de câte ori apar schimbări semnificative, pentru a se asigura că rămâne corespunzătoare, adecvată și eficace. Poate fi modificată sau completată ori de câte ori este necesar.

Întocmit: Ligia Ciureanu	**Data reviziei:** Revizia 7 – 01.10.2026	**Aprobat:** Cristian Nicolae, Administrator