



DECLARAȚIA PRIVIND POLITICA ÎN DOMENIUL SECURITĂȚII INFORMAȚIILOR

1. SCOP

Managementul de la cel mai înalt nivel consideră că informațiile sunt resurse care au o mare valoare pentru dezvoltarea durabilă a organizației. Protejarea corespunzătoare a informațiilor asigură continuitatea afacerii, reducerea riscului organizațional, creșterea profitului și a oportunităților de afaceri.

Prin administrarea informațiilor în conformitate cu cerințele standardului ISO 27001:2005, sunt protejate interesele S&T, ale clienților și partenerilor săi.

2. OBIECTIVE

Directorul S&T Romania este implicat personal și s-a angajat să dezvolte, să implementeze și să mențină un Sistem de Management al Securității Informațiilor pentru:

- Asigurarea continuității afacerii și minimizarea pierderilor ca urmare a apariției unor evenimente și incidente de securitate;
- Demonstrarea conformității cu standardul ISO/IEC 27001:2005 – “Sisteme de management pentru securitatea informațiilor”;
- Respectarea obligațiilor contractuale și legale în domeniul activităților specifice;
- Asigurarea și consolidarea reputației pe piață a organizației;
- Oferirea încrederii partenerilor de afaceri în ceea ce privește păstrarea confidențialității informațiilor procesate;
- Comunicarea politicii de securitate a informațiilor în interiorul organizației și terților;
- Demonstrarea adoptării celor mai bune practici în domeniul securității informațiilor.

3. DOMENIUL DE APLICARE

- Comercializare, consultanță, proiectare, dezvoltare, implementare, integrare, testare, întreținere, service, suport tehnic, instruire pentru: echipamente (hardware), sisteme, rețele și soluții de tehnologia informației și comunicații, software și licențe software, echipamente medicale; management de proiecte, outsourcing, activități legate de bazele de date.
- Intregul personal al S&T Romania.

4. PROCESE SPECIFICE

S&T Romania a efectuat evaluarea riscului luând în considerare amenințările interne, externe, deliberate sau accidentale existente, cât și vulnerabilitățile ce pot fi exploatare.

Pentru securitatea informațiilor s-au implementat următoarele procese cheie:

- Identificarea și evaluarea resurselor organizației în ceea ce privește importanța acestora;
- Evaluarea riscului de pierdere a confidențialității, integrității și disponibilității informațiilor pe baza identificării amenințărilor și vulnerabilităților;
- Tratarea și managementul riscului;
- Implementarea măsurilor de securitate în baza “Codului de practici pentru managementul securității informațiilor” - ISO/IEC 27002;
- Instruirea și conștientizarea personalului angajat;
- Evaluarea, măsurarea și stabilirea de acțiuni corective și preventive în scopul îmbunătățirii Sistemului de Management al Securității Informațiilor.

5. RESPONSABILITATE ȘI AUTORITATE

Responsabilul cu Sistemul de Management al Securității Informațiilor a fost investit cu autoritatea necesară conducerii sistemului de management al securității informațiilor, deciziile sale utilizând suportul Echipei de lucru SMSI.

Echipa de lucru SMSI este formată din personal special desemnat de Directorul S&T Romania.

Prin politica de securitate a informațiilor, Directorul S&T Romania susține implementarea, funcționarea și îmbunătățirea sistemului de management al securității informațiilor și asigură suportul său personal în realizarea obiectivelor stabilite.

Întregul personal trebuie să conștientizeze valoarea informațiilor din cadrul organizației, să protejeze și să nu folosească informațiile pentru uzul personal sau al unei terțe părți, în caz contrar fiind pasibili de sancțiuni disciplinare și legale, după caz.

Politica de securitate a informațiilor va fi revizuită la intervale planificate sau în cazul unor schimbări semnificative, pentru a se asigura că aceasta este, în continuare, corespunzătoare, adecvată și eficace.

Director General,

Bogdan Cocora