Politicile de securitate a informației

Crearea și implementarea politicilor de securitate a informațiilor (PSI) poate părea o formalitate pentru unele organizații. Cu toate acestea, PSI-urile pot forma coloana vertebrală a poziției de securitate a datelor organizației. Politicile și procedurile de securitate a informațiilor asigură prevenirea compromiterii datelor sensibile și protejarea reputației și finanțelor prin definirea a ceea ce este permis și a ceea ce nu este permis în cadrul organizației. O PSI bine proiectată poate îmbunătăți nivelul de securitate a organizației, figura 1.



Figura 1 – Beneficiile Politicii de securitate într-o organzație

[Ani Khachatryan, 10 Information Security Policies Every Organization Should Implement, 2023,

<https://www.ekransystem.com/en/blog/information-security-policies>]

* 1. **Reguli clare de securitate a datelor.** O IPSI oferă angajaților linii directoare clare pentru manipularea informațiilor sensibile în cadrul organizației. Acest lucru poate ajuta la îmbunătățirea gradului de conștientizare generală a securității cibernetice și la reducerea numărului de amenințări interne neintenționate.
  2. **Controale adecvate de securitate cibernetică.** Prin definirea obiectivelor de securitate, o PSI poate ajuta ofițerii de securitate să implementeze soluții software adecvate și să implementeze măsuri de securitate relevante pentru a le atinge.
  3. **Răspuns rapid și eficient la incidentele de securitate**. Prin prezentarea acțiunilor pas cu pas de răspuns la incident,PSI poate ajuta echipa de securitate cibernetică să abordeze în mod proactiv potențialele riscuri și vulnerabilități. Prin urmare, organizația poate răspunde prompt la incidentele de securitate și poate atenua posibilele consecințe.
  4. **Capacitatea de a îndeplini cerințele de conformitate IT**. O PSI poate ajuta organizația să respecte SWIFT CSP, GDPR, SOX și alte standarde, legi și reglementări. De asemenea, merită menționat faptul că a avea o politică de securitate a informațiilor este o cerință în sine pentru standarde și legi precum HIPAA, PCI DSS și ISO 27001.
  5. **Responsabilitatea utilizatorilor și a părților interesate**. Când definesc în mod clar rolurile și responsabilitățile pentru fiecare utilizator și parte interesată din cadrul organizației, PSI poate ajuta angajații să înțeleagă responsabilitatea lor în protejarea informațiilor sensibile. PSI poate promova, de asemenea, un sentiment de proprietate și responsabilitate în rândul utilizatorilor și părților interesate, rezultând o responsabilitate sporită.
  6. **Reputație îmbunătățită.** Un angajament față de standardele și practicile de securitate a informațiilor stimulează încrederea în rândul clienților. În plus, PSI ajută la reducerea numărului de incidente de securitate a datelor, crescând în continuare loialitatea clienților și percepția pozitivă a organizației.
  7. **Eficiență operațională sporită.** Avand politici clare în vigoare, organizația poate ajuta să își mențină eforturile de protecție a datelor standardizate, consecvente și sincronizate. În acest fel, echipa de securitate cibernetică va petrece mai puțin timp și mai puțin efort abordând problemele de securitate cibernetică.

**Destul de des politicile de securitate a informației sunt scrise prea detaliat, încercând să acopere totul, de la obiective strategice până la câte cifre numerice ar trebui să conțină o parolă. Singura problemă cu astfel de politici este că ele conțin 50 sau mai multe pagini și – nimeni nu le ia în serios. Ele ajung de obicei să servească drept documente artificiale al căror singur scop este satisfacerea auditorului.**

**Pentru implementarea unui SMSI (ISO 27001) sau a unui programde securitate (NIST SP 800-12), ar fi potrivite următoarele opțiuni:**

**O1: Toate politicile de securitate a informațiilor ar putea fi îmbinate într-un singur document - Politica de securitate a informațiilor**

**O2: Se scrie separat *Politica de securitate a informațiilor de nivel superior* și *Politica de securitate a informațiilor operaționale*, care să acopere majoritatea controalelor (garanțiilor) din anexa A.**

**Aceste opțiuni sunt potrivite dacă compania este foarte mică (mai puțin de 10 angajați), în special pentru a reduce numărul de documente.**

**O3: Deoarece, pe de o parte nu este fezabil să se pună toate regulile de securitate într-o singură politică, iar pe de altă parte, acest lucru duce la un document excesiv de mare, pe care nimeni nu vrea să-l citească, cu atât mai puțin să se conformeze acestuia, cea mai bună opținune este să existe separat o Politică Generală de securitate a informațiilor și diferite domenii, de exemplu din anexa A ISO 27001, să fie acoperite prin diferite documente:**

* **Politica de clasificare a informației**
* **Politica privind utilizarea acceptabilă a activelor informaționale**
* **Politica copiilor de rezervă**
* **Politica de control al accesului**
* **Politica privind utilizarea parolelor**
* **Politica pentru birou și ecran curat**
* **Politica privind utilizarea serviciilor de rețea**
* **Politica privind utilizarea dispozitivelor mobile**
* **Politica privind utilizarea controalelor criptografice etc.**

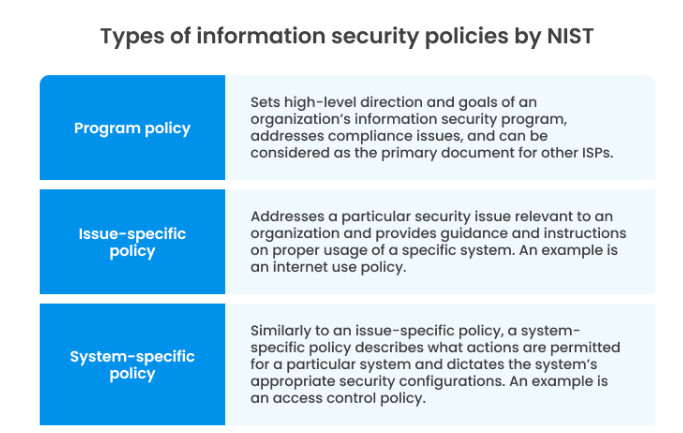
**Astfel de politici sunt mai scurte (și, prin urmare, mai ușor de citit și de înțeles) și mai ușor de întrețin (de exemplu, administratorul de sistem va fi responsabil pentru politica de backup, în timp ce managerul de securitate va fi responsabil pentru politica de clasificare a informației etc.).**

**Pentru diferite aspecte ale SMSI și diferite „grupuri țintă” ar trebui să existe politici diferite. Organizațiile mijlocii construiesc de obicei *până la 15 politici* pentru ISMS.**

**Standardele totuși nu cer implementarea și/sau documentarea tuturor acestor politici, deoarece decizia dacă aceste controale sunt aplicabile în organozație și în ce măsură depinde de rezultatele evaluării riscurilor.**

**O politică își va arăta valoarea – dacă nu imediat, atunci probabil în doi sau trei ani, prin scăderea numărului de incidente, doar dacă este scrisă cu intenția de a reduce riscurile. Cu siguranță politicile scrise doar având în vedere auditul de certificare nu vor aduce decât mai multe costuri și mai multă birocrație.**

**NIST SP 800-12 definește următoarele tipuri de politici de securitate a informațiilor, figura 2:**

****

**Figura 2 - Tipuri de politici de securitate a informațiilor după NIST**

**Politici la nivel înalt, cum ar fi *Politica generală de securitate a informațiilor* – astfel de politici la nivel înalt definesc de obicei intenția strategică, obiectivele etc. și ar trebui să fie utilizată de aproape fiecare angajat cu scopul principal de a se asigura că activitățile lor de zi cu zi respectă regulile de securitate.**

**Politici detaliate sau specifice (unei probleme sau unui sistem) – acest tip de politică descrie de obicei un domeniu selectat de securitate a informațiilor mai detaliat, cu responsabilități precise etc.**

***Politica generală de securitate a informațiilor* e**ste un document oficial care definește principiile, obiectivele și standardele unei organizații pentru protejarea informațiilor sale. Aceasta stabilește cadrul pentru implementarea controalelor de securitate și a altor măsuri pentru a proteja informațiile confidențiale, a asigura integritatea datelor și a menține disponibilitatea informațiilor pentru utilizatorii autorizați.

***Scopul Politicii generale de securitate a informațiilor***

**În multe cazuri, managerii de top nu au nicio idee despre modul în care securitatea informațiilor le poate ajuta organizația, așa că scopul principal al politicii este ca managementul de vârf să definească ceea ce dorește să realizeze cu securitatea informațiilor.**

**Al doilea scop este crearea unui document ușor de înțeles și cu ajutorul căruia se va putea controla tot ceea ce se întâmplă în cadrul unui sistem/program de securitate. Nu este necesar ca top-managementul să cunoască detaliile privind procedura de evaluare a riscurilor, managementul controlului accesului sau al copiilor de rezervă, dar trebuie să știe cine este responsabilii și care sunt așteptările.**

**ISO 27001 nu spune prea multe despre politică, dar următoarele aspecte sunt important de considerat:**

* **Politica trebuie adaptată la organizație – aceasta înseamnă că nu puteți pur și simplu să copiați politica de la o companie mare de producție și să o utilizați într-o companie IT mică.**
* **Trebuie să definească cadrul pentru stabilirea obiectivelor de securitate a informațiilor – în principiu, politica trebuie să definească modul în care sunt propuse obiectivele, cum sunt aprobate și cum sunt revizuite.**
* **Politica trebuie să arate angajamentul managementului de vârf de a îndeplini cerințele tuturor părților interesate și de a îmbunătăți continuu ISMS – acest lucru se realizează în mod normal printr-un fel de declarație în cadrul politicii.**
* **Politica trebuie comunicată în cadrul companiei, dar și – după caz – părților interesate (de exemplu, clienți și furnizori); cea mai bună practică este de a defini cine este responsabil pentru o astfel de comunicare, iar apoi acea persoană este responsabilă pentru a face acest lucru în mod continuu.**
* **Politica trebuie revizuită în mod regulat (de exemplu, anual) – trebuie definit proprietarul poliței, iar această persoană este responsabilă pentru menținerea la zi a politicii.**

***Conținutul unei Politici de securitate a informațiilor* include:**

* **obiective: obiectivele generale și specifice care trebuie atinse de securitatea informațiilor**
* **secțiunea cerințe: trimitere la cerințele legale, statutare și contractuale care trebuie îndeplinite;**
* **managementul riscurilor: referire la procesul de selectare a controalelor de securitate a informațiilor;**
* **responsabilități: d**escrie rolurile și responsabilitățile conducerii, angajaților și altor părți interesate în menținerea securității informației; **responsabilități pentru implementarea, întreținerea și raportarea performanței SMSI;**
* **comunicare: cui trebuie comunicată această politică**
* **suport: angajament cu resurse pentru implementarea și îmbunătățirea securității informațiilor**

**Deși nu este obligatoriu pentru companile mici, poate fi incluse și următoarele elemente (pentru companiile mai mari, acestea sunt de obicei documentate separat):**

* **Domeniul de aplicare,** specifică tipurile de informații protejate de politică și pe cine se aplică aceasta (angajați, contractori, furnizori etc.). **În acest fel domeniul de aplicare nu trebuie să existe ca document separat.**
* **Clasificarea informației:** definește diferite niveluri de clasificare a informației în funcție de sensibilitate (confidențial, secret etc.), daca nu există opolitică separată în acest sens.
* **Consecințe** – prezintă eventualele pierderi dacă politica nu va fi respectată.
* **Măsurare – cine va măsura dacă obiectivele de securitate a informațiilor au fost atinse, cui trebuie raportate rezultatele, cât de des etc.**
* **Monitorizare -** specifică modul în care se controlează/ auditează respectarea și actualizarea
* **Excepții** – menționează cazurile excepționale și modalitățile de tratare a lor; de regulă, au o durată limitată de aplicare.

**Din cele menționate mai sus este important să fie asigurate:**

* **Mijloace pentru a fi comunicat tuturor părților relevante (de exemplu, prin utilizarea de buletine informative, prezentări, traininguri etc.);**
* **Mijloace pentru ca politica să fie implementată și aplicată în cadrul tuturor elementelor necesare (de exemplu, oameni, sisteme, facilități etc.) în domeniul său de aplicare;**
* **Mijloace de evaluare a performanței (de exemplu, prin utilizarea indicatorilor cheie de performanță, monitorizare și măsurare);**
* **Mijloace de a furniza dovezi ale aplicării și rezultatelor acesteia (de exemplu, utilizarea jurnalelor și a rapoartelor);**
* **Mijloace de a asigura revizuirea acestuia (de exemplu, după timp, după eveniment etc.).**

**La elaborarea Politicii de securitate a informației la nivel înalt, este bine de considerat intențiile top managementului privind securitatea informațiilor. Se recomandă să fie realizat un interviu cu CEO-ul companiei și să fie parcurse toate elementele politicii. Până la interviu e bine ca CEO-ul să obțină documentul ca să reușească să-l studieze.**

Politica de securitate a informației **la nivel înalt** este un document esențial pentru orice organizație care dorește să își protejeze informațiile sensibile. Implementarea unei politici eficiente de securitate a informației poate ajuta organizațiile să gestioneze riscurile de securitate cibernetică, să respecte legile și reglementările și să își construiască încrederea cu clienții, partenerii și angajații.

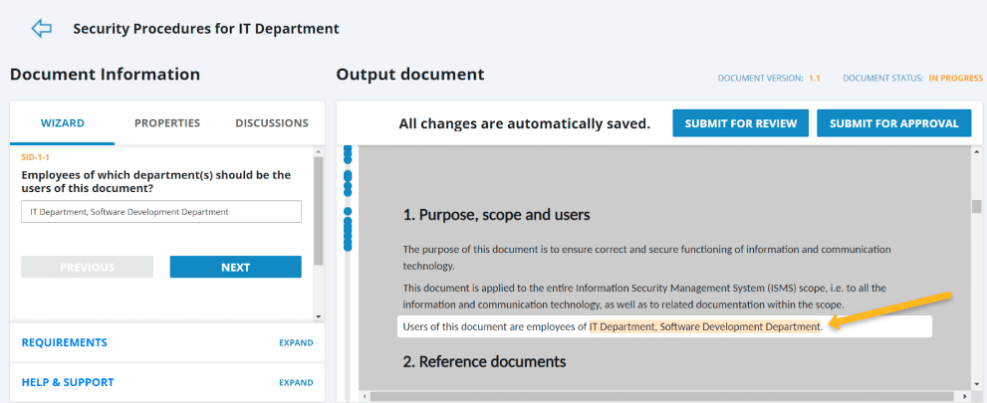
Politicile de securitate **detaliate** sunt implementate eficient prin intermediul controalelor tehnice, fizice și/sau umane, în conformitate cu scopurile propuse:

* **Controalele tehnice** sunt implementate în primul rând în sistemele informaționale, prin intermediul componentelor software, hardware și firmware adăugate sistemelor, de exemplu, backup, software antivirus etc.
* **Controalele fizice** sunt implementate în primul rând prin intermediul echipamentelor sau dispozitivelor care au o interacțiune fizică cu oameni și obiecte, de exemplu, camere CCTV, sisteme de alarmă, încuietori etc.
* **Controalele resurselor umane** sunt implementate prin intermediul activităților de conștientizare, instruire și educație, de exemplu, formare de conștientizare a securității, instruire pentru auditori interni ISO 27001, educație academică etc.

Politicile de securitate a informației trebuie să fie ușor accesibile și ușor de înțeles de către toți angajații, să fie comunicată clar tuturor angajaților și trebuie să se ofere instruiri privind securitatea informației, trebuie să fie revizuită și actualizată periodic pentru a reflecta noile amenințări și tehnologii.

Astazi companiile au posibilitatea să utilizeze soluții și platforme software specializate pentru a obține asistență în elaborarea politiciilor de securitate și nu doar:

* **Conformio**, în baza informațiilor despre companie, riscuri, legi, reglementări și contracte sugerează automat politici și proceduri. Asigura un proces de gestionare automatizată a politicilor de securitate care implică o mulțime de activități precum: colectarea datelor, analiza datelor, scrierea, coordonarea, revizuirea, aprobarea și distribuirea documentelor,figura 3;
* **Information Shield**, ;
* **ISMS Online** [https://www.isms.online/];
* Compliance Forge [].

****

**Figura 3 – [https://advisera.com/conformio/]**

**[Rhand Leal, How to automate an ISO 27001 security policy, https://advisera.com/articles/how-to-automate-an-iso-27001-security-policy/]**

**Indiferent de opțiunea aleasă sau instrumentele utilizate, Politica trebuie să țină cont de circumstanțele particulare ale companiei, să fie dezvoltată ca atare și să să funcționeze pentru obicetivele de securitate ale companiei.**

Pe nivelul inferior al politicilor de securitate se află trei elemente de simplificare a implementării politicilor: **standardele sau liniile directoare** (de obicei sunt obligatorii și **specifică tehnologiile și metodologiile pentru securizarea datelor și sistemelor**), **normele** (acțiuni recomandate, nu obligatorii) și **procedurile** (oferă cele mai mici detalii pentru **pentru îndeplinirea sarcinilor legate de securitate**). Ele conțin detaliile politicii sau metodologii ale sistemelor securizate, cum ar fi posibilitățile de implementare, ce standarde și proceduri să fie întrebuințate. Ele sunt făcute publice la nivel de organizație, prin manuale, Intranet, cărți, cursuri ș.a.

|  |
| --- |
| *Model de Politica de Securitate a Informației (O1)* ***1. Introducere***  *Acest document stabilește Politica de Securitate a Informației a [Numele Organizației] („Organizația”). Politica definește principiile, obiectivele și standardele Organizației pentru protejarea informațiilor sale confidențiale, asigurarea integrității datelor și menținerea disponibilității informațiilor pentru utilizatorii autorizați.*  ***2. Scop***  *Scopul acestei Politici este de a proteja activele informaționale ale Organizației și de a gestiona riscurile de securitate cibernetică. Politica stabilește cadrul pentru implementarea controalelor de securitate și a altor măsuri pentru a asigura confidențialitatea, integritatea și disponibilitatea informației.*  ***3. Domeniu de Aplicare***  *Această politică se aplică tuturor angajaților, contractorilor, furnizorilor, partenerilor de afaceri și altor părți terțe care accesează sau procesează informațiile Organizației.*  ***4. Responsabilități***   * ***Conducerea:****Conducerea Organizației este responsabilă pentru aprobarea și implementarea acestei Politici, precum și pentru alocarea resurselor necesare pentru menținerea securității informației.* * ***Managerul Securității Informației:****Managerul Securității Informației (MSI) este responsabil pentru dezvoltarea, implementarea și menținerea programului de securitate a informației al Organizației.* * ***Angajații:****Toți angajații sunt responsabili pentru respectarea acestei Politici și pentru raportarea oricăror incidente de securitate suspectate.* * ***Utilizatorii Autorizați:****Toți utilizatorii autorizați ai informațiilor Organizației sunt responsabili pentru utilizarea informațiilor în mod corespunzător și pentru păstrarea confidențialității acestora.*   ***5. Clasificarea Informației***  *Informațiile Organizației sunt clasificate în funcție de sensibilitate în următoarele categorii:*   * ***Confidențial:****Informație care, dacă este dezvăluită neautorizat, ar putea cauza daune semnificative Organizației.* * ***Intern:****Informație destinată utilizării interne a Organizației.* * ***Public:****Informație care poate fi pusă la dispoziția publicului.*   ***6. Controale de Securitate***  *Organizația implementează o varietate de controale de securitate pentru a proteja informațiile sale. Aceste controale includ:*   * ***Controlul accesului:****Se acordă acces la informații doar utilizatorilor autorizați, pe baza principiului necesității minime.* * ***Managementul parolelor:****Se impun cerințe minime pentru crearea și utilizarea parolelor puternice.* * ***Utilizarea computerului și a rețelei:****Se stabilesc reguli privind utilizarea echipamentelor IT și a rețelei corporative, inclusiv interzicerea activităților personale pe echipamentele de lucru.* * ***Securitatea datelor:****Se implementează măsuri pentru protejarea datelor în stare de repaus și în tranzit, cum ar fi criptarea.* * ***Securitatea fizică:****Se implementează măsuri pentru protejarea fizică a echipamentelor și a spațiilor care stochează informații.* * ***Monitorizare și raportare:****Se monitorizează activitatea de pe rețea și se raportează incidentele de securitate suspectate.*   ***7. Conștientizarea Securității Informației***  *Organizația oferă programe de instruire privind securitatea informației pentru toți angajații și utilizatorii autorizați. Instruirea îi ajută pe angajați să înțeleagă politicile de securitate ale Organizației, riscurile de securitate cibernetică și cele mai bune practici pentru protejarea informațiilor.*  ***8. Gestionarea Incidentelor de Securitate***  *Organizația are un plan de răspuns la incidente care definește procesul de identificare, raportare, investigare și remediere a incidentelor de securitate cibernetică.*  ***9. Audituri și Revizuiri***  *Organizația efectuează periodic audituri și revizuiri ale programului său de securitate a informației pentru a evalua eficacitatea acestuia.*  ***10. Îmbunătățire Continuă***  *Organizația se angajează să își îmbunătățească continuu programul de securitate a informației pe baza noilor amenințări și a experien* |