Aprobat
Director general

CLASIFICAREA INFORMATIEI

Cod: SI-01-1.0

Data aprobarii procedurii: 05.04.2023

Intocmit: RMI	**Data reviziei :**
Semnatura:	

1 Scop

Scopul acestui document este de a prezenta modul de clasificare a informatiei in cadrul SMART MERCHANDISING . Conform ISO/IEC 27001:2017 informatiile trebuiesc clasificate in functie de valoare, cerinte legale, importanta si nivel critic pentru organizatie.

2 Domeniu de aplicare

Aceasta procedura se aplica pentru toate categoriile de informatii din cadrul SMART MERCHANDISING , indiferent de:

- Forma : analogice sau digitale;
- Natura: date numerice (fisiere de date, baze de date, foi de calcul), documente , fisiere imagine, secvente audio, secvente video;
- Suport: magnetic , optic (CD/DVD), opac (hartie, folii,etc.).

3 Documente de referinta

Manualul de management integrat, revizia in vigoare.

4 Definitii si prescurtari

Termenii utilizati in prezenta procedura sunt definiti in Manualul de management integrat, revizia in vigoare.

Clasificarea informatiei - modalitatea prin care se asigura tratarea consecventa a informatiei de catre toate persoanele care intra in contact cu aceasta.

5 Procedura

Conform ISO/IEC 27001:2017 informatiile trebuie clasificate in funcție de valoare, cerinte legale, importanta si nivel critic pentru organizatie. Recomandarile standardului ISO/IEC 27002 pentru clasificarea informatiilor pot fi sintetizate in urmatoarele cerinte:

- Clasificarea informatiei trebuie sa tina cont de necesitatile obiective de protejare a informatiei rezultate din specificul organizatiei si de impactul pe care divulgarea, utilizarea neautorizata sau distrugerea unui tip de informatie il poate avea asupra sa.
- Nivelul de protectie al informației trebuie analizat in contextul profilului CID (**C**onfidentialitate, **I**ntegritate, **D**isponibilitate) asociat.
- Regulile de manevrare si masurile de control al securitatii informatiei trebuie stabilite pe baza clasificarii informatiei.
- Conducerea organizatiei trebuie sa revizuiasca periodic clasificarea informatiei in conformitate cu politicile de acces stabilite. Cu aceasta ocazie conducerea organizatiei poate decide schimbarea incadrarii intr-o alta categorie a unei de informatii care datorita trecerii timpului nu mai este critica.
- Responsabilitatea pentru modul de incadrare a unei informatii intr-o anumita categorie, si pentru revizuirea periodica a modului de incadrare a unei informatii intr-o anumita categorie, se afla in sarcina proprietarului desemnat al informatiei.
- Clasificarea trebuie sa tina cont de efectul de agregare, care face ca o cantitate mare de informatii cu nivel de risc mic sa produca prin agregare un risc de nivel superior.
- Atunci cand sunt partajate informatii cu terte organizatii, trebuie stabilite masuri de eliminare a unor posibile confuzii de manipulare datorate unor etichete cu denumire similara dar semnificatie diferita in cadrul fiecareia dintre organizatii.
- Proprietarii de informatie vor urmari ca operarea informatiilor din fiecare categorie de clasificare, sa fie facute astfel incat sa acopere, dupa caz, urmatoarele tipuri de prelucrari: creare/modificare, copiere, stocare, transmiterea prin posta, fax si posta electronica, transmiterea verbala, incluzand cea prin telefon mobil, mesagerie vocala, robot telefonic, declasificare, distrugere.

- Incadrarea resurselor de informatie cu cerinte de securitate similare in categoriile de clasificare este recomandabila pentru ușurarea procesului de clasificare.

Sistemele de clasificare a informatiei nu trebuie sa fie complicate dar trebuie sa existe si sa fie tratate standard in sensul de consecvent. Pentru a tine informatia sub control si pentru a diminua riscurile de manipulare a acesteia trebuie elaborat un model de clasificare.

Procesul de elaborare a unui model de clasificare a informatiilor presupune:

- identificarea categoriilor de informatii/ resurse de informatie
- analiza comportamentului informatiilor/resurselor de informatie
- definirea unui model de clasificare adecvat necesitatilor obiective ale organizatiei

In functie de cat de critica este pentru organizatie, fiecare categorie de informatie trebuie sa aiba asociat un nivel de risc de securitate si fiecare nivel de risc de securitate trebuie sa aiba definite masuri adecvate de control al riscului de securitate.

Este mai putin important cate niveluri de risc de securitate sunt definite pentru informatie, sau cum se numesc acestea. Este extrem de important insa ca modelul de clasificare adoptat sa reflecte necesitatile obiective ale organizatiei.

Modelul care este implementat in cadrul SMART MERCHANDISING este cel cu 4 niveluri de securitate:

- Informatii publice
- Informatii de uz intern
- Informatii confidentiale
- Informatii secret de serviciu

Informatiile publice sunt informatiile nerestrictionate. Sunt disponibile publicului larg, pe baza acestora firma facandu-si publicitate si oferind posibililor client posibilitatea de a afla informatiile de baza despre companie si serviciile pe care le ofera. Cel mai bun exemplu pentru astfel de inforamtii sunt datele de pe site-ul web al firmei.

Informatiile din acest nivel trebuie sa fie publice fara ca acest lucru sa genereze implicatii asupra organizatiei. Integritatea informatiilor nu este in acest caz vitala. Atacurile din exterior pot fi considerate riscuri acceptabile chiar daca afecteaza serviciile oferite de sistem.

Pentru aceasta clasa cerintele de securitate nu au la baza un anumit standard, recomandarile fiind „de bun simt', urmare a experientei practice. Recomandarile se rezuma la un minim de cerinte care trebuie respectate insa de orice organizatie. Acest lucru este impus de faptul ca si pentru aceasta clasa de informatii trebuie sa existe un nivel minim de securitate, in caz contrar existand bresa ce ar putea reprezenta punctul de intrare al atacurilor catre sistemele critice din organizatie. Cerintele minimale recomandate sunt: scanare antivirus, asigurarea protectiei site-ului web, verificarea informatiilor clasificate ca fiind publice.

Informatiile de uz intern reprezinta informatiile procesate in companie in cadrul diferitelor compartimente functionale pentru care accesul direct, neautorizat, trebuie prevenit. Accesul intern, de la angajatii companiei, la aceste date trebuie sa fie permis. in masura in care, din diferite cauze, aceste date devin publice acest lucru nu va determina consecinte critice. Integritatea acestor date este importanta dar nu vitala. Exemple de astfel de informatii : procedurile interne ale companiei, contractele cu clientii, contractele cu furnizorii, etc.

Accesul din extern la aceste informatii trebuie restrictionat. Considerant informatiile electronice care sunt stocate pe un server intern al companiei, accesul la acestea va trebui garantat doar pentru angajatii companiei (prin drepturi de acces). Documentele tiparite trebuiesc tinute in cadrul sediului, persoanele externe neavand acces direct la acestea.

Informatiile confidentiale sunt confidentiale in cadrul organizatiei si protejate fata de accesul extern. Exemple pot fi : informatii strategice ale companiei, ,date privind salariile, date de personal, date contabile, parole, informatii despre punctele slabe ale companiei, date despre clientii confidentiali ,etc. Afectarea confidentialitatii acestora ca urmare a unui acces neautorizat poate afecta eficienta operationala a organizatiei,

poate genera pierderi financiare si oferi un avantaj competitorilor sau o scadere importanta a increderii clientilor. De data aceasta integritatea datelor este vitala.

Pentru aceasta clasa se recomanda protejarea accesului controlat si securizarea transmisiilor de date. Astfel accesul la informatiile in format electronic va trebui acordat doar personalului care are acest privilegiu (management-ul companiei) , iar documentele tiparite vor trebui tinute "sub cheie".

Informatiile secret de serviciu sunt informatiile primite de la colaboratori, necesare pentru proiectele desfasurate de SMART MERCHANDISING . Fiind informatii cu o importanta sporita, acestea nu sunt decat in format tiparit. Transferul de astfel de informatii se face prin institutii specializate in acest domeniu (ex. : posta militara). Acestea sunt pastrate in cadrul firmei, in biroul directorul general, intr-un seif metatlic. Doar directorul general are acces la acestea si doar el poate delega persoanele care au access la ele. Informatiile nu vor parasi biroul directorului general.

Clasificarea informatiilor va trebui evidentiata pe fiecare document al SMART MERCHANDISING . Astfel, documentele de uz intern si confidentiale vor fi catalogate astfel prin imprimarea in head-erul fiecarei pagini a acestei clasificari. Documentele publice nu vor fi marcate in niciun fel (nu este necesar deoarece acestea vor fi transmise la oameni din afara companiei). Cele secret de servicui nu vor fi catalogate , nefiind utilizate nicaieri in afara biroului directorului general (de obicei acestea vor fi etichetate de catre entitatile de la care vor fi primite).

Pentru implementarea unui model de clasificare a informatiei, pentru fiecare categorie, este necesara stabilirea regulilor pentru etichetarea, salvarea, transmiterea, eliminarea, protejarea integritatii informatiei precum si drepturile de acces si de divulgare a acesteia.

Ce trebuie subliniat este faptul ca, in cadrul unui model de clasificare stabilit, incadrarea unei informatii intr-o categorie de clasificare nu este definitiva si ca ea poate suferi modificari conform politicilor stabilite de organizatie. Atunci cand o informatie inceteaza sa fie critica pentru organizatie, dupa o perioada de timp stabilita, ea poate fi incadrata intr-o alta categorie, de exemplu, poate fi facuta publica. Operatia poarta numele de declasificare.

Responsabilitatea utilizatorului este foarte importanta. In acest sens modul de clasificare a informatiilor si modul de manipulare a acestora va fi adus la cunostinta fiecaruia.

6 Responsabilitati

6.1. Director general

6.1.1. Verifica periodic respectarea procedurii de clasificare a informatiilor.

6.1.2. Aproba accesul anumitor angajati la informatiile clasificate.

6.1.3. Modifica clasificarea unui document in momentul schimbarii nivelului acestuia.

6.2. RSMSI

6.2.1. Analizeaza si clasifica fiecare document.

6.2.2. Verifica periodic valabilitatea clasificarii documentelor.

6.2.3. Propune Directorului General modificarea nivelului de clasificare a unui document in cazul in care acest lucru este necesar.

6.2.4. Aduce la cunostinta angajatilor modificarile aparute asupra clasificarii informatiilor.

7 Inregistrari

- F-SI-01-01 Fisa de evidenta a modificarilor clasificarii informatiilor

Modificare			Data	Semnătura
Denumire document modificat	**Clasificare inaintea modificării**	**Clasificare dupa modificării**		

INTOCMIT:
RSMSI

Data: