**Politica de Securitate a Băncii MAIB**



|  |  |
| --- | --- |
| Code: |  |
| Version: | 1.1 |
| Date of version: | 26.10.2022 |
| Created by: | Plugaru Victoria, Cucta Maria, Cebotari Dan, Golan Grigore |
| Approved by: | lect. univ. Bulai Rodica |
| Confidentiality level: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| 24.10.2022 | 1.0 | Plugaru Victoria, Cucta Maria, Cebotari Dan, Golan Grigore | Schița de bază a documentului |
| 26.10.2022 | 1.1 | Plugaru Victoria, Cucta Maria, Cebotari Dan, Golan Grigore | Modificări aduse în compartimentul ”Terminologia de bază de securitate a informațiilor” și ”Gestionarea securității informaționale” |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[SCOP, OBIECTIVE ȘI UTILIZATORI 3](#_Toc117666800)

[DOCUMENTE DE REFERINTA 3](#_Toc117666801)

[TERMINOLOGIA DE BAZĂ DE SECURITATE A INFORMAȚIILOR 4](#_Toc117666802)

[GESTIONAREA SECURITĂȚII INFORMAȚIILOR 4](#_Toc117666803)

[OBIECTIVE ȘI MĂSURARE 4](#_Toc117666804)

[CERINȚE DE SECURITATE A INFORMAȚIILOR 5](#_Toc117666805)

[CONTROALE DE SECURITATE A INFORMAȚIILOR 5](#_Toc117666806)

[CONTINUITATEA AFACERII 5](#_Toc117666807)

[RESPONSABILITĂȚI 6](#_Toc117666808)

[COMUNICARE POLITICĂ 6](#_Toc117666809)

[SPRIJIN PENTRU IMPLEMENTAREA ISMS 6](#_Toc117666810)

[VALIDITATEA ȘI GESTIONAREA DOCUMENTULUI 7](#_Toc117666811)

# SCOP, OBIECTIVE ȘI UTILIZATORI

Scopul acestei politici de nivel superior este de a defini scopul, direcția, principiile și regulile de bază pentru managementul securității informațiilor.

Obiectivele sunt:

* utilizarea în siguranță a cardurile de plată
* utilizarea sigură a bancomatelor
* utilizarea sigură a Internet Banking-ului
* utilizarea sigură a sistemului informațional intern
* utilizarea tranzacțiilor internaționale în siguranță

Obiectivele specifice ale unui ISMS:

* Identificarea și evaluarea riscurilor informaționale
* Introducerea și dezvoltarea unui sistem de management al riscului
* Identificarea informațiilor care necesită protecție
* Dezvoltarea măsurilor de protecție
* Stabilirea unei conștientizări a importanței securității în companie
* Îmbunătățirea continuă a măsurilor (ciclul PDCA)

Această politică se aplică întregului Sistem de management al securității informațiilor (ISMS) din domeniul financiar-bancar, așa cum este definit în Documentul de aplicare al ISMS.

Utilizatorii acestui document sunt toți angajații bancii MAIB, precum și părțile externe relevante.

# DOCUMENTE DE REFERINTA

* ISO/IEC 27001 standard
* ISMS Scope Document
* Risk Assessment and Risk Treatment Methodology
* Statement of Applicability
* List of Legal, Regulatory and Contractual Obligations
* Legea privind activitatea băncilor nr. 202 din 06.10.2017
* [Hotărâre pentru aprobarea Regulamentului cu privire la standardele tehnice de reglementare a supravegherii suplimentare a conglomeratelor financiare nr.31 din 13.02.2020](https://www.bnm.md/ro/content/hotarare-pentru-aprobarea-regulamentului-cu-privire-la-standardele-tehnice-de-reglementare)
* [Regulamentul cu privire la cerinţele de publicare a informaţiilor de către bănci, aprobat prin Hotărârea Comitetului executiv al Băncii Naţionale a Moldovei nr.158 din 9 iulie 2020](https://www.bnm.md/ro/content/regulamentul-cu-privire-la-cerintele-de-publicare-informatiilor-de-catre-banci-aprobat-prin)
* [Regulament privind tranzacţiile băncii cu persoanele sale afiliate, aprobat prin HCA al BNM nr.240/2013](https://www.bnm.md/ro/content/regulament-cu-privire-la-expunerile-mari-aprobat-prin-hca-al-bnm-nr240-din-09122013)
* [Regulament cu privire la tratamentul riscului operațional pentru bănci potrivit abordării de bază și abordării standardizate](https://www.bnm.md/ro/content/regulamentul-cu-privire-la-tratamentul-riscului-operational-pentru-banci-potrivit-abordarii)
* Legea privind protecția datelor cu caracter personal nr. 133 din 08.07.2011

# TERMINOLOGIA DE BAZĂ DE SECURITATE A INFORMAȚIILOR

Confidențialitate – caracteristică a informațiilor prin care acestea sunt disponibile numai persoanelor sau sistemelor autorizate.

Integritate – caracteristică a informațiilor prin care acestea sunt modificate numai de către persoane sau sisteme autorizate într-un mod permis.

Disponibilitate – caracteristică a informațiilor prin care poate fi accesată de către persoanele autorizate atunci când este nevoie.

Securitatea informațională – garantarea confidențialității, integrității și disponibilității informațiilor.

Sistem de management al securității informațiilor – parte a proceselor generale de management care se ocupă de planificarea, implementarea, menținerea, revizuirea și îmbunătățirea securității informațiilor.

Date cu caracter personal – orice informaţie referitoare la o persoană fizică identificată sau identificabilă (subiect al datelor cu caracter personal). Persoana identificabilă este persoana care poate fi identificată, direct sau indirect, prin referire la un număr de identificare sau la unul ori mai multe elemente specifice identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale.

Consimţămîntul subiectului datelor cu caracter personal – orice manifestare de voinţă liberă, expresă şi necondiţionată, în formă scrisă sau electronică, conform cerinţelor documentului electronic, prin care subiectul datelor cu caracter personal acceptă să fie prelucrate datele care îl privesc.

Depersonalizarea datelor – modificarea datelor cu caracter personal astfel încît detaliile privind circumstanţele personale sau materiale să nu mai permită atribuirea acestora unei persoane fizice identificate sau identificabile ori să permită atribuirea doar în condiţiile unei investigaţii care necesită cheltuieli disproporţionate de timp, mijloace şi forţă de muncă.

Bancă – persoană juridică a cărei activitate constă în atragerea de depozite sau de alte fonduri rambursabile de la public și în acordarea de credite în cont propriu.

# GESTIONAREA SECURITĂȚII INFORMAȚIILOR

## OBIECTIVE ȘI MĂSURARE

Obiectivele generale ale sistemului de management al securității informațiilor sunt următoarele: crearea unei imagini mai bune pe piață și reducerea daunelor cauzate de potențiale incidente; obiectivele sunt în concordanță cu obiectivele de afaceri, strategia și planurile de afaceri ale organizației. Echipa de securitate este responsabilă pentru revizuirea acestor obiective generale ISMS și stabilirea altora noi.

Toate obiectivele trebuie revizuite cel puțin o dată pe an.

Banca MAIB va măsura îndeplinirea tuturor obiectivelor. Managerul de securitate este responsabil pentru stabilirea metodei de măsurare a realizării obiectivelor – măsurarea va fi efectuată cel puțin o dată pe an și va analiza și evalua rezultatele măsurării și le va raporta.

## CERINȚE DE SECURITATE A INFORMAȚIILOR

Această Politică și întregul ISMS trebuie să fie conforme cu cerințele legale și de reglementare relevante pentru organizație în domeniul securității informațiilor, precum și cu obligațiile contractuale.

O listă detaliată a tuturor cerințelor contractuale și legale este furnizată în Lista obligațiilor legale, de reglementare și contractuale.

La consultarea cerințelor MaRisk și BAIT cu standardele ISO 27001 și protecția de bază IT, se pot determina următoarele: Pe lângă aspectele orientate spre risc și protecția datelor, conține, de asemenea, specificații și așteptări referitoare la protecția preventivă împotriva atacuri pentru sistemele de management al securității informațiilor. MaRisk și BAIT au stabilit sisteme informatice adecvate pentru a îndeplini cerințele operaționale, cerințele de afaceri și cerințele pentru gestionarea eficientă a riscurilor unei bănci. Sistemele și personalul IT ar trebui să contribuie la asigurarea disponibilității, autenticității și confidențialității datelor în ceea ce privește cerințele adecvate de protecție. Măsurile specifice care vizează realizarea acestui lucru pot fi găsite în setul de măsuri ISO 27001. În plus, BaFin împreună cu BAIT specifică standardele de strategie IT necesare pentru o perioadă lungă de timp împreună cu managementul riscului informațional. Din acest punct, strategia IT va fi privită ca o cerință de bază pentru configurarea cu succes a managementului riscului informațional. Din cauza acestei dezvoltări, multe bănci sunt nevoite să își modernizeze arhitectura și infrastructurile IT existente. Băncile constată că trebuie să ajusteze sau să revizuiască complet procesele și standardele adecvate pentru implementarea strategiei lor IT, care poate fi garantată doar prin crearea de noi responsabilități (de exemplu, Chief Data Officer) și creșterea bugetului IT.

## CONTROALE DE SECURITATE A INFORMAȚIILOR

Procesul de selectare a controalelor (garanțiilor) este definit în Metodologia de evaluare a riscurilor și de tratare a riscurilor.

Controalele selectate și starea lor de implementare sunt enumerate în Declarația de aplicabilitate.

O declarație de aplicabilitate (definitie ISO 27001 pentru securitatea informatiei) este un document care expune obiectivele de control si masurile de control legate de securitatea informatiei din organizatia dvs.

Pentru a va da seama despre care ar trebui sa fie obiectivele de control si masurile de control legate de securitatea informatiei proprii numai organizatiei dvs., trebuie sa efectuati o apreciere a riscului, sa alegeti tratamente ale riscului, sa identifice toate cerintele legale si de reglementare. relevante, sa va studiati obligatiile contractuale si sa analizati propriile nevoi si cerinte ale organizatiei dvs.

Odata ce ati infaptuit toate cele de mai sus, ar trebui sa fiti gata sa pregatiti declaratia de aplicabilitate proprie numai organizatiei dvs.

## CONTINUITATEA AFACERII

Managementul continuității afacerii este prescris în Politica de management al continuității afacerii.

Un sistem de management al continuității afacerii (SMCA) certificat ISO 22301 de LRQA pregătește organizațiile pentru situații extreme, cum sunt, de exemplu, defectarea sistemelor IT, incidente implicând personal sau telecomunicații, terorismul, fenomenele meteo extreme sau epidemiile. Prin implementarea unor procese clare, care să asigure o restabilire rapidă, ISO 22301 ajută la menținerea unui nivel de servicii constante pentru a vă oferi și toate părțile interesate.

Certificarea este valabilă pentru toate tipurile de organizații; iar revizuirea la fiecare cinci ani a standardului ISO 22301 asigură relevanța față de ultimele amenințări și riscuri apărute.

## RESPONSABILITĂȚI

Pe parcursul acestui proiect, specialiștii trebuie să efectueze următoarele lucrări:

* Analiza documentației ISMS
* Analiza proceselor existente de management IS și a semnelor de funcționare a ISMS
* Evaluarea completității și eficacității măsurilor IS luate în organizație
* Interviuri cu personalul ISMS, evaluarea competenței și a nivelului de conștientizare
* Analiza inconformității cu cerințele ISO 27001
* Pregătirea avizului de specialitate privind conformitatea ISMS cu ISO 27001
* Elaborarea recomandării privind eliminarea defectelor existente și asigurarea conformității cu ISO 27001

## COMUNICARE POLITICĂ

Indiferent de Sistemul de Management implementat in cadrul organizatiei pe care o conduce, este important ca politica privind calitatea, mediu sau SSM sa fie comunicata corect atat in cadrul organizatiei, cat si partilor interesate. Astfel, eficienta Standardelor Internationale pe care le-ai ales sa le implementeze in compania ta va fi asigurata la cel mai inalt nivel.

Politica referitoare la Sistemele de Management ISO 9001:2015, ISO 14001:2015 si ISO 45001:2018 trebuie:

* Sa fie disponibila ca informatie documentata
* Sa fie comunicata in cadrul organizatiei
* Sa fie disponibila pentru partile interesate
* Sa fie relevanta si adecvata

# SPRIJIN PENTRU IMPLEMENTAREA ISMS

Declararea că implementarea și îmbunătățirea continuă a ISMS vor fi susținute cu resurse adecvate pentru a atinge toate obiectivele stabilite în această Politică, precum și pentru a satisface toate cerințele identificate.

**Obținem suportul conducerii**

După cum este descris în ISO / IEC 27001, conducerea joacă un rol important în succesul unui ISMS.

**De ce avem nevoie:** secțiunea de responsabilitate a managementului ISO 27001. Managementul trebuie să se angajeze în stabilitatea, implementarea, funcționarea, monitorizarea, revizuirea, întreținerea și dezvoltarea ISMS. Angajamentul trebuie să includă activități cum ar fi asigurată disponibilități resurselor adecvate pentru a lucra la ISMS și ca toți angajații afectate de ISMS să are pregătirea, conștientizarea și competența respectivă.

**Rezultate:** Stabilirea următoarelor elemente demonstrează angajamentul de management:

O politică de securitate a informațiilor; această politică poate fi un document independent sau parte dintr-un manual global de securitate care este utilizat de o organizație.

Obiective și planuri de securitate a informațiilor; din nou, această informație poate fi un document independent sau parte dintr-un manual global de securitate care este utilizat de o organizație.

Roluri și responsabilități pentru securitatea informațiilor; o listă a rolurilor legate de securitate informațiilor ar trebui să fie documentată în documentele de descriere a postului organizației, fie ca parte a manualului de securitate sau a documentelor descriere a ISMS.

Anunțarea sau comunicarea către organizație a importanței aderării la politica de securitate a informatiilor.

Resurse suficiente pentru gestionarea, dezvoltarea, întreținerea și implementarea ISMS. În plus, conducerea va participa la procesul PDMS, așa cum este descris în ISO 27001, prin: Determinarea nivelului acceptabil de risc. Dovezi această activitate pot fi incluse în documentele de evaluare a riscurilor, descrie mai jos în acest ghid. Realizarea recenzelor de conducere ale ISMS la intervale planificate. Dovada aceasta activitate poate face parte din procesul de aprobare a documentelor din ISMS.

Asigurarea faptului că personalul afectat de ISMS este instruit, are competența de îndeplinire rolurile și responsabilitățile pe care trebuie să le îndeplinească și este conștient de aceste roluri și responsabilități. Dovada activităților poate fi prin intermediul înregistrării de instruire a angajaților și a documentelor de revizuire a angajaților.

# VALIDITATEA ȘI GESTIONAREA DOCUMENTULUI

Deținătorul acestui document trebuie să verifice și, dacă este cazul, să actualizeze documentul cel puțin o dată pe an.

Validarea si verificarea emisiilor pot fi urmarite de o organizatie din mai multe motive, cum ar fi:

* contribuția la raportul anual,
* comunicarea cu clientii,
* respectarea cerintelor de raportare ale autorităților de reglementare sau ale investitorilor sau
* publicarea realizarilor in materie de reducere a emisiilor.

Atunci când se evaluează eficacitatea și caracterul adecvat al acestui document, trebuie luate în considerare următoarele criterii:

• numărul de angajați și părți externe care au un rol în ISMS, dar nu sunt familiarizați cu acest document

• nerespectarea ISMS cu legile și reglementările, obligațiile contractuale și alte documente interne ale organizației

• ineficacitatea implementării și întreținerii ISMS

• responsabilități neclare pentru implementarea ISMS