1. Scop/ Obiective:

Această politică definește cerințele minime obligatorii de securitate a informațiilor pentru entitate.

Această politică acționează ca un document umbrelă pentru toate celelalte politici de securitate și standardele asociate. Această politică definește responsabilitatea companiei:

- să protejeze și să mențină confidențialitatea, integritatea și disponibilitatea informațiilor și a activelor de infrastructură aferente;
- să gestioneze riscul de expunere sau de compromitere a securității;
- asigurarea unui mediu informatic (IT) sigur și stabil;
- să identifice și să reacționeze la evenimentele care implică utilizarea abuzivă, pierderea sau divulgarea neautorizată a activelor informaționale;
- să monitorizeze sistemele pentru a detecta anomaliile care ar putea indica o compromitere; și
- promovarea și creșterea gradului de conștientizare a securității informațiilor.

Neasigurarea și neprotejarea confidențialității, integrității și disponibilității activelor informaționale în mediul de rețea extrem de interconectat de astăzi pot deteriora sau opri sistemele care operează infrastructuri critice, tranzacții financiare și comerciale și funcții guvernamentale vitale, pot compromite datele și pot duce la nerespectarea legislației și a reglementărilor.

Această politică este benefică pentru entități prin definirea unui cadru care va asigura existența unor măsuri adecvate pentru protejarea confidențialității, integrității și disponibilității datelor; și va asigura că personalul și toate celelalte entități afiliate își înțeleg rolul și

1. Purpose/ Objectives:

This policy defines the mandatory minimum information security requirements for the entity.
This policy acts as an umbrella document to all other security policies and associated standards. This policy defines company's responsibility to:

- protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets;
- manage the risk of security exposure or compromise;
- assure a secure and stable information technology (IT) environment;
- identify and respond to events involving information asset misuse, loss or unauthorized disclosure;
- monitor systems for anomalies that might indicate compromise; and
- promote and increase the awareness of information security.

Failure to secure and protect the confidentiality, integrity and availability of information assets in today's highly networked environment can damage or shut down systems that operate critical infrastructure, financial and business transactions and vital government functions; compromise data; and result in legal and regulatory non-compliance.

This policy benefits entities by defining a framework that will assure appropriate measures are in place to protect the confidentiality, integrity and availability of data; and assure staff and all other affiliates understand their role and

responsabilitățile, au cunoștințe adecvate privind politica, procedurile și practicile de securitate și știu cum să protejeze informațiile.

2. Proces

Informațiile care sunt colectate, analizate, stocate, comunicate și raportate pot fi supuse furtului, utilizării abuzive, pierderii și corupției. Informațiile pot fi puse în pericol de o educație și o formare deficitară și de încălcarea controalelor de securitate. Aceasta are rolul de a oferi o prezentare generală la nivel înalt și o justificare a controalelor de securitate a informațiilor bazate pe riscuri ale BOA RBT.
Obiectivele de securitate ale BOA RBT sunt următoarele:

- riscurile informatice sunt identificate, gestionate și tratate în conformitate cu o toleranță la risc convenită.
- utilizatorii noștri autorizați pot accesa și partaja informațiile în condiții de siguranță pentru a-și îndeplini rolurile.
- controalele noastre fizice, procedurale și tehnice să asigure un echilibru între experiența utilizatorului și securitate.
- obligațiile noastre contractuale și legale referitoare la securitatea informațiilor sunt îndeplinite.
- activitatea noastră de predare, de dezvoltare și administrativă ia în considerare securitatea informațiilor.
- persoanele care accesează informațiile noastre sunt conștiente de responsabilitățile lor în materie de securitate a informațiilor
- incidentele care afectează activele noastre informaționale sunt soluționate și se trage învățăminte din ele pentru a ne îmbunătăți controalele.

Politica de securitate a informațiilor și controalele, procesele și procedurile care o susțin se aplică

responsibilities, have adequate knowledge of security policy, procedures and practices and know how to protect information.

2. Process

Information that's collected, analysed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption. Information may be put at risk by poor education and training, and the breach of security controls. This is to provide the high-level outline of, and justification for, BOA RBT's risk-based information security controls.

BOA RBT's security objectives are that:

- our information risks are identified, managed and treated according to an agreed risk tolerance
- our authorised users can securely access and share information in order to perform their roles
- our physical, procedural and technical controls balance user experience and security
- our contractual and legal obligations relating to information security are met
- our teaching, development and administrative activity considers information security
- individuals accessing our information are aware of their information security responsibilities
- incidents affecting our information assets are resolved and learnt from to improve our controls

tuturor informațiilor utilizate la BOA RBT, în toate formatele. Aceasta include informațiile prelucrate de alte organizații în relațiile cu BOA RBT.

Politica privind sistemul de management integrat și controalele, procesele și procedurile de sprijinire a acesteia se aplică tuturor persoanelor care au acces la informațiile și tehnologiile BOA RBT. Aceasta include părțile externe care furnizează servicii de prelucrare a informațiilor către BOA RBT.
Respectarea controalelor din această politică va fi monitorizată de către echipa de securitate a informațiilor și va fi raportată echipei de conducere.
Politica BOA RBT este de a se asigura că informațiile sunt protejate împotriva unei pierderi de:

- confidențialitate - informațiile vor fi accesibile numai persoanelor autorizate
- integritate - se va menține acuratețea și caracterul complet al informațiilor
- disponibilitate - informațiile vor fi accesibile utilizatorilor și proceselor autorizate atunci când este necesar

BOA RBT va implementa un sistem de management al securității informațiilor bazat pe standardul TISAX, si va ține cont de abordările si cerintele tuturor părților interesate.

BOA RBT va adopta o abordare bazată pe riscuri în ceea ce privește aplicarea următoarelor controale:
1 - Se va defini un set de controale, procese și proceduri de nivel inferior pentru securitatea informațiilor, în sprijinul politicii de securitate a informațiilor de nivel înalt și a obiectivelor declarate ale acesteia. Această suită de documente justificative va fi publicată și comunicată utilizatorilor BOA RBT și părților externe relevante.
BOA RBT va defini și va pune în aplicare mecanisme de guvernanță adecvate pentru

The Information Security Policy and its supporting controls, processes and procedures apply to all information used at BOA RBT, in all formats. This includes information processed by other organisations in their dealings with BOA RBT.

The Integrated Management System Policy and its supporting controls, processes and procedures apply to all individuals who have access to BOA RBT information and technologies. This includes external parties that provide information processing services to BOA RBT.

Compliance with the controls in this policy will be monitored by the Information Security Team and reported to the Management Team.

It is BOA RBT's policy to ensure that information is protected from a loss of:

- confidentiality – information will be accessible only to authorised individuals
- integrity – the accuracy and completeness of information will be maintained
- availability – information will be accessible to authorised users and processes when required

BOA RBT will implement an Information Security Management System based on TISAX standard. BOA RBT will be mindful of the approaches adopted by its stakeholders, and all interested parties.

BOA RBT will adopt a risk-based approach to the application of the following controls:

1 - A set of lower-level controls, processes and procedures for information security will be defined, in support of the high-level Information Security Policy and its stated objectives. This suite of supporting documentation will be published and communicated to BOA RBT users and relevant external parties.

gestionarea securității informațiilor. Aceasta va include identificarea și alocarea responsabilităților în materie de securitate, pentru a iniția și controla punerea în aplicare și funcționarea securității informațiilor în cadrul BOA RBT.

2 - BOA RBT va numi:

- un responsabil cu protecția datelor (DPO) pentru a gestiona Regulamentul general privind protecția datelor
- un responsabil principal cu securitatea informațiilor (CISO) pentru a gestiona funcția de securitate a informațiilor
- un proprietar al activelor informaționale (Information Asset Owner - IAO) pentru a-și asuma responsabilitatea locală pentru gestionarea informațiilor

3 - Politicile de securitate și așteptările privind utilizarea acceptabilă ale BOA RBT vor fi comunicate tuturor utilizatorilor pentru a se asigura că aceștia își înțeleg responsabilitățile. Educația și formarea în domeniul securității informațiilor vor fi puse la dispoziția întregului personal. Comportamentul slab sau inadecvat va fi abordat.
Acolo unde este posibil, responsabilitățile de securitate vor fi incluse în descrierile de rol, în specificațiile personale și în planurile de dezvoltare personală.

4 - Toate activele vor fi documentate și contabilizate. Aceasta include: (informații, software, echipamente electronice de procesare a informației, utilități de serviciu, persoane).

Toate activele informaționale vor fi clasificate în funcție de cerințele legale, valoarea comercială, caracterul critic și sensibilitatea lor. Clasificarea va indica cerințele de manipulare corespunzătoare. Toate activele informaționale vor avea un program definit de păstrare și eliminare.

BOA RBT will define and implement suitable governance arrangements for the management of information security. This will include identification and allocation of security responsibilities, to initiate and control the implementation and operation of information security within BOA RBT.

2 - BOA RBT will appoint:

- an Data Protection Officer (DPO) to manage the General Data Protection Regulation
- an Chief Security Information Officer (CISO) to manage the information security function
- Information Asset Owner (IAOs) to assume local accountability for information management

3 - BOA RBT's security policies and expectations for acceptable use will be communicated to all users to ensure that they understand their responsibilities. Information security education and training will be made available to all staff. Poor or inappropriate behaviour will be addressed.

Where practical, security responsibilities will be included in role descriptions, person specifications and personal development plans.

4 - All assets will be documented and accounted for. This includes: (information, software, electronic information processing equipment, service utilities, people)

All information assets will be classified according to their legal requirements, business value, criticality and sensitivity. Classification will indicate appropriate handling requirements. All information assets will have a defined retention and disposal schedule.

5 - Accesul la toate informațiile va fi controlat și va fi determinat de cerințele de afaceri. Accesul va fi acordat sau se vor lua măsuri pentru utilizatori, în funcție de rolul lor și de clasificarea informațiilor, numai la un nivel care să le permită acestora să își îndeplinească sarcinile.	5 - Access to all information will be controlled and will be driven by business requirements. Access will be granted or arrangements made for users according to their role and the classification of information, only to a level that will allow them to carry out their duties.
6 - BOA RBT va furniza îndrumări și instrumente pentru a asigura utilizarea corectă și eficientă a criptografiei pentru a proteja confidențialitatea, autenticitatea și integritatea informațiilor și sistemelor.	6 - BOA RBT will provide guidance and tools to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information and systems.
7 - Instalațiile de procesare a informațiilor sunt adăpostite în zone sigure, protejate fizic împotriva accesului neautorizat, a deteriorării și a interferențelor prin perimetre de securitate definite. Vor fi instituite controale de securitate interne și externe stratificate pentru a descuraja sau a preveni accesul neautorizat și pentru a proteja activele. Aceasta include cele care sunt critice sau sensibile, împotriva atacurilor forțate sau ascunse.	7 - Information processing facilities are housed in secure areas, physically protected from unauthorised access, damage and interference by defined security perimeters. Layered internal and external security controls will be in place to deter or prevent unauthorised access and protect assets. This includes those that are critical or sensitive, against forcible or hidden attacks.
8 - BOA RBT va asigura funcționarea corectă și sigură a sistemelor de prelucrare a informațiilor. Acest lucru va include: proceduri de operare documentate, utilizarea unui management formal al schimbărilor și al capacității, controale împotriva programelor malware, utilizarea definită a jurnalizării și gestionarea vulnerabilităților	8 - BOA RBT will ensure the correct and secure operations of information processing systems. This will include: documented operating procedures, the use of formal change and capacity management, controls against malware, defined use of logging and vulnerability management
9 - BOA RBT va menține controale de securitate a rețelelor pentru a asigura protecția informațiilor din cadrul rețelelor sale. BOA RBT va furniza, de asemenea, instrumentele și îndrumările necesare pentru a asigura transferul securizat de informații atât în cadrul rețelelor sale, cât și cu entități externe. Acest lucru este în conformitate cu cerințele de clasificare și de manipulare asociate cu informațiile respective.	9 - BOA RBT will maintain network security controls to ensure the protection of information within its networks. BOA RBT will also provide the tools and guidance to ensure the secure transfer of information both within its networks and with external entities. This is in line with the classification and handling requirements associated with that information.
10 - Cerințele de securitate a informațiilor vor fi definite în timpul elaborării cerințelor de afaceri pentru noile sisteme de informații sau pentru modificările aduse sistemelor de informații existente.	10 - Information security requirements will be defined during the development of business requirements for new information systems or changes to existing information systems.

Vor fi implementate, după caz, controale pentru reducerea oricăror riscuri identificate.

11 - La stabilirea relațiilor cu furnizorii se vor lua în considerare cerințele de securitate a informațiilor ale BOA RBT, pentru a se asigura că activele accesibile furnizorilor sunt protejate. Activitatea furnizorilor va fi monitorizată în funcție de valoarea activelor și de riscurile asociate.

12 - Vor fi disponibile îndrumări cu privire la ceea ce constituie un incident de securitate a informațiilor și la modul în care acesta trebuie raportat. Încălcările reale sau suspectate ale securității informațiilor trebuie raportate și vor fi investigate. Se vor lua măsurile adecvate pentru a corecta încălcarea și orice învățătură va fi încorporată în controale.

13 - BOA RBT va avea în vigoare măsuri pentru a proteja procesele de afaceri critice de efectele unor defecțiuni majore ale sistemelor informatice sau ale unor dezastre. Aceasta va include rutine de backup adecvate și rezistență integrată.
Planurile de continuitate a activității trebuie să fie menținute și testate în sprijinul acestei politici. Se va efectua o analiză a impactului asupra activității, detaliind consecințele: (dezastre, defecțiuni de securitate, pierderea serviciului, lipsa disponibilității serviciului).

14 - Proiectarea, operarea, utilizarea și gestionarea sistemelor informatice trebuie să respecte toate cerințele de securitate legale, de reglementare și contractuale.
În prezent, aceasta include:

- Regulamentul general privind protecția datelor,
- standardul industriei cardurilor de plata,
- legile și reglementările guvernamentale,
- angajamentele contractuale ale BOA RBT (cerințele specifice ale clientului).

BOA RBT va utiliza o combinație de audituri interne și externe pentru a demonstra conformitatea cu standardele și bunele practici alese, inclusiv cu politicile și procedurile interne.

Controls to reduce any risks identified will be implemented where appropriate.

11 - BOA RBT's information security requirements will be considered when establishing relationships with suppliers, to ensure that assets accessible to suppliers are protected. Supplier activity will be monitored according to the value of the assets and the associated risks.

12 - Guidance will be available on what constitutes an information security incident and how this should be reported. Actual or suspected breaches of information security must be reported and will be investigated. The appropriate action to correct the breach will be taken, and any learning built into controls.

13 - BOA RBT will have in place arrangements to protect critical business processes from the effects of major failures of information systems or disasters. This will include appropriate backup routines and built-in resilience.

Business continuity plans must be maintained and tested in support of this policy. Business impact analysis will be undertaken, detailing the consequences of: (disasters, security failures, loss of service, lack of service availability).

14 - The design, operation, use and management of information systems must comply with all statutory, regulatory and contractual security requirements.

Currently this includes:

- General Data Protection Regulation,
- the payment card industry standard,
- the government's laws and regulations,
- BOA RBT's contractual commitments (Customer Specific Requirements)

BOA RBT will use a combination of internal and external audits to demonstrate compliance against chosen standards and best practice,

15 - Personalul care se dovedește că a încălcat această politică poate face obiectul unei cercetari disciplinare, urmate de măsuri disciplinare, inclusiv concedierea, și al unor sancțiuni civile sau penale aferente. Orice furnizor, consultant sau contractant despre care se constată că a încălcat prezenta politică poate face obiectul unor sancțiuni care pot ajunge până la și inclusiv la eliminarea drepturilor de acces, rezilierea contractului (contractelor) și sancțiuni civile sau penale aferente.	including against internal policies and procedures. 15 - Personnel found to have violated this policy may be subject to disciplinary inquiry followed by disciplinary action, up to and including termination of employment, and related civil or criminal penalties. Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

3. Revizii

3. Revisions

Rev. #	Data / Date	Creat de / Created by	Aprobat de / Approved by	Descrierea modificari Description of change
0	21/03/2024	Constantin BORLA	Christian CUREC	Elaborarea documentului Document creation
1				
2				