1. PURPOSE

Define Information Security guidelines to be complied with by Third Parties.

2. FIELD OF APPLICATION

It applies to Third Parties, as to know to any and all legal entities and/or individuals who are not CBMM employees, who carry out activities for CBMM remotely and/or in person at CBMM's facilities and/or offices and who have access to CBMM's data or information systems.

3. DEFINITIONS AND ACRONYMS

Threat: potential cause of an unexpected incident, which may result in damages to CBMM's information assets.

Asset: Anything that is of value to CBMM's business and needs to be protected.

Information Security Incident: Event that may cause damages to CBMM and impact CBMM's information assets due to loss of confidentiality, availability and integrity.

ITSM: Information Technology service management tool for opening calls.

Malware: Any type of unwanted program, installed without consent and that can damage CBMM's information assets, such as workstations, servers, infrastructure and network.

MFA: Multi-factor authentication.

Risk: Combination of the probability of occurrence of an event and its respective impacts.

Third Parties: Any and all legal entities and/or individuals who are not CBMM employees, who carry out activities for CBMM remotely and/or in person at CBMM's facilities and/or offices and who have access to CBMM's data or information systems.

Vulnerability: Fragility of a CBMM asset that can be exploited and cause damage to CBMM.

4. RESPONSIBILITIES AND AUTHORITIES

4.1. Third Parties

- Follow the guidelines set forth in this document.

4.2. Contract Manager

- Ensure that any Third Party complies with the guidelines here;
- Clarify any questions that Third Parties may have;
- Ensure training and instruction of guidelines related to operational demands regarding the service provision.

4.3. Information Security

- Define good practices, as well as promote the updating of and compliance with such practices;
- Monitor, follow-up and handle Information Security Incidents.

4.4. IT Governance

- Ensure, together with the responsible area, that this document is updated.

5. MISCELLANEOUS

5.1. Introduction

Information is a strategic asset for CBMM and covers three basic pillars of Information Security:

- Confidentiality: Information must be made available only to authorized people;
- Integrity: Information must not be altered improperly or without authorization;
- Availability: Information must be accessible at all times for legitimate use by authorized people.

5.2. Initial Guidelines

Third Parties must:

(i) comply with the Information Security principles set forth herein, with the guidelines provided for hereto and with any associated documentation.

(ii) in case of questions about this document, seek guidance from their superiors, the Contract Manager and/or CBMM's Information Security area.

(iii) protect CBMM's information against any unauthorized access, modification, destruction or dissemination, ensuring that technological resources are used appropriately.

(iv) refrain from using any CBMM information without CBMM's prior authorization.

(v) report issues related to privacy and personal data protection to CBMM's Privacy Office through this link.

5.3. Privacy and Data Protection

The processing of personal data by third parties on behalf of CBMM or jointly with CBMM must be carried out in accordance with applicable laws, the contract signed with CBMM and CBMM's practices.

5.4. Monitoring

- CBMM may, through its Information Security team, monitor, inspect and record the use of its network, systems and the internet, including access, receipt and transmission of information, to (i) ensure the integrity of data and information; (ii) audit and (iii) identify possible cyber threats.
- Third Parties must respect the level of access to systems, networks, equipment, programs, software, computer files, information and facilities as assigned to them.

5.5. Physical Security

- Third Parties must comply with security measures to access CBMM's facilities (when applicable).
- Third Parties may only access restricted areas together with a responsible employee. This employee shall be responsible for guiding Third Parties while they are in a restricted environment.
- Third Parties are forbidden to:
- Make any type of photographic, audio or video recording of internal areas without CBMM's prior authorization;
- Connect any device to the corporate network or any other available network without the prior authorization from the IT team (via ticket in the ITSM portal).
- Third Parties are responsible for the identification badge used to access CBMM's premises. In case of loss, theft or misplacement, Third Parties must immediately notify CBMM and the Contract Manager.

5.6. How to Use Credentials

Users must have good information security practices with respect to their passwords:

- Passwords shall not be written down or saved in files;

- Usernames and passwords shall not be distributed, disclosed, exposed or shared with others through any channel, whether verbally, in writing or electronically.
- Usernames and passwords are personal and non-transferable and must be properly protected;
- Users shall use multiple factor authentication on all systems where the feature is available;
- Passwords shall not include personal data, date of birth, address, soccer team, among other user information;
- Passwords used for private purposes shall not be used for corporate purposes.
- Password compromise is considered an Information Security Incident. In case of any indication that a password has been compromised, Third Parties shall (i) change the password immediately and (ii) report the incident in the ITSM tool.

5.7. Remote Access

- Any connection used to access information in CBMM's environment must be protected. VPN, Virtual Desktop or other solutions approved by CBMM's IT team must be used;
- A multiple factor authentication shall be used whenever possible.

5.8. Information Destruction and Storage

Third Parties must return or destroy any information or personal data in their possession or under their control in the following circumstances:

- When no longer necessary for the proposed purpose;
- If there is no legal obligation to store;
- At the end of the contract signed with CBMM;
- Information considered relevant to the continuity of operations must be stored in CBMM's corporate repositories.

5.9. Clear Desk and Clear Screen

Third Parties must ensure that no confidential information is accessed by unauthorized persons.

- Whenever Third Parties are not at their workstation, all hard copy documents as well as information considered restricted and confidential must be stored to prevent unauthorized access;
- Before leaving the workstation, Third Parties must lock the screen of their equipment;
- Documents including restricted or confidential information must be immediately removed from printers and copiers;
- Whiteboards, flipcharts and the like must be erased immediately after use.

5.10. Acceptable use of Technology Resources

- CBMM's email account must only be used for corporate purposes;
- No equipment, program, software or computer file shall be installed or saved without CBMM's prior written authorization, whether in CBMM's equipment, in any personal equipment or in any equipment provided by CBMM's contractors;
- Third Parties shall proactively collaborate and cooperate with CBMM's Information Security team in case of suspected or actual Information Security Incident;
- No equipment, program, software or computer file may be used for personal purposes, including, but not limited to, storing personal information.

5.11. Violation of Guidelines

Violations of these guidelines include, but are not limited to:

- Failure to immediately report whenever required according to the provisions here;
- Any action or omission that has the potential to cause financial loss and/or damage to CBMM's image;
- Use of data, information, equipment, programs, software, computer files, systems or other technological resources for illegal purposes, including but not limited to, in violation of laws, internal regulations and CBMM's Code of Ethics and Conduct available on the intranet;
- Use of unlicensed software and/or equipment without proper invoices;
- Improper use or storage of data, as well as unauthorized disclosure of confidential information, trade secrets or other information, without CBMM's prior written authorization.

The violation of any of the rules established here shall be deemed as an Information Security Incident that shall be analyzed by CBMM's Information Security team. In such cases, the provider responsible for the Third Party shall be subject to the penalties provided for in the contract.

5.12. Final Provisions

Any questions related to the compliance with this document shall be directed to CBMM's Information Security team or to the Contract Manager. This document is subject to changes and updates which, once disclosed to Third Parties, shall be immediately complied with.

6. EXHIBITS

Exhibit 1 – Reviews

VERSION	ITEM	HISTORY OF REVISIONS	REVISION DATE
00	All	Initial issuance of the document replacing PR-GSTI-29 version 1.0.	01.25.24