Esse documento contém versão em inglês a partir da página 10
This document contains English version from 10

1. OBJETIVO

Estabelecer diretrizes de Segurança da Informação a serem observadas por Terceiros.

Estabelecer diretrizes e práticas para garantir a proteção dos dados pessoais tratados por fornecedores e terceiros em nome da CBMM ou em conjunto, em conformidade com as legislações de proteção de dados aplicáveis e outras regulamentações pertinentes.

2. CAMPO DE APLICAÇÃO

Aplica-se a Terceiros, assim entendidos como todas as pessoas físicas e/ ou jurídicas que não sejam colaboradoras da CBMM, que executem atividades para a CBMM de forma remota e/ ou presencialmente na planta e/ou escritórios da CBMM e que tenham acesso às informações ou sistemas de informação da CBMM. Aplica-se também a todos os fornecedores, parceiros, prestadores de serviços, consultores e qualquer outra entidade terceira que trate dados pessoais em nome da CBMM ou em colaboração com ela.

3. DEFINIÇÕES E SIGLAS

Ameaça: causa potencial de um incidente inesperado, que pode resultar em danos aos ativos de informação da CBMM.

Anonimização: técnica de processamento de dados que remove ou modifica informações que possam identificar uma pessoa. Essa técnica resulta em dados que não podem ser associados a nenhum indivíduo em específico.

Ativo: Algo que tenha valor para os negócios da CBMM e precise ser protegido.

Bases Legais: Hipóteses trazidas pela lei que autorizam a realização de atividades de tratamento de dados pessoais com finalidades especificas e devidamente informadas aos titulares de dados pessoais.

Controlador: Pessoa natural ou jurídica, de direito público e privado, a quem competem as decisões referente ao tratamento dos dados pessoais.

Dados Pessoais: Informações relacionadas a uma pessoa natural identificada ou identificável.

Dados sensíveis: Dados pessoais relacionados a origem racial, étnica, convicção religiosa, opinião política, filiação a sindicato ou qualquer organização

de caráter religioso, filosofo ou político, além de dados referentes à saúde, vida sexual, dados genéticos ou biométricos.

Encarregado de Proteção de Dados (DPO): Pessoa indicada pela CBMM para atuar como ponto de contato entre a empresa, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

Incidente de Segurança da Informação: Ocorrência que pode causar danos à CBMM e impactar os ativos de informação da CBMM devido a perda de confidencialidade, disponibilidade e integridade.

ITSM: ferramenta de gestão de serviços de Tecnologia da Informação para abertura de chamados.

Malware: Qualquer tipo de programa indesejado, instalado sem o consentimento e que pode trazer danos aos ativos de informação da CBMM, como estações de trabalho, servidores, infraestrutura e rede.

MFA (Múltiplo fator de autenticação): método para atestar a identidade de alguém para concessão de acesso a informações, sistemas, aplicativos, entre outros.

Operador: Pessoa natural ou jurídica, de direito público e privado, que realiza o tratamento de dados pessoais em nome do controlador.

Risco: Combinação da probabilidade de ocorrência de algum evento e seus respectivos impactos.

ROPA: Registro das operações de tratamento de dados pessoais.

Terceiros: Todas as pessoas físicas e/ou jurídicas que não sejam colaboradoras da CBMM, que executem atividades para a CBMM de forma remota e/ou presencialmente na planta e/ou escritórios da CBMM e que tenham acesso às informações ou sistemas de informação da CBMM.

Titular dos Dados: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Transferência Internacional: transferência de dados para um país estrangeiro ou organismo internacional do qual o país seja membro.

Tratamento de Dados: Qualquer operação realizada com dados pessoais, como coleta, armazenamento, uso, processamento, compartilhamento ou eliminação.

Vulnerabilidade: Fragilidade de um ativo da CBMM que pode ser explorada e gerar danos à CBMM.

4. RESPONSABILIDADES E AUTORIDADES

4.1. Terceiros

- Seguir as diretrizes estabelecidas neste documento.

4.2. Gestor do contrato

- Garantir que o Terceiro cumpra as diretrizes aqui aplicadas;
- Esclarecer eventuais dúvidas dos Terceiros;
- Garantir o direcionamento e treinamento de orientações relacionadas às demandas operacionais referentes à prestação de serviço;
- Garantir informar o início e fim de contrato aos envolvidos na CBMM;
- Garantir e verificar a disseminação referente a execução dos treinamentos e orientações relacionadas à segurança da informação da CBMM para a prestação de serviço;
- Garantir a ação do onboarding e offboarding dos terceiros;
- Garantir a divulgação dos canais de comunicação – pós projetos implementados.

4.3. Segurança da Informação

- Definir boas práticas, bem como promover a atualização e manutenção de tais práticas;
- Monitorar, acompanhar e tratar e direcionar os Incidentes de Segurança da Informação para os envolvidos.

4.4. Governança de TI

- Garantir a atualização deste documento em conjunto com a área responsável.

4.5. Escritório de Privacidade

- Definir boas práticas de Privacidade e Proteção de Dados;
- Solucionar dúvidas de terceiros e parceiros através do canal disponibilizado neste documento.

5. DISPOSIÇÕES GERAIS

5.1. Introdução

A informação é um ativo estratégico para a CBMM e abrange três pilares básicos da Segurança da Informação:

- Confidencialidade: Informações devem ser disponibilizadas somente a pessoas autorizadas;

- Integridade: Informações não devem alteradas de forma indevida ou sem autorização;
- Disponibilidade: Informações devem estar acessíveis a qualquer momento, para uso legítimo das pessoas autorizadas.

5.2. Orientações Iniciais

Os Terceiros devem:

(i) Observar os princípios de Segurança da Informação aqui dispostos, cumprir as diretrizes estabelecidas neste documento e a documentação porventura associada.

(ii) Em caso de dúvidas relacionadas a este documento, buscar orientação de seus superiores, do Gestor do contrato e/ou da área de Segurança da Informação da CBMM.

(iii) Proteger as informações da CBMM contra qualquer acesso não autorizado, modificação, destruição ou disseminação, assegurando que os recursos tecnológicos sejam utilizados de maneira adequada.

(iv) Abster-se de utilizar qualquer informação da CBMM sem prévia autorização da CBMM.

(v) Endereçar questões relacionadas à privacidade e proteção de dados pessoais ao Escritório de Privacidade CBMM por meio do e-mail dpo@cbmm.com.

5.3. Monitoramento

- A CBMM poderá, por meio do seu time de Segurança da Informação, monitorar, inspecionar e registrar o uso da sua rede, sistemas e da internet, incluindo o acesso, recebimento e transmissão de informações, para fins de (i) garantir a integridade dos dados e das informações; (ii) auditoria; e (iii) identificação de possíveis ameaças cibernéticas.
- Os Terceiros devem respeitar o nível de acesso aos sistemas, redes, equipamentos, programas, softwares, arquivos informatizados, informações e instalações conforme que lhes for atribuído.

5.4. Segurança Física

- Os Terceiros devem respeitar as medidas de segurança para acessar as instalações da CBMM (quando aplicável).
- Os Terceiros poderão acessar áreas restritas somente em companhia de um colaborador responsável. Este colaborador será responsável por orientá-lo durante toda sua estada no ambiente restrito.
- É proibido:

- Qualquer tipo de gravação fotográfica, áudio ou vídeo das áreas internas sem autorização prévia da CBMM;
- Conectar qualquer dispositivo à rede corporativa ou qualquer outra rede disponível sem autorização prévia da equipe de TI (via chamado no portal ITSM).
- O Terceiro é responsável pelo crachá de identificação utilizado para acessar as dependências da CBMM. Em caso de perda, roubo ou extravio, o Terceiro deverá comunicar imediatamente a CBMM e o Gestor do contrato.

5.5. Cuidados com Credenciais

Os usuários devem empregar boas práticas de segurança da informação com relação às suas senhas;

- As senhas não devem ser anotadas em papel ou arquivos;
- O usuário e senha não podem ser distribuídos, divulgados, expostos ou compartilhados com outras pessoas por meio de qualquer canal, seja verbalmente, por escrito ou eletronicamente;
- O usuário e senha são pessoais e intransferíveis e devem ser devidamente protegidos;
- Os usuários deverão utilizar múltiplo fator de autenticação em todos os sistemas em que o recurso puder ser utilizado;
- As senhas não deverão conter dados pessoais, data de nascimento, endereço, time de futebol, entre outras informações do usuário;
- Senhas usadas para fins particulares não deverão ser utilizadas para fins corporativos;
- O comprometimento da senha é considerado um Incidente de Segurança da Informação. Se houver qualquer indicação de um incidente de segurança, não apenas comprometimento da senha, o Terceiro deverá (i) alterar a senha imediatamente e (ii) reportar o incidente na ferramenta de ITSM.

5.6. Acesso Remoto

- Qualquer conexão feita para se acessar informações no ambiente CBMM deverá ser protegida. É mandatória a utilização de soluções de VPN, de Desktop virtual ou solução homologada pelo time de TI da CBMM;
- É mandatório o uso do múltiplo fator de autenticação sempre que possível.

5.7. Descarte e Armazenamento de Informações

O Terceiro deverá devolver ou descartar informações ou dados pessoais em sua posse ou sob seu controle nas seguintes situações:

- Se não for mais necessário para a finalidade proposta;
- Se não houver obrigação legal que demande o armazenamento;
- Após o término do contrato firmado com a CBMM.

Informações consideradas relevantes para a continuidade das operações deverão ser armazenadas em repositórios corporativos da CBMM.

5.8. Mesa Limpa e Tela Limpa

- Os Terceiros devem garantir que nenhuma informação confidencial seja acessada por pessoas não autorizadas;
- Caso o Terceiro não esteja na sua estação de trabalho, todos os documentos em papel assim como informações consideradas restritas e confidenciais devem ser guardados para impedir o acesso não autorizado;
- Antes de se ausentar da estação de trabalho, o Terceiro deve bloquear a tela do seu equipamento;
- Documentos contendo informações restritas ou confidenciais deverão ser removidos imediatamente das impressoras e copiadoras;
- Quadros brancos, flipcharts e outros devem ser apagados imediatamente após sua utilização.

5.9. Uso Aceitável de Recursos de Tecnologia

- A conta de e-mail CBMM deverá ser utilizada somente para fins corporativos;
- É vedada instalar ou inserir qualquer tipo de equipamento, programa, software ou arquivo informatizado sem a prévia autorização por escrito da CBMM, seja em equipamentos da CBMM, pessoais ou fornecidos pelas empresas contratadas da CBMM;
- O Terceiro deverá colaborar e cooperar proativamente com o time de Segurança da Informação CBMM em caso de suspeita de ou de efetivo Incidente de Segurança da Informação;
- É vedado o uso de equipamento, programa, software ou arquivo informatizado para fins pessoais, incluindo, mas não se limitando ao armazenado de informações de cunho pessoal.
- É vedado o uso de qualquer tipo de tecnologia utilizada para gravar ou transcrever informações relacionadas à CBMM ou sob sua responsabilidade sem aviso prévio e sem a devida autorização.

5.10. Privacidade e Proteção de Dados

5.10.1. Obrigações dos Fornecedores e Parceiros

Serão considerados como premissa a todos os fornecedores e parceiros CBMM quando do tratamento de dados pessoais:

- Adotar medidas técnicas e administrativas e de segurança das informações tratadas, de forma a proteger os dados contra acessos indevidos ou não autorizados de acordo com o contrato regente. Estas medidas podem incluir, mas não se limita a:
- Gestão e rastreabilidade de acessos as informações e dados;

- Uso de medidas técnicas para proteção dos dados pessoais (antivírus, criptografia, MFA (quando possível), entre outros);
- Planos de comunicação de incidentes relacionados a segurança das informações, incluindo requisitos de proteção de dados, conforme orientação da Autoridade Nacional de Proteção de Dados;
- Agir conforme as instruções da CBMM, jamais utilizando os dados tratados para fins e vantagens comerciais ou finalidades não previstas em contrato;
- Assegurar que as obrigações de sigilo, segurança da informação e proteção dos dados pessoais tratados se estendam aos colaboradores, contratados e subcontratados;
- Assumir integralmente a responsabilidade por quaisquer danos, sejam eles diretos ou indiretos, que resultem do tratamento inadequado dos dados pessoais de maneira irregular ou contrária ao estabelecido em contrato, devendo inclusive, ressarcir em caso de descumprimento;
- Cooperar com a CBMM para resolução de questões envolvendo a garantia de conformidade sob os dados tratados, respondendo os questionários e avaliações solicitadas e provendo documentação necessária para demonstrar o cumprimento das obrigações legais e as obrigações estabelecidas em contrato;
- Cooperar e prestar assistência a CBMM, dentro dos limites das obrigações impostas, em caso de atendimento a Autoridade Nacional de Proteção de Dados, ao titular, ou qualquer outra autoridade governamental, sobre questões relacionadas ao tratamento dos dados pessoais;
- Documentar os processos e manter o inventário (ROPA) atualizado de todas as operações de tratamento de dados pessoais realizadas, abrangendo também a indicação de transferências internacionais de dados pessoais eventualmente realizadas além da garantia e mecanismos adotados para proteção das informações;
- Efetuar somente o tratamento de dados pessoais minimamente necessários para atingir aos propósitos de negócio da CBMM, responsabilizando-se no caso de tratamento de dados pessoais realizados em desacordo com as leis e/ou com o contrato acordado;
- Garantir por meio de um canal formal, o contato do Encarregado de Proteção de Dados, autorizado a responder dúvidas e/ou consultas relacionadas ao tratamento de dados pessoais;
- Garantir que o tratamento de dados pessoais, especialmente dados pessoais sensíveis e/ou dados pessoais de crianças e adolescentes sejam realizados observando todos os princípios da lei, e conferindo as medidas de proteção adequadas e compatíveis com a sensibilidade dos dados;
- Garantir que nenhum dado pessoal decorrente da execução do contrato seja armazenado de forma descentralizada ou em dispositivos sem as devidas medidas de segurança adequadas. Equipamentos locais devem ser evitados, salvo somente se tiver sido implementadas técnicas de criptografia;
- Garantir que transferências internacionais de dados pessoais, quando aplicáveis, sejam realizadas única e exclusivamente com os serviços estabelecidos em contrato, observando todos os mecanismos previstos pela legislação de proteção de dados e demais leis aplicáveis;

- Prestar auxílio e/ ou notificar assim que identificado (via e-mail dpo@cbmm.com) qualquer violação ou incidente de segurança da informação envolvendo os dados pessoais tratados, informando inclusive sobre as providencias adotadas para minimização de impactos em primeiro momento. Para este item favor observar as diretrizes disponíveis pela Autoridade Nacional de Proteção de Dados.

5.10.2. Incidente de Segurança da Informação

- Será considerada como premissa a todos os fornecedores e parceiros CBMM quando da ocorrência de um incidente de segurança da informação que gere riscos, impacto aos serviços, dados ou qualquer transtorno para as operações da CBMM, como canal para a comunicação do incidente de segurança.

O gestor da terceirizada informará o gestor do contrato, que de posse de todas as informações, realizará a abertura do incidente via ITSM da CBMM, acessando – (Reportar Incidente de Segurança da Informação).

5.11. Violações das Diretrizes

As violações a estas diretrizes incluem, mas não se limitam a:

- Falta de reporte imediato nos casos em que a tal comunicação deva ser feita conforme estabelecido neste documento;
- Quaisquer ações ou omissões que tenham o potencial de acarretar perda financeira e/ou danos à imagem da CBMM;
- Uso dos dados, informações, equipamentos, programas, softwares, arquivos informatizados, sistemas ou outros recursos tecnológicos para propósitos ilícitos, incluindo mas não se limitando a violação de legislações, regulamentos internos, e ao Código de Ética e Conduta da CBMM disponível na intranet;
- Uso de softwares não licenciados e/ou equipamentos sem notas fiscais;
- Uso ou armazenamento indevido de dados bem como divulgação não autorizada de informações confidenciais, segredos comerciais ou outras informações, sem a autorização prévia e por escrito da CBMM.
- Deixar de observar os requisitos legais mínimos aplicáveis para a adequação dos processos relacionados ao tratamento de dados pessoais, conforme previsto na legislação;
- Disponibilizar, compartilhar ou transferir dados pessoais tratados à terceiros que não sejam contratados ou subcontratados (quando aplicável) e que não faça parte das atividades previstas em contrato;
- Utilizar de meios inadequados ou inseguros para transferir ou compartilhar os dados pessoais tratados;
- Tratar dados pessoais fora do escopo do contrato acordado ou após a extinção do contrato. O fornecedor deverá proceder com a exclusão definitiva ou implementar técnicas de anonimização quando possível, após o término do contrato ou quando solicitado pela CBMM, salvo exceções para retenção dos dados como fundamento legal ou obrigações legais.

5.12. Infrações

Em caso de descumprimento, a CBMM poderá adotar a seu critério todas as medidas legais e contratuais cabíveis.

5.13. Considerações Finais

Dúvidas relacionadas ao cumprimento deste documento deverão ser direcionadas ao time de Segurança da Informação da CBMM ou ao Gestor do contrato. O documento está sujeito a mudanças e atualizações que, assim que transmitidas ao Terceiro, deverão ser imediatamente observadas.
Em caso de dúvidas relacionadas as obrigações e responsabilidades enquanto agente de tratamento entre em contato conosco através do dpo@cbmm.com

6. ATUALIZAÇÕES

Este documento, juntamente com outros procedimentos complementares ou aplicáveis deverão ser revisados com periodicidade máxima de 02 (dois anos) ou quando mudanças significativas que afetem as diretrizes ou gestão das medidas técnicas e administrativas se fizerem necessárias.

7. ANEXOS

Anexo 1 – Histórico das Revisões.

1. PURPOSE

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

To establish guidelines and practices in order to ensure the protection of personal data processed by suppliers and third parties on behalf of CBMM or jointly, in accordance with applicable data protection laws and other relevant regulations.

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. It also applies to all suppliers, partners, service providers, consultants and any other third party that processes personal data on behalf of CBMM or in collaboration with it.

3. DEFINITIONS AND ACRONYMS

Anonymization: A data processing technique that removes or modifies information that can identify a person. This technique results in data that cannot be associated with any specific individual.

Asset: Anything that is of value to CBMM's business and needs to be protected.
Controller: A natural or legal person, governed by public or private law, who is responsible for decisions regarding the processing of personal data.

Data Protection Officer (DPO): The person appointed by CBMM to act as a contact between the company, the data subjects and the National Data Protection Authority.

Data Subject: A natural person to whom the personal data that are subject to processing refers.

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

International Transfer: Transfer of data to a foreign country or international organization of which the country is a member.

ITSM: Information Technology service management tool for opening calls.
Legal Basis: Hypotheses provided for in the law that authorizes the performance of personal data processing activities for specific purposes and duly informed to the data subjects.

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 (Multiple Factor Authentication): A method to attest to someone's identity to grant access to information, systems, applications, among others.

Processor: A natural or legal person, under public or private law, that processes personal data on behalf of the controller.

Personal Data: Information related to an identified or identifiable natural person.
Processing: Any operation carried out with personal data, such as collection, storage, use, processing, sharing or deletion.

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

ROPA: Record of data processing activities.

Sensitive Data: Personal data related to racial, ethnic origin, religious belief, political opinion, membership in a union or any organization of a religious, philosophical or political nature, in addition to data regarding health, sexual life, genetic or biometric data.

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.

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

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.

-
- Ensure to inform the start and end of the contract to those involved in CBMM.
- Ensure and verify the dissemination regarding the execution of training and guidelines related to CBMM's information security for service provision.
- Ensure the action of onboarding and offboarding of third parties.
- Ensure the dissemination of communication channels – post-implemented projects.

4.3. Information Security

- Define good practices, as well as promote the updating of and compliance with such practices;
- Monitor, follow up, address, and direct Information Security Incidents to the involved parties.

4.4. IT Governance

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

4.5. Privacy Office

- Define Privacy and Data Protection practices;
- Resolve queries from third parties and partners through the channel provided in this document.

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 via e-mail dpo@cbmm.com. link.

5.3. 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.

5.4. 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.

5.5. 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.
- The compromise of a password is considered an Information Security Incident. If there is any indication of a security incident, not just password compromise, the third party must (i) change the password immediately and (ii) report the incident as per item 5.10.2

5.6. 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.

5.7. 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.

5.8. 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.

5.9. 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.

5.10. Privacy and Data Protection

5.10.1. Obligations of suppliers and partners

The following shall be considered as a premise for all CBMM suppliers and partners when processing personal data:

- To adopt technical, administrative, and security measures for the information processed in order to protect the data against improper or unauthorized access in accordance with the governing contract. These measures may include, but are not limited to:

- Management and traceability of access to information and data;
- The use of technical measures to protect personal data (antivirus, encryption, MFA (when possible), among others;
- Incident reporting plans related to information security, including data protection requirements, as per Data Protection Authority guidelines.

- To act in accordance with CBMM's instructions, never using the processed data for commercial purposes, or advantages or purposes not provided for in the contract.
- To ensure that obligations of confidentiality, information security and protection of the processed personal data extend to employees, contractors and subcontractors.
- To bear full responsibility for any damage, whether direct or indirect, resulting from the improper processing of personal data in an irregular manner or contrary to that established in the contract, and also having to compensate in the event of non-compliance.
- To cooperate with CBMM to resolve issues involving compliance with the data processed, responding to the requested questionnaires and evaluations, and providing the necessary documentation to demonstrate compliance with legal obligations and obligations established in the contract.
- To cooperate and provide assistance to CBMM, within the limits of the obligations imposed in the event of compliance with the Data Protection Authority, with the data holder, or with any other government authority on issues related to the processing of personal data.

- To document the processes and maintain an updated record (ROPA) of all personal data processing activities carried out, also including the indication of international transfers of personal data that may have been carried out, in addition to the guarantees and mechanisms adopted to protect the information.
- To only process personal data that is minimally necessary to achieve CBMM's business purposes, taking responsibility in the event of personal data processing carried out in disagreement with the law and/or the agreed contract.
- To ensure, through an official channel, contact with the Data Protection Officer, authorized to respond to questions and/or queries related to the processing of personal data.
- To ensure that the processing of personal data, especially sensitive personal data and/or personal data of children and adolescents, is carried out in compliance with all principles of the law, and ensuring appropriate protection measures compatible with the sensitivity of the data.
- To ensure that no personal data arising from the execution of the contract is stored in a decentralized manner or on devices without the appropriate security measures. Local equipment should be avoided, except if encryption techniques have been implemented.
- To ensure that international transfers of personal data, when applicable, are carried out solely and exclusively with the services established in the contract, observing all mechanisms provided for by the GDPR and other applicable laws.
- To provide assistance and/or to notify as soon as any information security breach or incident involving the processed personal data is identified (via email dpo@cbmm.com), including information on the measures taken to minimize impacts in the initial phase. For this item, please follow the guidelines provided by the Data Protection Authority.

5.10.2. Information Security Incident

- It will be considered a premise for all CBMM suppliers and partners that, in the event of an information security incident that generates risks, impacts services, data, or any disruption to CBMM operations, the third-party manager will inform the contract manager as the channel for communicating the security incident. The contract manager, having all the information, will open the incident via CBMM's ITSM, accessing – (Report Information Security Incident).

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.
- To fail to observe the minimum legal requirements applicable to the adequacy of processes related to the processing of personal data, as provided for in the legislation.
- To make available, share, or transfer processed personal data to third parties that are not contracted or subcontracted (when applicable) and that are not part of the activities provided for in the contract.
- To use inadequate or insecure means to transfer or share processed personal data.
- To process personal data outside the scope of the agreed contract or after the contract termination. The supplier must proceed with the definitive deletion or implement anonymization techniques when possible after the termination of the contract or when requested by CBMM, apart from exceptions for data retention as a legal basis or legal obligations.

5.12. Infringements

In the event of non-compliance, CBMM may adopt at its discretion all applicable legal and contractual measures.

5.13. 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.
In case of doubts regarding this topic, or about your obligations and responsibilities as a data processing operator, please contact us at dpo@cbmm.com.

6. UPDATES

This document, along with other complementary or applicable procedures related to Information Security and Privacy, must be reviewed at least every 2 (two) years or when significant changes that affect the guidelines or management of technical and administrative measures are necessary.

7. EXHIBITS

Exhibit 1 – Reviews.

VERSÃO VERSION	ITEM	HISTÓRICO DA REVISÃO HISTORY OF REVISION	DATA DA REVISÃO REVIEW DATE
00	Todos *All*	Emissão inicial do documento em substituição ao PR-GSTI-29 versão 1.0 *Initial issuance of the document replacing PR-GSTI-29 version 1.0*	25.01.24 *01.25.24*
01	Todos *All*	Revisão geral e inclusão do item 5.10 *General review and inclusion of item 5.10*	29.08.24 *08.29.24*
02	4.2	Revisão do item incluindo atividades do Gestor do contrato. *Item review including activities of the Contract Manager.*	03.04.25 *04.03.25*
	4.3	Revisão do item – incluído – ações para segurança da informação. *Item review – included – actions for information security.*	
	5.5	Revisão do item – incluído – não apenas comprometimento da senha. *Item review – included – not just password compromisse.*	
	5.10.2	Revisão do item – incluído - responsabilidade do gestor do fornecedor e gestor do contrato. *Item review – included – responsability for the outsourced manager and contract manager.*	