

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Checkmob's Information Security

and Compliance Committee

Versão Português

English Version Included

Informação Pública

Este documento é de propriedade da Checkmob e contém informações que são proprietárias, confidenciais ou restritas à divulgação. Se você não estiver autorizado a recebê-las, favor devolver este documento ao proprietário acima mencionado. A divulgação, distribuição, reprodução ou uso total ou parcial deste documento por qualquer terceiro que não seja a pessoa a quem se destina, sem o consentimento prévio por escrito da Checkmob, é estritamente proibida.

SUMÁRIO

[**1. CONCEITOS, TERMOS E ABREVIAÇÕES 4**](#_icmd1ibrtw2j)

[**2. INTRODUÇÃO 4**](#_n2vk1suy8ofp)

[**3. PRINCÍPIOS 4**](#_vfm4a18xp2jv)

[**4. OBJETIVOS 4**](#_vfm4a18xp2jv)

[**5. ABRANGÊNCIA 5**](#_vfm4a18xp2jv)

[**6. ATRIBUIÇÕES 5**](#_vfm4a18xp2jv)

[**7. DIRETRIZES 7**](#_1ux3iibf631)

[**8. SEGURANÇA EM RECURSOS HUMANOS 8**](#_nbai7gp5guw)

[**9. GESTÃO DE ATIVOS 11**](#_cz7aifr4q5po)

[**10. POLÍTICAS COMPLEMENTARES (PC) 12**](#_e0m2b5xzip0s)

[**11. COMPROMISSO E PENALIDADES 13**](#_1mp40kalf6f4)

[**12. REFERÊNCIAS LEGAIS E NORMATIVAS 13**](#_jil9mid5o7b8)

[**13. DISPOSIÇÕES FINAIS 13**](#_ce4ptusk92mw)

[**14. ENGLISH VERSION OF THIS POLICY 15**](#_u6u7zy99nw4d)

HISTÓRICO DE VERSÕES

| DATA | VERSÃO | AUTOR | DESCRIÇÃO |
| --- | --- | --- | --- |
| 27/05/2021 | 1.0 | Lucas Willian Farias | Criação do documento |
| 21/03/2024 | 1.2 | Felipe Antunes Silva | Atualização dos membros do CSIC |
| 26/03/2024 | 1.3 | Norton Luiz Ritzmann | Nova formatação e inclusão da versão em Inglês. |
| 06/08/2024 | 1.4 | Information Security  and Compliance Committee | Revisão geral e inclusão da política de Segurança em Recursos Humanos, Gestão de Ativos e inclusão de novas políticas complementares. |

# CONCEITOS, TERMOS E ABREVIAÇÕES

Devem ser compreendidos nesta Política como:

Incidente de Segurança da Informação: Evento que decorre da exploração de uma vulnerabilidade do sistema de segurança da informação e que, portanto, pode afetar questões relacionadas à confidencialidade e integridade dos dados.

Riscos de Segurança da Informação: Todo e qualquer risco associado à violação de normas, procedimentos e requisitos de segurança, seja físico ou virtual.

Ativos de tecnologia: estações de trabalho, servidores, e-mail, dispositivos móveis, componentes da rede, entre outros.

Sistemas de tecnologia: expressão utilizada para descrever um sistema, seja ele automatizado, manual, que abrange pessoas, máquinas e/ou métodos organizados para coletar, processar, transmitir e disseminar dados que representam informação para o usuário e/ou cliente.

# 

# INTRODUÇÃO

Esta Política de Segurança da Informação estabelece diretrizes, princípios e responsabilidades, além de orientar na execução das ações relacionadas ao tratamento das informações e ao uso adequado de ativos e/ou informações pelos colaboradores, estagiários, terceiros, fornecedores, parceiros e outras partes interessadas nos negócios da CHECKMOB S/A.

# PRINCÍPIOS

O presente documento norteia-se pelos princípios:

a) Confidencialidade: tem por objetivo garantir que os dados coletados e utilizados sejam de conhecimento exclusivo de pessoas autorizadas a acessá-los;

b) Integridade: os dados utilizados devem se manter íntegros ao seu propósito, sem que sejam realizadas modificações indevidas (acidentais ou propositais), sem a devida autorização;

c) Disponibilidade: garante que as informações e dados estejam disponíveis a todas as pessoas autorizadas a tratá-las.

# OBJETIVOS

Esta Política de Segurança da Informação define os princípios, responsabilidades e diretrizes acerca da segurança cibernética e a informação na CHECKMOB S/A, a qual se mantém comprometida com a observância da legislação em vigor aplicável e às boas práticas para a segurança da informação. O documento possui diretrizes para proteção de processos, tecnologias e ferramentas, bem como controles para assegurar a segurança da informação, dos ativos e ambientes que suportam o armazenamento e processamento de informações.

Objetivos específicos:

1. Garantir confidencialidade, integridade, disponibilidade e autenticidade da informação;
2. Otimizar mecanismos para segurança da informação;
3. Assegurar que as informações sejam prontamente identificáveis e recuperáveis de acordo com sua aplicação;
4. Controlar informações geradas na organização;
5. Garantir adequada utilização da Tecnologia da Informação.

# ABRANGÊNCIA

Esta Política tem relevância organizacional, sendo aplicável a todos os colaboradores, funcionários, sócios, estagiários, parceiros e partes interessadas.

# ATRIBUIÇÕES

## Comitê de Segurança da Informação e Compliance (CSIC)

Fazem parte do Comitê de Segurança da Informação e Compliance: (i) Norton Luiz Ritzmann, CEO; (ii) André Zacarias Neto, Diretor de Vendas e Serviços; (iii) Lucas Landarin Zanona, Diretor de Tecnologia e; (iv) Felipe Antunes Silva, DPO.

Constituem-se atribuições do CSIC:

1. Propor ajustes, aprimoramentos e modificações desta Política;
2. Analisar os casos de violação desta Política e das Normas de Segurança da Informação, comunicar à Diretoria, quando for necessário;
3. Gerenciar, coordenar, orientar, avaliar e promover a implantação das ações, atividades e projetos relativos à Segurança da Informação na CHECKMOB S/A, promovendo ações de interesse da empresa, programas educacionais e de conscientização do capital humano;
4. Prover treinamentos e capacitação sobre segurança da informação.

## Atribuições das macro áreas da Checkmob

A responsabilidade direta pela segurança da informação de cada área da empresa é do diretor correspondente, conforme o organograma estabelecido, o qual também deverá, caso necessário, nomear um interlocutor do tema junto ao comitê e DPO.

### 6.2.1 Área Tecnológica

1. Manter o ambiente tecnológico estável, operacional, atualizado, íntegro, disponível e monitorado;
2. Relatar mensalmente ao Comitê ou representante indicado os incidentes de Segurança da Informação identificados, ocorridos no ambiente tecnológico.
3. Elaborar e atualizar os procedimentos relativos à operacionalidade do ambiente tecnológico;
4. Garantir que os requisitos de Segurança da Informação constem nas aquisições e/ou implementações tecnológicas.

### 6.2.2 Área Comercial

1. Desenvolver e implementar estratégias comerciais de acordo as regras de segurança da informação;
2. Observar as regras estabelecidas na Política da Segurança da Informação ao adquirir novos clientes e gerenciar relacionamentos com clientes (novos e existentes);
3. Fornecer suporte técnico dos produtos e serviços oferecidos pela CHECKMOB S/A respeitando os requisitos mínimos de segurança.

### 6.2.3 Diretoria Administrativa

1. Gerir as informações relativas à contratação de novos colaboradores;
2. Estipular, junto ao departamento jurídico, contratos de confidencialidade de dados, com o objetivo de resguardar o sigilo de informações internas;
3. Proporcionar, sempre que possível, treinamentos a respeito das medidas de segurança estipuladas na PSI;
4. Zelar, com base nas regras internas de segurança, pelos dados financeiros e administrativos da organização;

## Atribuições relacionadas a terceiros:

## 

Colaboradores, estagiários, terceiros, fornecedores, parceiros e partes interessadas das empresas relacionadas à CHECKMOB S/A são responsáveis por:

1. Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI;
2. Conhecer e cumprir as normas e orientações estabelecidas nesta Política e demais Regulamentos que compõem a Política de Segurança da Informação da CHECKMOB S/A;
3. Informar as situações que comprometam a segurança das informações na organização;
4. Toda informação criada, modificada no exercício das funções e qualquer informação contida em mensagens do correio eletrônico corporativo deve ser tratada como referente ao negócio da CHECKMOB S/A, não devendo ser considerada como pessoal, particular ou confidencial, mesmo que arquivadas na sua pasta pessoal;
5. Garantir que seja conhecida e cumprida a proibição de compartilhamento ou negociação de credencias (ID, senhas, crachás, tokens e similares);
6. Relatar prontamente à área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, etc.

# DIRETRIZES

Na gestão de riscos cibernéticos e da informação deverão ser observados:

1. **Responsabilidade e comprometimento:** todos os colaboradores, funcionários, sócios, fornecedores, terceiros e parceiros, em qualquer vínculo ou nível hierárquico, são responsáveis pela proteção e segurança dos ativos e informações que tenham acesso ou contato, tanto em ambiente físico, quanto virtual, independentemente das medidas tecnológicas implementadas para garantir a segurança.
2. **Acesso de dados e informações gerenciadas:** o acesso lógico e físico aos ativos de informação deve ser devidamente controlado, rastreável, restrito aos usuários com autorização e que necessitam do acesso às informações para o desempenho de suas funções. O processo de gestão de acesso deve considerar a proteção contra acesso, alteração, destruição ou publicação não autorizada. Todo o controle de acesso às informações deve possui recursos que permitam a sua rastreabilidade
3. **Gerenciamento remoto de dados e informações:** compreende a gestão remota de equipamentos da CHECKMOB S/A, em modo desktop e mobile, o que possibilita o escaneamento dos equipamentos, atualização do antivírus, instalação e correções de vulnerabilidades, bloqueamento de portas USB e Sites, acesso à relação de sites visitados, bem como controle de wi-fi que o equipamento poderá acessar. Poderá, ainda, estipular requisitos básicos de segurança relacionado à redes domésticas, regras e diretrizes sobre o acesso de familiares e visitantes ao equipamento, além de procedimentos de auditoria e monitoramento da segurança;
4. **Proteção em camadas:** a arquitetura tecnológica que suporta o processamento e armazenamento de informação deve considerar a proteção em camadas e segmentação de rede, com o objetivo de mitigar possível comprometimento de uma das camadas de defesa.
5. **Monitoramento de ativos:** os ativos de tecnologia que suportam o processamento e armazenamento de informação devem ser devidamente protegidos, monitorados e seus controles avaliados periodicamente quanto a confidencialidade, integridade e disponibilidade. Os ativos de tecnologia devem ser inseridos em processo de gerenciamento contínuo de vulnerabilidades
6. **Proteção e armazenamento de dados:** o processamento e armazenamento de dados por parte da CHECKMOB S/A ocorre apenas em provedores de serviço condizentes com as legislações e/ou regulamentações aplicáveis e vigentes, devendo esta regra ser observada por todos os colaboradores e demais interessados.
7. **Processo de contratação de soluções tecnológicas:** o processo de desenvolvimento ou contratação de soluções tecnológicas deve incluir a análise prévia de segurança cibernética e da informação, e, posteriormente, monitorados através do processo de gerenciamento contínuo de vulnerabilidades. Havendo possibilidade, deverá a CHECKMOB S/A solicitar ao fornecedor atualização de suas tecnologias a fim de proporcionar maior segurança.
8. **Proteção de dados e privacidade:** o desenvolvimento de sistemas de tecnologia ou adoção de tecnologias contratadas deve considerar a privacidade desde a concepção e a proteção de dados como padrão. As soluções de processamento ou armazenamento de dados devem ser analisadas previamente quanto a proteção técnica e jurídica com o objetivo de assegurar a conformidade da privacidade exigida em legislação vigente
9. **Prevenção e Auditoria:** as tecnologias utilizadas pela CHECKMOB S/A, desenvolvidas internamente ou soluções contratadas, devem possuir recursos de rastreabilidade de transações. As trilhas de auditoria devem ser protegidas através de recursos para assegurar a confidencialidade, integridade e disponibilidade.
10. **Plano de continuidade dos negócios:** todo ativo ou infraestrutura crítica aos negócios da CHECKMOB S/A, clientes e parceiros deve ser contemplado no programa de continuidade de negócios e recuperação de desastres. O plano de continuidade de negócios deve ser testado periodicamente e o registro dos testes preservados para fins de auditoria.
11. **Plano de resposta à incidentes:** os incidentes de segurança de informação e cibernética devem ser suportados por um plano efetivo de resposta ao incidente devidamente atualizado, inclusive quando ocorrido com parceiros da CHECKMOB S/A, considerando as boas práticas e legislação/regulamentação aplicável e as seguintes etapas: detecção, mitigação emergencial e análise de causa raiz. O plano de resposta a incidentes deve considerar a classificação dos dados para o tratamento de resposta em tempo hábil, condizente com a criticidade do mesmo e seu impacto aos negócios e dados sob custódia. O plano de resposta a incidentes deve incluir a gestão de serviços de processamentos e armazenamento de dados em nuvem. Também poderão ser elaborados cenários de incidentes para realização periódica de testes de continuidade de segurança.

# SEGURANÇA EM RECURSOS HUMANOS

A segurança em recursos humanos é um componente fundamental da política de segurança da informação da CHECKMOB S/A, abrangendo todos os estágios de envolvimento de funcionários, estagiários, contratados e terceiros com a empresa. Esta seção define as diretrizes para assegurar que todos os indivíduos compreendam suas responsabilidades em relação à segurança da informação e atuem de maneira a proteger os dados e ativos da organização.

## Recrutamento e Seleção

* Verificação de antecedentes, qualificação e referências

Todos os candidatos selecionados para trabalhar na Checkmob devem passar por uma verificação de antecedentes, de qualificações e de referências profissionais. O nível e rigor da verificação deve ser proporcional aos requisitos de negócio, grau de acesso a informações ou sistemas críticos e deve ser realizada de forma a respeitar a privacidade do profissional e as leis aplicáveis.

* Termos de contrato

Os contratos de trabalho e acordos com terceiros devem incluir cláusulas de confidencialidade e de conformidade com as políticas de segurança da informação da CHECKMOB S/A.

## Durante a vigência do contrato de trabalho

* Treinamento e conscientização

Todos os novos funcionários e terceiros devem receber um treinamento inicial em segurança da informação, que inclui as políticas, procedimentos e responsabilidades associadas. Treinamentos de reciclagem devem ser realizados a cada 12 meses para assegurar que todos estejam atualizados sobre as práticas e ameaças atuais.

* Responsabilidades de Segurança da Informação

As responsabilidades individuais em relação à segurança da informação devem ser claramente definidas e comunicadas a todos os funcionários e terceiros. Isso inclui a responsabilidade de relatar incidentes de segurança e cumprir com as políticas estabelecidas.

* Monitoramento e avaliação

O desempenho em relação à conformidade com as políticas de segurança da informação deve ser avaliado regularmente. Medidas corretivas devem ser implementadas em caso de não conformidade.

## Encerramento ou mudança de Contrato

* Devolução de ativos

No término do contrato de trabalho ou de prestação de serviços, todos os ativos da empresa, incluindo equipamentos, documentos e dados, devem ser devolvidos. Isso inclui a remoção de quaisquer acessos a sistemas da empresa.

* Revogação de Acessos

O acesso lógico e físico aos sistemas e instalações da empresa deve ser revogado imediatamente após o encerramento do contrato. Isto inclui o acesso a redes, sistemas de e-mail e qualquer outro recurso da empresa.

* Confidencialidade Pós-Contrato

Os ex-funcionários e terceiros devem ser lembrados de suas obrigações contínuas em relação à confidencialidade das informações da CHECKMOB S/A. A divulgação não autorizada de informações após o término do vínculo pode resultar em ações legais.

## Gerenciamento de Incidentes

* Relato de Incidentes

Todos os funcionários e terceiros têm a obrigação de relatar imediatamente qualquer incidente de segurança da informação, suspeito ou confirmado, ao Comitê de Segurança da Informação e Compliance (CSIC) ou ao DPO, através dos e-mails [dpo@checkmob.com](mailto:dpo@checkmob.com) ou [privacy@checkmob.com](mailto:privacy@checkmob.com).

## Responsabilidades

* Gestão de Recursos Humanos

A equipe de Recursos Humanos, subordinada à Diretoria Administrativa (6.2.3), é responsável por implementar processos de recrutamento e seleção que incluam verificações de segurança, além de garantir que todos os contratos contenham cláusulas apropriadas de segurança da informação. A área também é responsável por implementar processos de desligamento que estejam em conformidade com esta Política.

* Gestão de Segurança da Informação

É responsabilidade do Comitê de Segurança da Informação da CHECKMOB S/A, conforme o item 6.1, "d", fornecer os treinamentos necessários e garantir que as políticas e procedimentos de segurança sejam seguidos.

* Gerentes e coordenadores

São responsáveis por assegurar que seus subordinados diretos compreendam e cumpram com as políticas de segurança da informação. Eles devem monitorar o cumprimento e atuar em casos de não conformidade.

# GESTÃO DE ATIVOS

A Checkmob reconhece a importância dos ativos de informação para o sucesso contínuo de suas operações e para a garantia da segurança das informações sensíveis. Esta seção estabelece diretrizes para a atribuição de propriedade e responsabilidade pelos ativos de informação.

## Diretrizes

1. Todos os ativos devem ser catalogados em um sistema de inventário centralizado, permitindo um monitoramento eficiente.
2. Os proprietários de ativos devem ser definidos com base em conhecimento técnico e responsabilidades funcionais.
3. A política de uso aceitável dos ativos deve ser comunicada a todos os colaboradores e reforçada regularmente.
4. Processos de devolução de ativos devem incluir verificações de segurança.

A responsabilidade pelos ativos é um componente fundamental da estratégia de segurança cibernética da Checkmob, garantindo a proteção dos dados e informações da empresa.

## Identificação dos ativos

A Checkmob mantém e deverá manter sempre atualizado, um inventário detalhado de todos os ativos associados à informação. Isso inclui hardware, software, sistemas e documentação. Cada ativo deverá continuamente estar identificado, registrado e atualizado em ferramentas apropriadas.

## Uso aceitável dos ativos

O uso adequado e seguro dos ativos é fundamental para garantir a proteção e a confidencialidade dos dados da organização. Todos os colaboradores e terceiros deve respeitar as seguintes normas:

1. O acesso aos ativos da empresa é restrito aos colaboradores que possuam autorização oficial.
2. O acesso deve ser limitado ao escopo das responsabilidades individuais e ao propósito de trabalho.
3. Os ativos da Checkmob devem ser utilizados exclusivamente para fins profissionais relacionados às atividades da empresa.
4. O uso para atividades pessoais ou não relacionadas ao trabalho são permitidos apenas mediante autorização especial.
5. A violação das normas por parte de colaboradores e terceiros poderá acarretar em processo disciplinar, na proporção da gravidade da falta, a juízo do Comitê de Segurança da Informação em conjunto com a Diretoria da empresa.

## Devolução de Ativos

Ao término de seu contrato ou quando solicitado, os colaboradores deverão devolver todos os ativos sob sua responsabilidade. Ao realizar a devolução, os ativos serão verificados para garantir que todos os dados sejam removidos de maneira segura e que não haja risco de vazamento de informações.

## Segurança de Dispositivos Endpoint

Todos os dispositivos endpoint utilizados pela Checkmob, incluindo laptops, desktops, e dispositivos móveis, devem cumprir os seguintes requisitos de segurança:

1. **Antivírus**: Todos os dispositivos devem ter software antivírus atualizado e configurado para realizar verificações regulares.
2. **Senhas Fortes**: Senhas fortes e únicas devem ser utilizadas para acessar os dispositivos. Estas senhas devem ser trocadas regularmente.
3. **Atualizações de Software**: Sistemas operacionais e software devem ser mantidos atualizados com os patches de segurança mais recentes.
4. **Bloqueio de Tela**: Dispositivos devem ser configurados para bloquear a tela automaticamente após um período de inatividade, exigindo autenticação para desbloquear.

Essas medidas garantem que os dispositivos endpoint, que são frequentemente alvos de ataques cibernéticos, estejam protegidos contra ameaças e contribuem para a segurança geral da informação na Checkmob.

## 

# POLÍTICAS COMPLEMENTARES (PC)

PC01 - Política de Continuidade de Negócios e Recuperação de Desastres

PC02 - Política de Segurança de Servidores

PC03 - Política de Gestão de Vulnerabilidade

PC04 - Política de Segurança de Rede

PC05 - Política de Segurança de Aplicações

PC06 - Política de Controle de Acesso

PC07 - Política de Classificação da Informação

PC08 - Política de Gestão operações de TI

PC09 - Plano de Resposta a Incidentes

PC09 - Tech Stack

PC11 - Política de Retenção e Exclusão de Dados

PC12 - Data Flow Map

# COMPROMISSO E PENALIDADES

Os colaboradores, estagiários, terceiros, fornecedores, parceiros e partes interessadas das empresas relacionadas à CHECKMOB S/A que, de alguma maneira, venham a apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, arquivo ou programa de computador, estará sujeito às penalidades previstas na legislação nacional;

O colaborador infrator poderá ser notificado e a ocorrência da transgressão será imediatamente comunicada ao seu chefe imediato e ao Comitê de Segurança da Informação e Compliance (CSIC).

Todas as partes interessadas, ao tomarem conhecimento de qualquer incidente de segurança da informação, devem informar o ocorrido imediatamente ao DPO, integrante do Comitê de Segurança da Informação e Compliance (CSIC), através do e-mail [dpo@checkmob.com](mailto:dpo@checkmob.com).

# **REFERÊNCIAS** LEGAIS E NORMATIVAS

1. Lei Geral de Proteção de Dados - nº 13.709/2018 (dispõe sobre a regulamentação geral de proteção de dados no Brasil);
2. Marco Civil da Internet - nº 12.965/2014 (Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;
3. ISO/IEC 27000
4. ABNT NBR ISO 27001
5. ABNT NBR ISO 27002
6. ABNT NBR ISO 27701

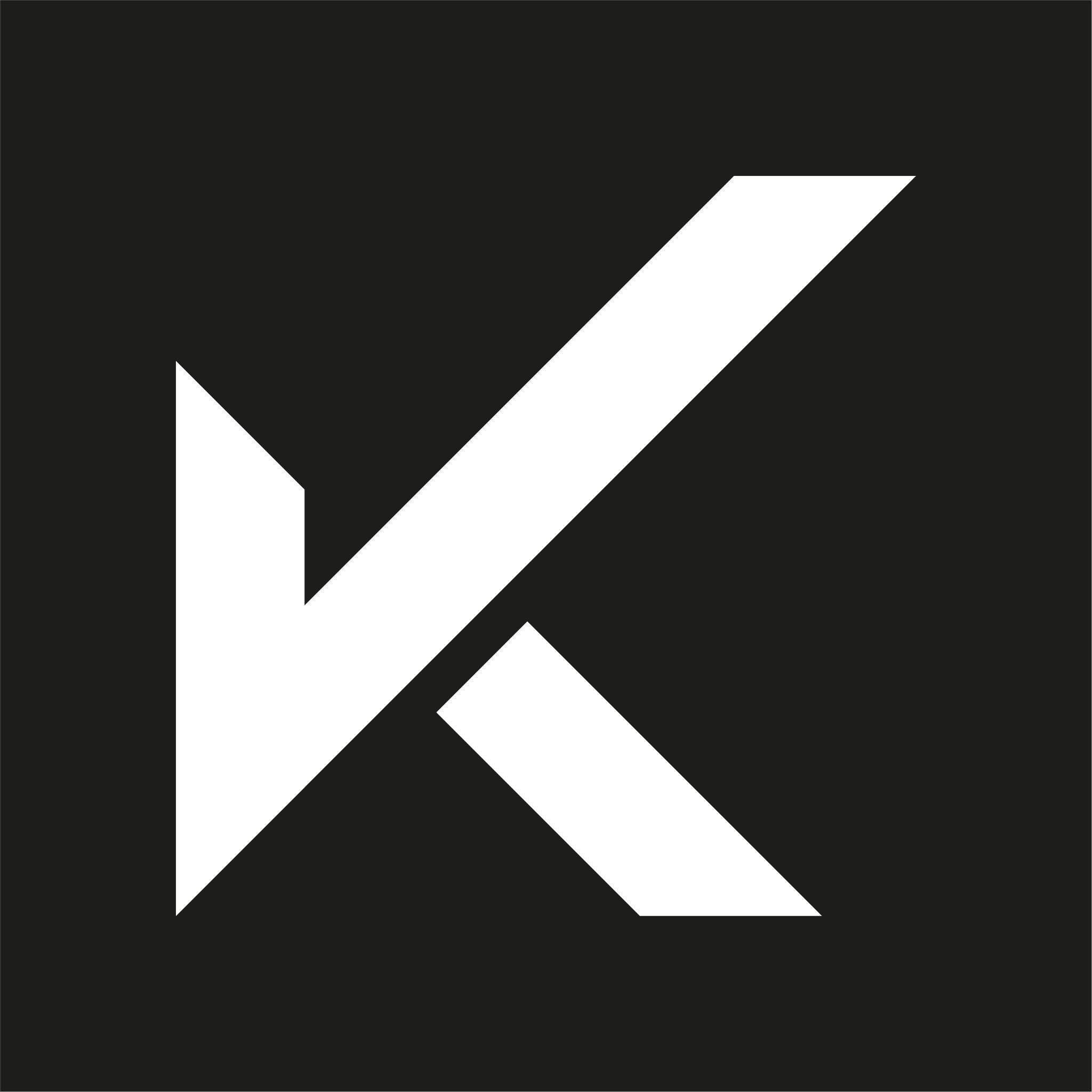
# DISPOSIÇÕES FINAIS

Esse documento foi criado para formalizar e manter o processo de gestão de Segurança da

Informação na Organização.

Esse documento será gerido e atualizado bi-anualmente ou após mudanças significativas, atendendo às melhores práticas de SI.

# ENGLISH VERSION OF THIS POLICY



INFORMATION SECURITY POLICY

Checkmob's Information Security

and Compliance Committee

English Version

Public Information

This document is the property of Checkmob and contains information that is proprietary, confidential, or restricted in disclosure. If you are not authorized to receive it, please return this document to the aforementioned owner. The disclosure, distribution, reproduction, or use, in whole or in part, of this document by any third party other than the intended recipient without the prior written consent of Checkmob is strictly prohibited.

TABLE OF CONTENTS

[**15. CONCEPTS, TERMS, AND ABBREVIATIONS 17**](#_4ky8jsm9ct6b)

[**16. INTRODUCTION 17**](#_ld01qfjhmdk0)

[**17. PRINCIPLES 17**](#_vfm4a18xp2jv)

[**18. OBJECTIVES 17**](#_vfm4a18xp2jv)

[**19. SCOPE 18**](#_vfm4a18xp2jv)

[**20. RESPONSIBILITIES 18**](#_2jxvuc1exyww)

[**21. GUIDELINES 20**](#_bqpk7mm8gqgk)

[**22. HUMAN RESOURCES SECURITY 21**](#_wrg00p2190w5)

[**23. ASSET MANAGEMENT 23**](#_nikvhgigji4g)

[**24. COMPLEMENTARY POLICIES (CP) 24**](#_8hyg46sf3fh6)

[**25. COMMITMENT AND PENALTIES 25**](#_3jgkf8ojc3dp)

[**26. LEGAL AND REGULATORY REFERENCES 25**](#_94f9s9o3m1l0)

[**27. FINAL PROVISIONS 25**](#_lpck8hjltirf)

VERSION HISTORY

| DATE | VERSION | AUTHOR | DESCRIPTION |
| --- | --- | --- | --- |
| 27/05/2021 | 1.0 | Lucas Willian Farias | Document Creation |
| 21/03/2024 | 1.2 | Felipe Antunes Silva | Update of ISCC Members |
| 26/03/2024 | 1.3 | Norton Luiz Ritzmann | New Formatting and Inclusion of English Version |
| 06/08/2024 | 1.4 | Checkmob's Information Security  and Compliance Committee | General review and inclusion of the Human Resources Security Policy, Asset Management, and addition of new complementary policies. |

# CONCEPTS, TERMS, AND ABBREVIATIONS

For the purposes of this Policy, the following definitions apply:

Information Security Incident: An event resulting from the exploitation of a vulnerability in the information security system, which may therefore affect issues related to the confidentiality and integrity of data.

Information Security Risks: Any risks associated with the violation of security norms, procedures, and requirements, whether physical or virtual.

Technology Assets: Workstations, servers, email, mobile devices, network components, among others.

Technology Systems: A term used to describe a system, whether automated or manual, encompassing people, machines, and/or organized methods to collect, process, transmit, and disseminate data that represents information for the user and/or customer.

# 

# INTRODUCTION

This Information Security Policy establishes guidelines, principles, and responsibilities, as well as provides direction for actions related to the handling of information and the appropriate use of assets and/or information by employees, interns, third parties, suppliers, partners, and other stakeholders in CHECKMOB S/A’s business.

# PRINCIPLES

This document is guided by the following principles:

a) Confidentiality: Aims to ensure that the data collected and used is known exclusively to individuals authorized to access it.

b) Integrity: Ensures that the data remains intact and unaltered from its intended purpose, without unauthorized modifications (whether accidental or deliberate).

c) Availability: Ensures that information and data are accessible to all individuals authorized to process them.

# OBJECTIVES

This Information Security Policy defines the principles, responsibilities, and guidelines concerning cybersecurity and information at CHECKMOB S/A, which remains committed to complying with applicable legislation and best practices for information security. The document provides guidelines for the protection of processes, technologies, and tools, as well as controls to ensure the security of information, assets, and environments that support the storage and processing of information.

Specific Objectives:

1. Ensure the confidentiality, integrity, availability, and authenticity of information;
2. Optimize mechanisms for information security;
3. Ensure that information is readily identifiable and recoverable according to its application;
4. Control information generated within the organization;
5. Ensure the proper use of Information Technology.

# SCOPE

This Policy is of organizational relevance and applies to all employees, staff, partners, interns, associates, and stakeholders.

# RESPONSIBILITIES

## Information Security and Compliance Committee (ISCC)

The Information Security and Compliance Committee consists of:(i) Norton Luiz Ritzmann, CEO; (ii) André Zacarias Neto, Director of Sales and Services; (iii) Lucas Landarin Zanona, Director of Technology; and (iv) Felipe Antunes Silva, DPO.

Responsibilities of the ISCC:

1. Propose adjustments, improvements, and modifications to this Policy;
2. Analyze cases of violations of this Policy and Information Security Standards, and communicate with the Directorate when necessary;
3. Manage, coordinate, guide, evaluate, and promote the implementation of actions, activities, and projects related to Information Security at CHECKMOB S/A, including promoting company initiatives, educational programs, and human capital awareness;
4. Provide training and capacity-building on information security.

## Responsibilities of Checkmob's Macro Areas

The direct responsibility for information security within each area of the company lies with the respective director, as per the established organizational chart. The director must also, if necessary, appoint a liaison for the topic with the committee and DPO.

### 6.2.1 Technology Area

1. Maintain the technological environment stable, operational, up-to-date, intact, available, and monitored;
2. Report monthly to the Committee or designated representative any Information Security incidents identified or occurring within the technological environment;
3. Develop and update procedures related to the operation of the technological environment;
4. Ensure that Information Security requirements are included in technological acquisitions and/or implementations.

### 6.2.2 Commercial Area

1. Develop and implement commercial strategies in accordance with information security rules;
2. Adhere to the rules established in the Information Security Policy when acquiring new clients and managing relationships with clients (both new and existing);
3. Provide technical support for the products and services offered by CHECKMOB S/A while respecting minimum security requirements.

### 6.2.3 Administrative Directorate

1. Manage information related to the hiring of new employees;
2. Establish, with the legal department, data confidentiality contracts to safeguard the confidentiality of internal information;
3. Provide training on security measures specified in the PSI whenever possible;
4. Safeguard, based on internal security rules, the financial and administrative data of the organization.

## Responsibilities Related to Third Parties:

## 

Employees, interns, third parties, suppliers, partners, and stakeholders of companies associated with CHECKMOB S/A are responsible for:

1. Adapting norms, processes, procedures, and systems under their responsibility to comply with this PSI;
2. Knowing and adhering to the norms and guidelines established in this Policy and other Regulations that are part of CHECKMOB S/A’s Information Security Policy;
3. Reporting situations that compromise information security within the organization;
4. Treating all information created or modified in the course of their duties, and any information contained in corporate email messages, as pertaining to CHECKMOB S/A's business, and not considering it personal, private, or confidential, even if stored in their personal folder;
5. Ensuring awareness and compliance with the prohibition on sharing or negotiating credentials (ID, passwords, badges, tokens, and similar items);
6. Promptly reporting to the IT department any facts or threats to the security of resources, such as security breaches, vulnerabilities, malfunctions, presence of viruses, etc.

# GUIDELINES

Cybersecurity and Information Risk Management Considerations

1. **Responsibility and Commitment:** All employees, staff, associates, suppliers, third parties, and partners, regardless of their link or hierarchical level, are responsible for the protection and security of the assets and information they access or handle, both in physical and virtual environments, regardless of the technological measures implemented to ensure security.
2. **Access to Managed Data and Information:** Logical and physical access to information assets must be properly controlled, traceable, restricted to authorized users who need access to information for their roles, and protected against unauthorized access, alteration, destruction, or publication. Access control processes must include features that allow traceability.
3. **Remote Management of Data and Information:** Includes remote management of CHECKMOB S/A equipment, both desktop and mobile, allowing for scanning, antivirus updates, vulnerability patches, blocking of USB ports and sites, access to visited site logs, and control over Wi-Fi connections. It may also set basic security requirements for home networks, rules and guidelines for family and visitor access to equipment, and procedures for auditing and monitoring security.
4. **Layered Protection:** The technological architecture supporting information processing and storage should include layered protection and network segmentation to mitigate potential breaches of any defense layer.
5. **Asset Monitoring:** Technology assets supporting information processing and storage must be adequately protected, monitored, and their controls periodically evaluated for confidentiality, integrity, and availability. Technology assets should be included in continuous vulnerability management processes.
6. **Data Protection and Storage:** CHECKMOB S/A processes and stores data only with service providers that comply with applicable and current laws and regulations. This rule must be observed by all employees and other interested parties.
7. **Technology Solution Acquisition Process:** The development or acquisition process for technology solutions must include prior cybersecurity and information security analysis and be monitored through continuous vulnerability management processes. If possible, CHECKMOB S/A should request technology updates from suppliers to enhance security.
8. **Data Protection and Privacy:** The development of technology systems or adoption of contracted technologies must consider privacy by design and data protection as standard. Data processing or storage solutions should be assessed for technical and legal protection to ensure compliance with current privacy legislation.
9. **Prevention and Auditing:** Technologies used by CHECKMOB S/A, whether developed internally or contracted, must include transaction traceability features. Audit trails should be protected to ensure confidentiality, integrity, and availability.
10. **Business Continuity Plan:** All critical assets or infrastructure for CHECKMOB S/A, clients, and partners must be included in the business continuity and disaster recovery program. The business continuity plan should be tested periodically, and test records preserved for audit purposes.
11. **Incident Response Plan:** Information security and cybersecurity incidents should be supported by an effective and up-to-date incident response plan, including incidents involving CHECKMOB S/A partners, considering best practices and applicable laws/regulations, including detection, emergency mitigation, and root cause analysis. The incident response plan should consider data classification for timely response, aligned with the data’s criticality and impact on business and data under custody. The plan should also include the management of cloud data processing and storage services. Additionally, incident scenarios may be developed for periodic security continuity testing.

# HUMAN RESOURCES SECURITY

Human resources security is a fundamental component of CHECKMOB S/A's information security policy, covering all stages of employee, intern, contractor, and third-party involvement with the company. This section outlines the guidelines to ensure that all individuals understand their responsibilities regarding information security and act in a way that protects the organization's data and assets.

## Recruitment and Selection

* Background Checks, Qualifications, and References

All candidates selected to work at Checkmob must undergo background checks, qualification verification, and professional reference checks. The level and rigor of the checks should be proportional to the business requirements, the degree of access to critical information or systems, and should be conducted in a manner that respects the individual's privacy and applicable laws.

* Contract Terms

Employment contracts and agreements with third parties must include confidentiality clauses and compliance with CHECKMOB S/A's information security policies.

## During the Employment Contract

* Training and Awareness

All new employees and third parties must receive initial information security training, which includes the policies, procedures, and associated responsibilities. Refresher training should be conducted every 12 months to ensure that everyone is up-to-date on current practices and threats.

* Information Security Responsibilities

Individual responsibilities regarding information security must be clearly defined and communicated to all employees and third parties. This includes the responsibility to report security incidents and comply with established policies.

* Monitoring and Evaluation

Performance in relation to compliance with information security policies should be regularly assessed. Corrective measures should be implemented in case of non-compliance.

## Contract Termination or Change

* Return of Assets

Upon termination of the employment or service contract, all company assets, including equipment, documents, and data, must be returned. This includes removing any access to company systems.

* Access Revocation

Logical and physical access to company systems and facilities must be revoked immediately upon contract termination. This includes access to networks, email systems, and any other company resources.

* Post-Contract Confidentiality

Former employees and third parties must be reminded of their ongoing obligations regarding the confidentiality of CHECKMOB S/A's information. Unauthorized disclosure of information after the end of the association may result in legal actions.

## Incident Management

* Incident Reporting

All employees and third parties are obligated to immediately report any suspected or confirmed information security incidents to the Information Security and Compliance Committee (ISCC) or the DPO, through the emails dpo@checkmob.com or privacy@checkmob.com.

## Responsibilities

* Human Resources Management

The Human Resources team, under the Administrative Directorate (6.2.3), is responsible for implementing recruitment and selection processes that include security checks, as well as ensuring that all contracts contain appropriate information security clauses. The department is also responsible for implementing termination processes that comply with this Policy.

* Information Security Management

It is the responsibility of CHECKMOB S/A's Information Security Committee, as per item 6.1, "d", to provide necessary training and ensure that security policies and procedures are followed.

* Managers and Coordinators

They are responsible for ensuring that their direct reports understand and comply with information security policies. They must monitor compliance and act in cases of non-compliance.

# ASSET MANAGEMENT

Checkmob recognizes the importance of information assets for the ongoing success of its operations and for ensuring the security of sensitive information. This section sets guidelines for the assignment of ownership and responsibility for information assets.

## Guidelines

1. All assets should be cataloged in a centralized inventory system, allowing for efficient monitoring.
2. Asset owners should be defined based on technical knowledge and functional responsibilities.
3. The acceptable use policy for assets should be communicated to all employees and reinforced regularly.
4. Asset return processes should include security checks.

Ownership of assets is a fundamental component of Checkmob's cybersecurity strategy, ensuring the protection of the company's data and information.

## Asset Identification

Checkmob maintains, and will always maintain, an up-to-date detailed inventory of all information-associated assets. This includes hardware, software, systems, and documentation. Each asset should continuously be identified, recorded, and updated in appropriate tools.

## Acceptable Use of Assets

Proper and secure use of assets is essential to ensure the protection and confidentiality of the organization's data. All employees and third parties must adhere to the following standards:

1. Access to company assets is restricted to employees with official authorization.
2. Access should be limited to the scope of individual responsibilities and work purposes.
3. Checkmob assets should be used exclusively for professional purposes related to company activities.
4. Use for personal or non-work-related activities is permitted only with special authorization.
5. Violations of the standards by employees and third parties may result in disciplinary action, based on the severity of the offense, at the discretion of the Information Security Committee in conjunction with the company's Board.

## Return of Assets

At the end of their contract or when requested, employees must return all assets under their responsibility. Upon return, assets will be checked to ensure that all data is securely removed and that there is no risk of information leakage.

## Endpoint Device Security

All endpoint devices used by Checkmob, including laptops, desktops, and mobile devices, must meet the following security requirements:

1. **Antivirus:** All devices must have up-to-date antivirus software configured to perform regular scans.
2. **Strong Passwords:** Strong and unique passwords must be used to access the devices. These passwords should be changed regularly.
3. **Software Updates:** Operating systems and software must be kept updated with the latest security patches.
4. **Screen Lock:** Devices must be configured to lock the screen automatically after a period of inactivity, requiring authentication to unlock.

These measures ensure that endpoint devices, which are often targets of cyber-attacks, are protected against threats and contribute to the overall information security at Checkmob.

# 

# COMPLEMENTARY POLICIES (CP)

CP01 - Business Continuity and Disaster Recovery Policy

CP02 - Server Security Policy

CP03 - Vulnerability Management Policy

CP04 - Network Security Policy

CP05 - Application Security Policy

CP06 - Access Control Policy

CP07 - Information Classification Policy

CP08 - IT Operation Management Policy

CP09 - Incident Response Plan

CP10 - Tech Stack

CP11 - Data Retention and Deletion Policy

CP12 - Data Flow map

# COMMITMENT AND PENALTIES

Employees, interns, third parties, suppliers, partners, and stakeholders of companies associated with CHECKMOB S/A who, in any way, delete, destroy, modify, or otherwise render useless, in whole or in part, any file or computer program, will be subject to penalties as provided by national legislation.

The offending employee may be notified, and the occurrence of the transgression will be immediately reported to their immediate supervisor and the Information Security and Compliance Committee (ISCC).

All stakeholders, upon becoming aware of any information security incident, must immediately report the incident to the DPO, a member of the Information Security and Compliance Committee (ISCC), via email at [dpo@checkmob.com](mailto:dpo@checkmob.com).

# LEGAL AND REGULATORY REFERENCES

1. General Data Protection Law (Lei Geral de Proteção de Dados) - No. 13,709/2018: Regulates general data protection in Brazil.
2. Brazilian Internet Law (Marco Civil da Internet) - No. 12,965/2014: Establishes principles, guarantees, rights, and duties for the use of the Internet in Brazil.
3. ISO/IEC 27000: Overview and vocabulary for information security management.
4. ABNT NBR ISO 27001: Information security management systems - Requirements.
5. ABNT NBR ISO 27002: Code of practice for information security controls.
6. ABNT NBR ISO 27701: Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management.

# FINAL PROVISIONS

This document has been created to formalize and maintain the process of Information Security Management within the Organization.

This document will be managed and updated biannually or following significant changes, in accordance with best practices in Information Security.