

PC01 - POLÍTICA DE CLASSIFICAÇÃO 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. OBJETIVOS 4**](#_y4ingsouj03)

[**2. DEFINIÇÕES 4**](#_v0cjhsfboosk)

[**3. RESPONSABILIDADES 4**](#_47ipuvunp9o5)

[**4. CLASSIFICAÇÃO DA INFORMAÇÃO 4**](#_ltdagapn28gr)

[**5. GERENCIAMENTO DE INFORMAÇÕES 5**](#_lbponsccwn0r)

[**6. TREINAMENTO E CONSCIENTIZAÇÃO 6**](#_5mkffn24p47n)

[**7. MONITORAMENTO E CUMPRIMENTO 6**](#_bp0hsalpzxgl)

[**8. DISPOSIÇÕES FINAIS 6**](#_t38w06kmrkdn)

[**9. ENGLISH VERSION OF THIS POLICY 7**](#_fll15dlb1ukv)

HISTÓRICO DE VERSÕES

| DATA | VERSÃO | AUTOR | DESCRIÇÃO |
| --- | --- | --- | --- |
| 18/01/2024 | 1.0 | Felipe Antunes | Criação do documento |
| 05/08/2024 | 1.1 | Information Security  and Compliance Committee | Formatação e inclusão da tradução em inglês. |

# OBJETIVOS

A Política de Classificação da Informação da Checkmob tem como objetivo proteger e gerenciar adequadamente todas as informações pertencentes à empresa, garantindo a confidencialidade, integridade e disponibilidade dos dados. Esta política estabelece diretrizes para a classificação de informações em quatro níveis: Confidencial, Restrita, Interna e Público.

# **DEFINIÇÕES**

1. Informação Confidencial: Informações altamente sensíveis que, se divulgadas ou acessadas por indivíduos não autorizados, podem causar sérios danos à empresa ou violar regulamentações legais. Podem ser protegidas, por exemplo, por criptografia ou senhas de acesso.
2. Informação Restrita: Informações estratégicas que devem estar disponíveis apenas para grupos restritos de colaboradores. Podem ser protegidas, por exemplo, restringindo o acesso a uma pasta ou diretório interno.
3. Informação Interna: Informações de uso interno da Checkmob, destinadas a funcionários e colaboradores autorizados para o desempenho de suas funções. Essas informações não devem ser divulgadas externamente sem autorização.
4. Informação Pública: Informações que podem ser divulgadas ao público em geral sem restrições. São dados que não necessitam de proteção sofisticada contra vazamentos, pois podem ser de conhecimento público.

# RESPONSABILIDADES

O Comitê de Segurança da Informação da CHECKMOB S/A é o órgão responsável por monitorar e orientar a implementação desta política.

Todos os funcionários, contratados e colaboradores da CHECKMOB S/A são responsáveis por entender e aplicar esta política em suas atividades diárias.

# **CLASSIFICAÇÃO** DA INFORMAÇÃO

Seguem abaixo exemplos de informações e suas possíveis classificações:

* 1. Informação Confidencial 🟥
* Dados financeiros e contábeis sensíveis
* Detalhes de pesquisa e desenvolvimento
* Informações pessoais de clientes (como números de CPF, RG, telefone)
* Estratégias de negócios e planos estratégicos
* Senhas e chaves de acesso críticas
* Políticas indicadas como confidencial
  1. Informação Restrita 🟧
* Políticas internas da empresa.
* Planos estratégicos de médio prazo.
* Detalhes de projetos em andamento.
* Lista de funcionários e salários.
* Informações de contato de fornecedores e parceiros comerciais.
  1. Informação Interna 🟨
* Anúncios internos e comunicações da empresa.
* Programas de treinamento internos.
* Informações sobre eventos corporativos internos.
* Documentação de processos e procedimentos internos.
  1. Informação Pública 🟩
* Comunicados dos produtos oferecidos pela Checkmob.
* Relatórios financeiros públicos.
* Informações disponíveis no site da empresa.
* Informações que não são sensíveis ou estratégicas e estão disponíveis ao público em geral.

# **GERENCIAMENTO DE INFORMAÇÕES**

* 1. **Informações Confidenciais** devem ser:
* Acesso altamente restrito: Apenas pessoas autorizadas e com uma necessidade específica de conhecimento devem ter acesso a informações confidenciais.
* Monitoradas regularmente: Registrar e monitorar atividades relacionadas a informações confidenciais para detectar possíveis ameaças ou acessos não autorizados.
* Compartilhadas com cautela: Compartilhar informações confidenciais somente com partes autorizadas por meio de canais seguros.
  1. **Informações Restritas** devem ser:
* Acesso limitado: Restringir o acesso a informações restritas a pessoas ou departamentos específicos dentro da organização.
* Comunicadas com cautela: Compartilhar informações restritas apenas com partes que têm uma necessidade de conhecimento específica.
* Monitoradas para conformidade: Monitorar o acesso e a distribuição de informações restritas para garantir conformidade com políticas internas.
  1. **Informações Internas** devem ser:
* Acesso limitado aos funcionários: Limitar o acesso a informações internas a funcionários da organização.
* Compartilhadas internamente: Facilitar o compartilhamento eficiente de informações internas entre os departamentos relevantes.
* Controladas e atualizadas: Manter controle de versões para garantir que as informações internas estejam atualizadas e refletindo com precisão os procedimentos e políticas vigentes.
* Comunicadas por meios internos: Utilizar canais internos, como e-mails corporativos, Slack e Discord , para comunicação eficaz de informações internas.
  1. **Informações Públicas** devem ser:
* Acessíveis ao público: Disponibilizar informações públicas para acesso geral.
* Compartilhadas proativamente: Divulgação de informações públicas por meio de sites, comunicados de marketing e outros canais de comunicação.
* Atualizadas regularmente: Manter informações públicas atualizadas e refletindo com precisão a posição e os fatos mais recentes da Checkmob.
* Compartilhadas de forma transparente: Divulgar informações públicas de maneira transparente, evitando ocultação desnecessária.

# TREINAMENTO E CONSCIENTIZAÇÃO

O Comitê de Segurança da Informação da CHECKMOB S/A deverá fornecer treinamento regular aos funcionários para garantir o entendimento e a aderência a esta política.

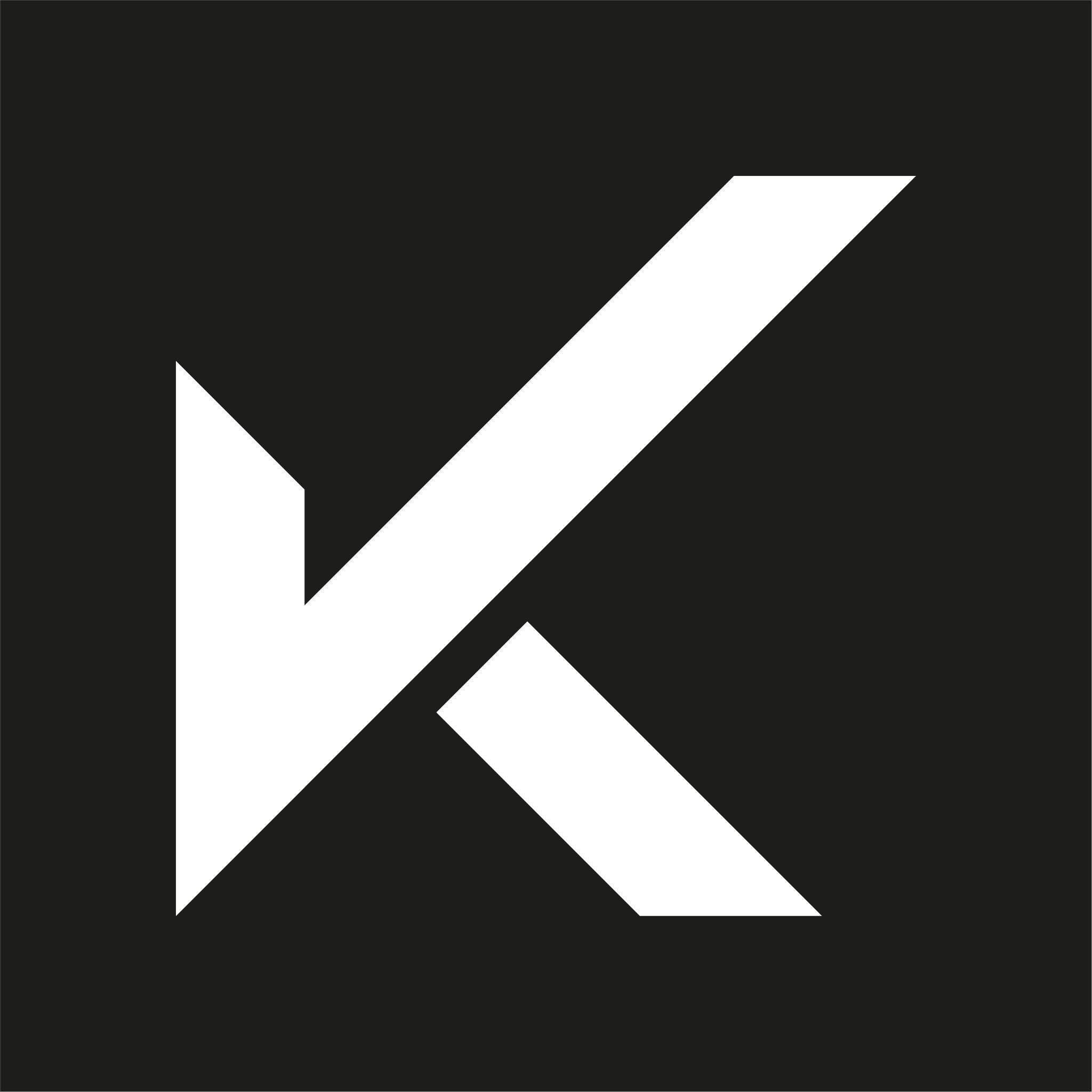
# MONITORAMENTO E CUMPRIMENTO

O Comitê de Segurança da Informação é o responsável por monitorar o cumprimento desta política e tomará medidas corretivas em caso de violações.

# DISPOSIÇÕES FINAIS

Esta política será gerida e atualizada bi-anualmente ou após mudanças significativas, atendendo às melhores práticas de SI de forma a garantir sua eficácia em caso de necessidade.

# ENGLISH VERSION OF THIS POLICY



INFORMATION CLASSIFICATION 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 from disclosure. If you are not authorized to receive it, please return this document to the aforementioned owner. Disclosure, distribution, reproduction or use of all or part of this document by any third party other than the person for whom it is intended, without Checkmob's prior written consent, is strictly prohibited.

SUMMARY

[**9. ENGLISH VERSION OF THIS POLICY 7**](#_fll15dlb1ukv)

[**10. OBJECTIVES 10**](#_ife03a3b99ly)

[**11. DEFINITIONS 10**](#_b8qt1sdrmd73)

[**12. RESPONSIBILITIES 10**](#_ea0jravyfxxl)

[**13. INFORMATION CLASSIFICATION 10**](#_sp7ml859u3j8)

[**14. INFORMATION MANAGEMENT 11**](#_ipdykczg8f91)

[**15. TRAINING AND AWARENESS 12**](#_5hwsgcbpepd2)

[**16. MONITORING AND COMPLIANCE 12**](#_ajikiywb1199)

[**17. FINAL PROVISIONS 12**](#_h70vmcouo476)

VERSION HISTORY

| DATE | VERSION | AUTHOR | DESCRIPTION |
| --- | --- | --- | --- |
| 18/01/2024 | 1.0 | Felipe Antunes | Creation of the document |
| 05/08/2024 | 1.1 | Information Security  and Compliance Committee | Formatting and inclusion of English translation. |

# OBJECTIVES

The Information Classification Policy of Checkmob aims to adequately protect and manage all information belonging to the company, ensuring the confidentiality, integrity, and availability of data. This policy establishes guidelines for classifying information into four levels: Confidential, Restricted, Internal, and Public.

# DEFINITIONS

1. Confidential Information: Highly sensitive information that, if disclosed or accessed by unauthorized individuals, can cause serious harm to the company or violate legal regulations. It can be protected, for example, by encryption or access passwords.
2. Restricted Information: Strategic information that should only be available to restricted groups of employees. It can be protected, for example, by restricting access to a specific folder or internal directory.
3. Internal Information: Information intended for internal use by Checkmob, meant for authorized employees and collaborators to perform their duties. This information should not be disclosed externally without authorization.
4. Public Information: Information that can be shared with the general public without restrictions. These are data that do not require sophisticated protection against leaks, as they can be public knowledge.

# RESPONSIBILITIES

The Information Security Committee of CHECKMOB S/A is responsible for monitoring and guiding the implementation of this policy.

All employees, contractors, and collaborators of CHECKMOB S/A are responsible for understanding and applying this policy in their daily activities.

# INFORMATION CLASSIFICATION

Below are examples of information and their possible classifications:

* 1. Confidential Information 🟥
* Sensitive financial and accounting data
* Research and development details
* Personal information of clients (such as CPF numbers, RG, phone numbers)
* Business strategies and strategic plans
* Critical passwords and access keys
* Policies marked as confidential
  1. Restricted Information 🟧
* Internal company policies
* Medium-term strategic plans
* Details of ongoing projects
* Employee list and salaries
* Contact information for suppliers and business partners
  1. Internal Information 🟨
* Internal announcements and company communications
* Internal training programs
* Information about internal corporate events
* Documentation of internal processes and procedures
  1. Public Information 🟩
* Announcements of products offered by Checkmob
* Public financial reports
* Information available on the company's website
* Information that is not sensitive or strategic and is available to the general public

# INFORMATION MANAGEMENT

* 1. **Confidential Information** should be:
* Highly restricted access: Only authorized individuals with a specific need to know should have access to confidential information.
* Regularly monitored: Record and monitor activities related to confidential information to detect potential threats or unauthorized access.
* Shared cautiously: Share confidential information only with authorized parties through secure channels.
  1. **Restricted Information** should be:
* Limited access: Restrict access to restricted information to specific individuals or departments within the organization.
* Communicated cautiously: Share restricted information only with parties who have a specific need to know.
* Monitored for compliance: Monitor the access and distribution of restricted information to ensure compliance with internal policies.
  1. **Internal Information** should be:
* Limited to employees: Limit access to internal information to employees of the organization.
* Shared internally: Facilitate efficient sharing of internal information among relevant departments.
* Controlled and updated: Maintain version control to ensure internal information is up-to-date and accurately reflects current procedures and policies.
* Communicated through internal means: Use internal channels, such as corporate emails, Slack, and Discord, for effective communication of internal information.
  1. **Public information** should be:
* Accessible to the public: Make public information available for general access.
* Proactively shared: Disseminate public information through websites, marketing communications, and other channels.
* Regularly updated: Keep public information updated and accurately reflecting the latest position and facts about Checkmob.
* Shared transparently: Disclose public information transparently, avoiding unnecessary concealment.

# TRAINING AND AWARENESS

The Information Security Committee of CHECKMOB S/A shall provide regular training to employees to ensure understanding and adherence to this policy.

# MONITORING AND COMPLIANCE

The Information Security Committee is responsible for monitoring compliance with this policy and will take corrective action in case of violations.

# FINAL PROVISIONS

This policy will be managed and updated bi-annually or after significant changes, adhering to best practices in Information Security to ensure its effectiveness when necessary.