Information Security Policy

G ERP · Grubtech · Version 1.0 · Effective from November 10, 2026

> **Company:** RAPHAEL DE ARAUJO SILVA (trade name GRUBTECH), CNPJ 30.444.499/0001-97
> R. Costa Barros, 698, Conj 3, Vila Alpina, São Paulo/SP, Brazil, CEP 03210-000
> **Security and privacy contact:** privacidade@grubtech.com.br

1. Purpose and scope

This policy sets the rules Grubtech follows to protect the confidentiality, integrity, and availability of G ERP, its servers, its databases, and the data it processes for customers, including personal data received from marketplaces. It applies to the company owner, to anyone who works for Grubtech, and to every system, workstation, and account used to build or operate G ERP.

2. Roles and responsibilities

Role	Responsibilities
Information Security Officer and Data Protection Officer: Raphael de Araujo Silva, owner	Approves and reviews this policy, grants and removes access, applies the controls below, handles incidents under the Incident Response Policy, and is the contact for customers, partners, and authorities.
Anyone working for Grubtech	Follows this policy, protects credentials, and reports any suspected incident immediately to privacidade@grubtech.com.br.
Customers	Manage their own G ERP users and permissions, as data controllers.

3. Data classification

Class	Examples	Handling
Confidential	Personal data of customers' clients and marketplace buyers (name, CPF/CNPJ, address, phone, e-mail), passwords, authorization tokens, API keys and secrets, digital certificates	Encrypted in transit and at rest; access only by the people and processes that need it; never sent by chat or e-mail in plain text.
Internal	Customers' business data (products, stock, orders, invoices, finance), logs	Kept in the customer's own database; access limited by permissions.
Public	Website, product presentation, published policies	No restriction.

4. Access control (least privilege)

- In G ERP each user has a personal login and receives only the tools needed for their work, at "no access", "view only", or "full access" level. Only the customer's administrator grants permissions.
- Access to production servers, databases, and cloud console is restricted to the company owner.
- Access is removed as soon as it is no longer needed.

- Marketplace data is used only to fulfill the seller's orders and is never shared beyond what the order and the invoice require.

5. Authentication and passwords

- User passwords are stored only as hashes; logins are blocked after repeated failed attempts, and idle sessions expire.
- Multi-factor authentication is required on the cloud provider and company e-mail accounts.
- Workstations sign in with Windows Hello (face recognition or PIN) and lock after inactivity.

6. Encryption

- All traffic uses HTTPS/TLS.
- Data at rest is encrypted by the cloud provider's disk encryption.
- Marketplace authorization tokens and other secrets are stored encrypted in the database.

7. Network security

- G ERP runs on Google Cloud. Only HTTPS is exposed to the internet, through an nginx reverse proxy.
- The application servers and the PostgreSQL database are not reachable from the internet; cloud firewall rules restrict inbound traffic.
- Each customer has its own isolated database.

8. Workstation security baseline

- Company workstations run a supported operating system with automatic updates and Microsoft Defender Antivirus with real-time protection.
- Screen lock after inactivity, sign-in required, and no shared accounts.
- Confidential data is not stored on workstations beyond what the work requires.

9. Vulnerability and change management

- Security updates for the server operating system are applied regularly.
- The application runtime (.NET) and libraries are kept up to date with each release.
- Changes are tested before release, and vulnerabilities found are fixed with priority according to their risk.

10. Logging and monitoring

- The system records who accessed it and when, and who made each change.
- Server and application logs, and blocked login attempts, are reviewed.

11. Backup and data retention

- Customer databases are backed up regularly so they can be restored after a failure or incident.
- When a contract ends, the customer can export their data; their database and backups are then deleted within 90 days. Marketplace authorization tokens are deleted as soon as the account is disconnected.

12. Suppliers

Suppliers that process data for G ERP (cloud hosting and the electronic invoice service) are chosen for their security practices, and receive only the data needed for their service.

13. Incidents

Security incidents are handled under the Grubtech Incident Response Policy, which defines roles, the reporting channel, the response steps, and notification of customers, marketplace partners, and authorities.

14. Review

This policy is reviewed at least once a year, and whenever the system, the infrastructure, or the law changes significantly.

Approved by: Raphael de Araujo Silva, owner and Information Security Officer · São Paulo, November 10, 2026

Política de Segurança da Informação

G ERP · Grubtech · Versão 1.0 · Em vigor a partir de 10 de novembro de 2026

> **Empresa:** RAPHAEL DE ARAUJO SILVA (nome fantasia GRUBTECH), CNPJ 30.444.499/0001-97
> R. Costa Barros, 698, Conj 3, Vila Alpina, São Paulo/SP, CEP 03210-000
> **Contato de segurança e privacidade:** privacidade@grubtech.com.br

1. Objetivo e abrangência

Esta política define as regras que a Grubtech segue para proteger a confidencialidade, a integridade e a disponibilidade do G ERP, de seus servidores, de seus bancos de dados e dos dados que trata para os clientes, inclusive os dados pessoais recebidos dos marketplaces. Vale para o titular da empresa, para quem trabalhar para a Grubtech e para todo sistema, computador e conta usados para desenvolver ou operar o G ERP.

2. Funções e responsabilidades

Função	Responsabilidades
Responsável pela segurança da informação e Encarregado de dados: Raphael de Araujo Silva, titular	Aprova e revisa esta política, concede e retira acessos, aplica os controles abaixo, trata incidentes pela Política de Resposta a Incidentes e é o contato de clientes, parceiros e autoridades.
Quem trabalhar para a Grubtech	Segue esta política, protege as próprias credenciais e avisa na hora qualquer suspeita de incidente em privacidade@grubtech.com.br.
Clientes	Administram os próprios usuários e permissões no G ERP, como controladores dos dados.

3. Classificação dos dados

Classe	Exemplos	Tratamento
Confidencial	Dados pessoais dos clientes dos clientes e dos compradores dos marketplaces (nome, CPF/CNPJ, endereço, telefone, e-mail), senhas, autorizações, chaves e segredos de APIs, certificados digitais	Criptografados em trânsito e em repouso; acesso só por quem e pelo que precisa; nunca enviados por chat ou e-mail em texto aberto.
Interno	Dados de negócio dos clientes (produtos, estoque, pedidos, notas, financeiro), registros (logs)	Ficam no banco de dados do próprio cliente; acesso limitado pelas permissões.
Público	Site, apresentação do produto, políticas publicadas	Sem restrição.

4. Controle de acesso (privilégio mínimo)

- No G ERP cada usuário tem login próprio e recebe só as ferramentas de que precisa, em nível "sem acesso", "só consulta" ou "acesso total". Só o administrador do cliente concede permissões.
- O acesso aos servidores, aos bancos de dados e ao console da nuvem é restrito ao titular da empresa.
- O acesso é retirado assim que deixa de ser necessário.
- Os dados dos marketplaces são usados só para atender os pedidos do vendedor e não vão além do que o pedido e a nota fiscal exigem.

5. Autenticação e senhas

- As senhas dos usuários são guardadas só como hash; o login é bloqueado depois de tentativas erradas, e a sessão sem uso expira.
- Autenticação em dois fatores é obrigatória nas contas do provedor de nuvem e do e-mail da empresa.
- Os computadores entram com Windows Hello (rosto ou PIN) e bloqueiam a tela sem uso.

6. Criptografia

- Todo o tráfego usa HTTPS/TLS.
- Os dados em repouso são criptografados pela criptografia de disco do provedor de nuvem.
- As autorizações dos marketplaces e outros segredos são guardados criptografados no banco.

7. Segurança da rede

- O G ERP roda no Google Cloud. Só o HTTPS fica exposto à internet, por um proxy reverso nginx.
- Os servidores da aplicação e o banco PostgreSQL não são acessíveis pela internet; regras de firewall da nuvem restringem a entrada.
- Cada cliente tem o próprio banco de dados, separado dos outros.

8. Segurança dos computadores

- Os computadores da empresa usam sistema operacional com suporte e atualização automática, e o Microsoft Defender Antivírus com proteção em tempo real.
- Bloqueio de tela sem uso, entrada obrigatória e nenhuma conta compartilhada.
- Dados confidenciais não ficam nos computadores além do que o trabalho exige.

9. Gestão de vulnerabilidades e mudanças

- As atualizações de segurança do sistema operacional dos servidores são aplicadas regularmente.
- O ambiente da aplicação (.NET) e as bibliotecas são mantidos atualizados a cada versão.
- As mudanças são testadas antes de ir para o ar, e as vulnerabilidades encontradas são corrigidas com prioridade conforme o risco.

10. Registros e monitoramento

- O sistema registra quem acessou e quando, e quem fez cada alteração.
- Os registros dos servidores e do sistema, e as tentativas de login bloqueadas, são revisados.

11. Cópias de segurança e guarda dos dados

- Os bancos de dados dos clientes têm cópias de segurança regulares, para serem restaurados depois de uma falha ou incidente.
- No fim do contrato, o cliente pode exportar os dados; depois, o banco dele e as cópias são excluídos em até 90 dias. As autorizações dos marketplaces são apagadas assim que a conta é desconectada.

12. Fornecedores

Os fornecedores que tratam dados para o G ERP (hospedagem em nuvem e o serviço de emissão de notas fiscais) são escolhidos pelas práticas de segurança e recebem só os dados necessários ao serviço.

13. Incidentes

Os incidentes de segurança são tratados pela Política de Resposta a Incidentes da Grubtech, que define funções, canal de comunicação, passos de tratamento e a comunicação a clientes, marketplaces e autoridades.

14. Revisão

Esta política é revista pelo menos uma vez por ano e sempre que o sistema, a infraestrutura ou a lei mudarem de forma relevante.

Aprovada por: Raphael de Araujo Silva, titular e responsável pela segurança da informação · São Paulo, 10 de novembro de 2026