RGIS®

RGIS 2026

CODE OF BUSINESS CONDUCT AND ETHICS

RGIS®

CONTENTS

DEAR COLLEAGUES

As the global leader of inventory services, RGIS is most successful when everyone works honestly, professionally, and together as a team. We want to take this opportunity to remind everyone of our company's core values.

These core values serve as the cornerstone of the RGIS Code of Business Conduct and Ethics. In today's global marketplace, it is more important than ever that we reflect and live these values in all of our business dealings, every day. By following this Code, we will continue to excel, provide outstanding service to our customers, and meet the high ethical standards we have set for ourselves.

Please contact the Office of Legal Department (generalcounsel@rgis.com) with any questions about this Code, or if you suspect any violations. Thank you for your commitment to our company and its values.

Sincerely,

ASAF COHEN
Chief Executive Officer

RESPECT EXCELLENCE INTEGRITY TEAMWORK INNOVATION

RGIS®

SECTION 1

INTEGRITY

WHY THIS CODE?

RGIS built its legacy on honesty and integrity. These values are the foundation for our future success as the global leader in inventory service, data collection, insight, merchandising and optimisation solutions. This Code of Business Conduct and Ethics (the "Code") aims to inspire and guide us by reinforcing our core values and establishing clear standards for ethical behaviour. The Code applies to RGIS, its subsidiaries, and all of its officers, directors, and employees around the world.

Everyone is responsible for reading, understanding and following this Code, RGIS company policies, and all applicable laws and regulations.

ASK QUESTIONS AND USE COMMON SENSE

This Code cannot cover every situation that you or your colleagues may face. For this reason, every member of the RGIS team is expected to use common sense, especially if an action seems unusual or unethical. When in doubt, always ask yourself the following questions:

- Is the action legal?
- Is the action consistent with RGIS's core values?
- Is the action consistent with RGIS's policies and procedures?

If the answer to any of these questions is "no," then you have a responsibility to report your concerns. Your supervisor, the Human Resources Department, and the Office of General Counsel can all help you with questions regarding this Code and other RGIS policies.

CONFLICTS OF INTEREST

RGIS expects employees to work solely for the company's benefit without any conflicts of interest. This can occur whenever your personal, family, or business interests conflict with the company's interests. Employing a family member as a contractor or supplier is one example of a possible conflict. You are expected to avoid conflicts of interest whenever possible. If a conflict cannot be avoided, then you must disclose it promptly to management. The RGIS Board of Directors must approve any conflicts of interest (or potential conflicts of interest) involving one of the company's officers or directors. Other specific requirements include:

- **Business Opportunities:** All RGIS employees have a duty to promote the company's legitimate business interests whenever possible. You must not promote your own personal or family business opportunities at the company's expense. RGIS is also the sole owner of all intellectual property, trademarks, logos, product designs, and domain names that it uses in its business. All employees agree to assign to RGIS all rights in any intellectual property created as a part of his or her work.
- **Competition:** Employees cannot compete with RGIS. You are prohibited from being employed by, performing services for, or receiving any compensation from, any RGIS competitor. With limited exceptions, employees may not own any financial interest in any business that does business with, seeks to do business with, or is in competition with, RGIS.
- **Outside Employment:** Your primary employment obligation is to RGIS. Any outside activity, including a second job, family business, self-employment, or volunteer activity, must be kept completely separate. You may not use RGIS's customers, suppliers, time, name, influence, assets, facilities, materials, or other resources for any outside activities unless RGIS specifically authorises you to do so.

SECTION 1

INTEGRITY

CONFLICTS OF INTEREST (CONTINUED)

- **Family Members:** You must never use your position to secure RGIS business for family members or any organisation associated with your family members, unless your department head and the Office of General Counsel both authorise the activity. For the purposes of this Code, the term “family members” includes spouses, domestic partners, children (including adopted children, stepchildren, and wards), grandchildren, parents, grandparents, siblings, in-laws, uncles, aunts, nieces, nephews, and cousins.
- **Personal Relationships:** Personal relationships between RGIS employees can create conflicting loyalties and conflicts of interests that harm RGIS. You must never use your position at RGIS to approve payments, compensation, or any favoured treatment for family members or any other person with whom you have a personal relationship. You must also disclose the existence of any romantic relationship with a co-worker to your immediate supervisor or to the Human Resources Department. This will help RGIS to determine whether any conflict of interest exists. The company will attempt to resolve any conflicts or risks it identifies. In some cases, it may be necessary to transfer you to another position or department. Refusing a transfer to a reasonable alternative position will be treated as a voluntary resignation. If no alternatives are available, then one or both employees may be terminated.

Reporting at:

- apacethics@rgis.com

Human Resources:

- Generalcounsel@rgis.com

Legal:

- Generalcounsel@rgis.com
- ecordier@rgis.com

RGIS®

SECTION 2

OUR LEGAL DUTIES

FAIR COMPETITION AND ANTITRUST

RGIS is committed to the principles of free and competitive enterprise. Accordingly, it is RGIS policy to follow the antitrust laws wherever we do business. These laws are based on the idea of open competition, and that businesses should not threaten that idea through unlawful and unfair behaviour.

Discussion of any of the following topics with competitors, whether relating to either RGIS services or those of the competitor, are prohibited: past, present or future prices, pricing policies, lease rates, bids, discounts, promotions, profits, costs, margins, new products or processes not previously disclosed, terms of service, warranties, customers or territorial markets.

At RGIS, those involved in pricing decisions, or who engage in direct contact with competitors, are especially at risk for potential antitrust concerns, and should become thoroughly familiar with the RGIS Antitrust Policy. Trade associations must not be used for contacts and communications with competitors that are prohibited by RGIS, such as discussing prices.

For additional information, please see the **RGIS Antitrust Policy**.

You must NOT offer, make or receive payments, or anything of value, to:

- Influence a desired action;
- Encourage a violation of the law;
- Obtain an improper advantage;
- Influence the decision of a government or an official; or
- Improperly gain business.

ANTI-CORRUPTION AND ANTI-BRIBERY

RGIS conducts its worldwide operations ethically and in compliance with U.S. and applicable foreign laws, including all anti-bribery and anti-corruption laws. RGIS has zero tolerance for bribery and corruption.

The U.S. Foreign Corrupt Practices Act, and the U.K. Bribery Act, as well as similar laws in other countries, prohibit RGIS, its employees and representatives from offering or receiving a bribe, a kickback, or any other improper payment to obtain or retain business or influence a business decision.

These laws apply to RGIS all over the globe, and the penalties for violations can be severe to RGIS and to you personally, including fines, and even imprisonment.

A bribe can take many forms, including a payment, a gift, a favour, a kickback, an offer of entertainment or travel, or anything of value. Even a charitable or political contribution, if meant to influence a business decision, can be considered a bribe.

Regardless of local practice or the practice of other companies, avoid even the appearance of inappropriate behaviour.

Accordingly, you may neither give nor accept, directly or indirectly, gifts, gratuity, or entertainment that are greater than nominal ($50) in value or that could otherwise be viewed as influencing business decisions. You should never solicit a gift or favour from anybody with whom RGIS does business. For entertainment, there must be a clear purpose for the event.

Be aware that RGIS can be held responsible for bribes made on our behalf by third parties, including by our partners, customers, suppliers, and vendors. Exercise due diligence in the selection of business partners, and avoid relationships with parties that have a history of corrupt practices.

SECTION 2

OUR LEGAL DUTIES

ANTI-CORRUPTION AND ANTI-BRIBERY (CONTINUED)

It is expected that you:

- Ensure all team members you supervise understand the Anti-Corruption and Anti-Bribery portion of this Code;
- Create an environment to encourage team members to speak up;
- Never ask team members to achieve business results "at all costs", especially at the expense of ethical behaviour;
- Review any situation that shows a potential anti-corruption concern, and report suspected violations to the Office of General Counsel; and
- Respond, as appropriate, to questions and concerns related to this Code, including contacting the Office of General Counsel if necessary.

EXPORT CONTROLS AND ECONOMIC SANCTIONS

The U.S. Government and foreign governments impose economic sanctions, export controls, and other restrictive trade measures to promote various foreign policy and national security objectives. Examples include the International Traffic in Arms Regulations ("ITAR"), the Export Administration Regulations ("EAR") and the economic sanctions programs implemented by the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC"). These laws impose different prohibitions on different countries and entities, and change rapidly in response to world events. RGIS is prohibited from engaging with any countries and territories subject to OFAC sanctions in any business transactions or dealings with (i) any government, department, agency, instrumentality or subdivision of these countries, (ii) any entity controlled by these countries, (iii) any individual or entity based in or subject to the jurisdiction of these countries, or (iv) an entity considered a supporter of terrorism or proliferator of weapons of mass destruction (as listed on the U.S. Office of Foreign Asset Control "Blocked Persons and Specifically Designated Nationals List").

The United States, United Nations, and European Union ("EU") may impose additional sanctions and export controls on other countries or entities at any time.

All RGIS employees must comply with U.S. economic sanctions and export controls regardless of their nationality or location. This is true even if local laws are less restrictive in the countries where they live and work. Additionally, RGIS employees may never facilitate any third-party business that might violate these laws, even if the business occurs outside the United States. If you suspect that RGIS is engaging in prohibited activities, please notify the Office of General Counsel immediately.

MANAGING THIRD PARTY RISKS

Although RGIS encourages good relations with our suppliers and other business partners, you may not benefit personally from the purchase of any goods or services for RGIS. Employees whose responsibilities include purchasing (including merchandise, fixtures, services, real estate, etc.), or who have contact with suppliers or service providers, must not exploit their position for personal gain.

Similar conflict of interest and anti-bribery requirements apply whenever RGIS engages a professional consultant. You may never receive cash or cash equivalents from any supplier, consultant, agent or other service provider, whether directly or indirectly. When in doubt, RGIS employees should exercise diligence when selecting business partners, and avoid working with those that have a history of bribery or other corrupt practices.

Finally, RGIS requires its suppliers to respect human rights, and prohibits all forms of slavery in its global supply chain. All employees must report any supplier known to use child labour, forced labour, human trafficking and other forms of slavery to the Office of General Counsel. Please see the **RGIS UK Modern Slavery Act Statement** for more information.

RGIS®

SECTION 2

OUR LEGAL DUTIES

DIVERSITY AND INCLUSION/HARASSMENT AND DISCRIMINATION

RGIS's employees are our greatest asset, and we value diversity in our workforce. By blending our unique experiences, perspectives and talents together, we create an environment that encourages innovation and contribution. To these ends, no applicant or employee should be subjected to unlawful discrimination or harassment because of their race, colour, religious creed, gender, gender identity or sexual orientation, disability, age, national origin, ancestry, genetic information, military status, or any other characteristic protected by applicable law. Hiring, promotion, raises, discipline, or termination decisions should only be based on job performance and valid business reasons.

RGIS is also committed to maintaining a respectful work environment free from harassment and discrimination. We prohibit all conduct – whether intentional or unintentional – that results in unlawful harassment, abuse, or intimidation based on any characteristic protected by applicable law. Harassment and discrimination are prohibited whether they occur in the workplace, at customer or vendor sites, or at other employment-related events or activities.

RGIS will investigate all good faith harassment and discrimination complaints promptly and thoroughly. In this instance, the term "good faith" does not mean that the report or concern raised must be correct, but it does require that the person making the report, or raising the concern, believes that he or she is providing truthful information. It is unlawful to retaliate against, or punish, any employee who files a good faith complaint of discrimination or harassment, or who cooperates in any investigation of a complaint.

WORKPLACE SAFETY

RGIS is committed to providing its team members with a safe and healthy workplace. All team members have the right to a hazard-free environment. As part of this commitment, each team member has a personal responsibility for working safely, and for helping others to remain safe.

RGIS is committed to:

- Complying with all applicable safety regulations and codes, as well as its own operating standards and procedures.
- Continuously developing, communicating, and promoting safety programs based on injury prevention.
- Providing safety orientation, procedures, training, and necessary personal protective equipment (PPE) as needed.
- Escalating, communicating, and partnering to resolve safety issues.
- Investigating and making recommendations to prevent injuries.
- Never retaliating against an employee for reporting an incident, or voicing a safety concern.
- Promoting continuous improvement of our safety management system, procedures, and results.

Employees are responsible for:

- Immediately reporting incidents and unsafe conditions to their supervisor or other designated persons.
- Learning and complying with all RGIS safety rules.
- Evaluating risks and hazards in their work area at all times.
- Only performing work that they are trained to perform.
- Observing safe driving practices, as outlined in the RGIS Vehicle Use and Safety manual and local laws.
- Acting immediately if they see a co-worker putting themselves or another person at risk.
- Understanding that unsafe acts will be handled in the same way as performance issues.

RGIS®

SECTION 3

AI POLICY

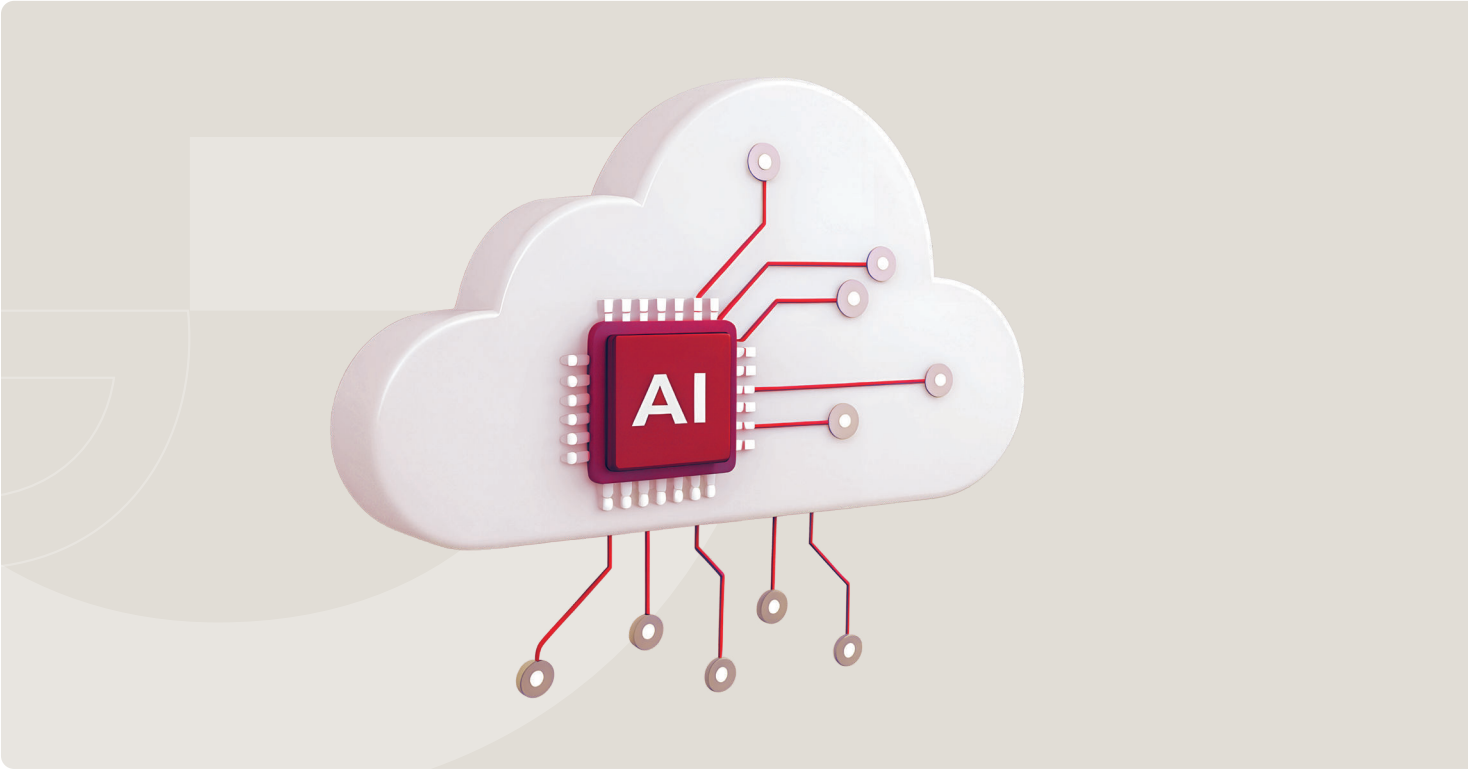
AI IN OUR WORKPLACE: WHY AN AI POLICY?

As AI continues to evolve, its potential to enhance productivity, streamline operations, and drive innovation is undeniable. However, with great potential comes inherent risks – ranging from data security and compliance concerns to ethical considerations and accuracy challenges. Our AI Policy is designed to strike the right balance between opportunity and risk, ensuring that AI is integrated securely, strategically, and in alignment with our business objectives.

Under the AI Director's leadership, AI integrations within our processes will be carefully assessed and implemented where they provide the greatest value, ensuring that AI supports – not replaces – human expertise. This policy serves as a framework to guide responsible AI use, ensuring clarity, security, and compliance across all departments.

Recent assessments highlight varying levels of AI adoption across our organisation. While some teams have embraced AI for automation, analysis, and content generation, others remain hesitant due to concerns over security, compliance, and accuracy. Our approach acknowledges these concerns, prioritising education, governance, and secure implementation to build confidence in AI's role within our business.

Through this policy, we emphasise that AI is not just a tool—it is a responsibility. Employees must use AI ethically, avoiding the sharing of confidential data, ensuring accuracy in outputs, and maintaining human oversight in decision-making. By following these guidelines, we can harness AI's full potential while safeguarding our operations, our people, and our future.



RGIS®

SECTION 3

AI POLICY

1. INTRODUCTION

This policy establishes the guidelines and standards for the responsible use of Artificial Intelligence (AI) technologies, including Generative Artificial Intelligence (GenAI), within RGIS. AI tools are technologies designed to perform tasks that typically require human intelligence, while GenAI tools specifically generate new, previously undefined content based on user inputs or prompts. Examples of GenAI tools include ChatGPT, Gemini, Microsoft Co-Pilot, and other similar platforms. AI and GenAI technologies offer transformative potential across RGIS, enabling us to streamline operations, enhance productivity, and drive creativity in areas such as data analysis, content creation, and process automation.

2. PURPOSE

Whilst offering incredible potential, AI also introduces significant risks, including those related to data security, confidentiality, accuracy, intellectual property compliance, and ethical use. Finding the right balance between leveraging AI's transformative potential and mitigating its inherent risks is essential to ensuring responsible and effective implementation.

It requires a proactive approach, where innovation is encouraged while maintaining rigorous safeguards to protect data, ensure compliance, and uphold ethical standards. This policy outlines guidelines for the internal use, development, and deployment of Artificial Intelligence (AI) systems within RGIS.

The goal is to ensure that our AI use:

- Aligns with ethical standards;
- Respects data privacy in safeguarding RGIS's sensitive and confidential information,
- Customer data,
- Adheres to regulatory frameworks AI introduces significant risks, including those related to data security, confidentiality, accuracy, intellectual property compliance, and ethical use.

The goal is to ensure that our AI use aligns with ethical standards, respects data privacy in safeguarding RGIS's sensitive and confidential information, and adheres to regulatory frameworks, including the EU AI Act.

3. SCOPE

This policy applies to all employees, including temporary staff and interns, contractors, affiliates, and third parties who work with or interact with AI tools and systems provided or approved by RGIS and accessing RGIS data. It covers AI applications, data handling, and compliance requirements associated with AI systems used within the organisation.

4. DEFINITIONS

- **AI Tools:** Any software, application, or hardware that utilises artificial intelligence techniques (including machine learning, natural language processing, image recognition, and generative capabilities).
- **AI Governance Team:** A group within an organisation responsible for overseeing and managing the development, deployment, and ethical use of artificial intelligence (AI) technologies.
- **Confidential Information:** Confidential Information refers to data that is proprietary or private to RGIS, including trade secrets, business strategies, financial information, and any other information that is not publicly available. All sensitive or non-public information, including but not limited to RGIS's proprietary RM technology, inventory management systems, RFID solutions, wireless technology implementations, client inventory data (including healthcare facility audit data), internal communications, and operational strategies.

SECTION 3

AI POLICY

4. DEFINITIONS (CONTINUED)

- **Data:** refers to any information collected, processed, or stored by AI systems, including user inputs, system outputs, metadata, and any structured or unstructured information used for training, inference, or decision-making.
- **Ethical Standards:** Principles that guide the responsible use of AI, ensuring fairness, transparency, and respect for individual rights.
- **Generative AI:** A category of artificial intelligence systems that are designed to generate new, previously undefined content based on user inputs or prompts. This content can include text, images, audio, video, or other forms of media.
- **Proprietary Systems:** RGIS's RM technology, inventory management systems, RFID and wireless technology implementations, and associated digital infrastructure.
- **Sensitive Information:** Sensitive Information encompasses data that requires protection due to its nature, including personal data, health records, and any information that could lead to identity theft or privacy breaches.
- **Unauthorised AI Systems:** AI tools or platforms not explicitly reviewed and approved by the AI Governance Team.

5. ETHICS OF ARTIFICIAL INTELLIGENCE

5.1. Non-discrimination

We are committed to developing and using artificial intelligence algorithms fairly. We apply controls to detect and minimise bias in training data and AI models, ensuring no discrimination in terms of age, gender, ethnicity, creed, etc.

5.2. Transparency

Decisions automated by our algorithms are explained in an accessible way to the relevant users, to ensure that they are understood. This allows users to better understand the logic behind automated decisions, especially when results influence professional or personal aspects.

5.3. Human Control

People remain at the heart of decision-making processes in operations that incorporate AI technologies. Human recourse is always possible for any important decision involving AI, allowing users or employees to question and clarify the results produced by AI.

6. APPROVED AI TOOLS AND USAGE

Employees may use AI tools that meet one of the following criteria:

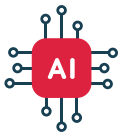
- **Recognised Providers:** Tools originating from well-known, reputable vendors – primarily from the United States – or those with a proven track record for compliance and security.
- **Internally Developed Tools:** AI applications developed and maintained by the RGIS IT team.

All other AI tools or applications must undergo a formal review process and receive explicit authorisation from the AI Governance Team prior to use.

RGIS®

SECTION 3

AI POLICY



7. PROHIBITED PHYSICAL AND SOFTWARE PRACTICES

Employees MUST NOT:

Install or Use Unauthorised AI Tools:

- Install, download, or operate any AI software or hardware on RGIS-owned devices, or on personal devices connected to RGIS networks, without prior review and explicit written approval from the AI Governance Team.
- Introduce AI tools that integrate or interface with any proprietary RGIS systems (including RM technology, inventory management systems, RFID solutions, wireless technology implementations, tablet applications, and dashboard systems) unless specifically authorised.

Circumvent Security or Approval Protocols:

- Modify, bypass, or disable any security measures or approval processes designed to control the integration or use of AI systems within RGIS.

Integrate AI Tools with Core Systems:

- Connect or integrate any AI tools with RGIS's proprietary systems – including RM technology, inventory management systems, RFID solutions, wireless technology platforms, tablet applications, and dashboards – without explicit authorisation from both the AI Governance Team and IT Security.

Misuse Customer Data:

- The use of unauthorised software, hardware, or external storage devices to collect, process, or store customer data is strictly prohibited. All AI systems must adhere to company-approved security protocols to prevent data breaches and unauthorised access.

8. CROSS-BORDER DATA TRANSFERS AND REGIONAL COMPLIANCE

Given RGIS's global presence, employees must:

- Ensure that any AI tool handling data complies with the data protection laws and regulations of the relevant jurisdictions (e.g., GDPR in the EU, CCPA in California, HIPAA for healthcare data, and other national standards).
- Not transfer any confidential or sensitive data across national borders via AI systems unless such transfers have been specifically reviewed, documented, and approved by the AI Governance Team.

9. ENVIRONMENTAL AND RESPONSIBLE DIGITAL CONSEQUENCES

Reducing the digital footprint:

- RGIS incorporates responsible practices to reduce the environmental impact of its digital activities. This includes optimised server utilisation, proper equipment recycling, and energy-efficient technology choices.

Responsible digital awareness:

- We promote the responsible use of digital technologies and promote environmentally friendly behaviour among employees, such as limiting paper printing and optimising the use of IT resources.

SECTION 3

AI POLICY

10. LIABILITY, COMPLIANCE, AND MONITORING

Liability for AI-Generated Errors:

- RGIS shall not be held liable for AI-generated errors in inventory counts, audits, or operational reports if the AI tool was used without proper approval or outside the bounds of this Policy. Any such error will be subject to internal review, and disciplinary action may be taken against employees found in violation.

Monitoring and Auditing:

- RGIS reserves the right to monitor and audit the use of AI tools on all company-owned or RGIS-connected devices. Non-compliance with this Policy may result in disciplinary measures, up to and including termination of employment.

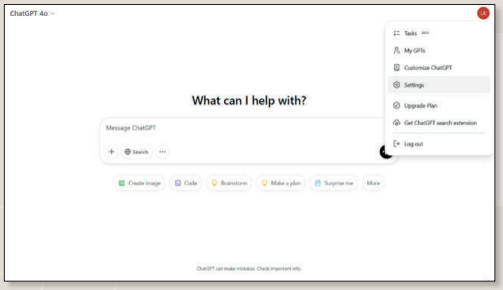
Reporting Violations:

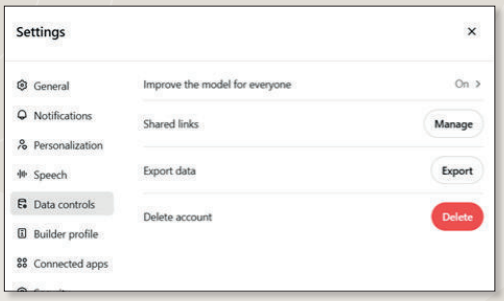
- Employees must immediately report any suspected violations of this Policy to their supervisor, IT Security, or the AI Governance Team.

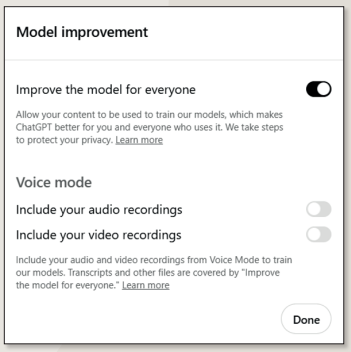
11. POLICY AMENDMENTS

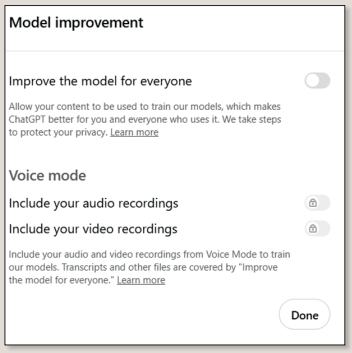
RGIS reserves the right to amend or update this Policy at any time. Any changes will be communicated through official channels and will take effect immediately upon release.

ChatGPT









RGIS®

SECTION 4

OUR COMPANY POLICIES

QUALITY AND ACCURACY

The success of RGIS depends on its ability to efficiently and accurately perform in a professional and courteous manner. Our customers expect, and should receive, an accurate count during inventory events. Inaccurate inventory results can impact our customers' bottom line, and the reputation of RGIS. Further, all inventory and merchandising work should be performed professionally and up to the customer's standards. RGIS must build and maintain strong working relationships by listening, and responding to, our customers.

BUSINESS RECORDS

RGIS employees must accurately and honestly document any information appearing in the company's business records. These books and records must accurately and fairly reflect, in reasonable detail, RGIS's assets, liabilities, revenues, and expenses. Falsifying records, or causing others to falsify records, is strictly prohibited. Making false or misleading statements to anyone, including internal or external auditors, RGIS's counsel, other RGIS employees, or regulators, can be a criminal act, and may result in severe penalties.

Our customers expect, and should receive, an accurate count.

Employees preparing financial statements must always do so in accordance with RGIS's internal control and disclosure policies, Generally Accepted Accounting Principles ("GAAP"), and any other applicable accounting standard. RGIS financial statements must materially, fairly and completely reflect our business transactions and financial condition.

Finally, you must never destroy, falsify, or modify any document that is subject to a legal hold issued by the Office of General Counsel, or may be relevant to an alleged violation of law, or sought as part of a government investigation. Doing so may lead to fines, penalties, or prosecution for obstruction of justice.

COMPANY PROPERTY

All employees must protect RGIS assets and ensure their efficient use. All RGIS assets, whether tangible or intangible, are to be used only by authorised employees or their designees, and only for legitimate RGIS business purposes. You are responsible for the proper use of company property, and must never loan, sell, take, or donate RGIS assets without appropriate authorisation. Misusing your time, including through the excessive use of RGIS computers and networks for personal activities, is also prohibited.

COMMUNICATIONS AND SOCIAL MEDIA

All media inquiries must be referred to the Chief Executive Officer ("CEO"). You are not allowed to speak to a member of the media unless authorised to do so by the CEO. You may also not post any materials on social media on behalf of RGIS without prior authorisation from the Human Resources Department.

If you are authorised to post to social media on behalf of RGIS, you may never use offensive, demeaning, discriminatory, or harassing language, or make threats of violence or similar inappropriate or unlawful conduct. All confidentiality policies included in this Code apply to your use of social media.

CONFIDENTIAL INFORMATION

RGIS confidential information is defined as all non-public information that might be of use to competitors, or harmful to the company or its customers, if shared, for example, inventory business service technology. You must protect all confidential information relating to RGIS. You should not disclose (even to family) or use any confidential information for any purpose unless the company authorises you to do so. This obligation lasts throughout your time with RGIS, and continues after you leave RGIS.

RGIS®

SECTION 4

OUR COMPANY POLICIES

CONFIDENTIAL INFORMATION (CONTINUED)

Further, RGIS protects individually identifiable employee information from inappropriate or unauthorised use or disclosure. You must protect all confidential information relating to your fellow team members. Do not disclose or use any confidential information for any purpose other than on a “need to know” basis within RGIS. This obligation of confidentiality lasts during the entire length of your time with RGIS, and also continues after you depart RGIS.

DATA AND PRIVACY PROTECTION

RGIS is committed to protecting confidential customer information in accordance with applicable law, even if the customer does not have a confidentiality agreement with us. RGIS must protect private customer data. You should not disclose private customer information (even to family) or use any customer confidential information for any purpose unless authorised by RGIS. This obligation of confidentiality lasts during the entire length of your time with RGIS, and also continues after you leave the company.

RGIS is committed to protecting the private information of our customers and employees, including their names, addresses, banking details, and other Personal Identifying Information (“PII”). Employees must not disclose PII outside the company unless it is authorised by the customer or employee, permitted by local law, or necessary to comply with a lawful government order (such as a subpoena or warrant).

Privacy laws vary widely. The EU Data Privacy Regulation, for example, sets much stricter privacy standards than U.S. laws. Strict laws may also exist in other countries where RGIS does business. For this reason, RGIS employees must always comply with the privacy laws that apply in the country where they are actually working, even if they usually live or work in another country. Employees should contact their managers or the Office of General Counsel (in Europe, contact Head of Legal Europe) with any questions regarding the EU Data Privacy Regulation or other privacy protection laws.

ENVIRONMENTAL RESPONSIBILITY

RGIS promotes socially and environmentally responsible business. Conducting business as a responsible member of society is a key part of our strategy for the future, and we remain committed to continuous improvement in all aspects of our performance. RGIS encourages environmental conservation by reducing the use of paper, recycling when possible, and minimising unnecessary waste.

SUBSTANCE ABUSE

Employees under the influence of illegal drugs, controlled substances, or alcohol at work are a risk to RGIS, themselves, and others. Unless prescribed, the possession, use, distribution, or sale of illegal drugs, controlled substances, and alcohol on RGIS premises, during company-sponsored travel or business, at RGIS- sponsored events, or at any place where RGIS work is conducted, is strictly prohibited. Violators are subject to disciplinary action up to and including termination.

RGIS has a duty to carry out its business activities in a socially responsible manner.

All employees are also required to follow all other RGIS policies relating to the off-duty use of illegal drugs and alcohol during company-sponsored travel. Off-the-job involvement with illegal drugs can have an impact on health and safety in the workplace.

RGIS®

SECTION 5

REPORTING SUSPECTED VIOLATIONS

PURPOSE

RGIS is committed to conducting business ethically, lawfully, and in line with this Code of Conduct. RGIS encourages employees and external stakeholders to speak up if they become aware of, or suspect, any violation of this Code, company policies, or applicable laws. This Whistleblower Procedure explains how concerns can be raised and how RGIS will respond.

WHO CAN REPORT?

This procedure is available to all stakeholders, including RGIS employees, temporary workers, contractors, agency workers, suppliers, business partners, consultants, customers, and other third parties who interact with RGIS.

WHAT SHOULD BE REPORTED?

You should report any concern or suspicion of misconduct, including (for example):

- Bribery, corruption, facilitation payments, kickbacks, or improper gifts and hospitality.
- Fraud, theft, false records, or improper accounting practices.
- Conflicts of interest or unethical business practices.
- Harassment, bullying, discrimination, or other inappropriate workplace conduct.
- Health and safety risks or unsafe working practices.
- Breaches of confidentiality, misuse of company property, or information security concerns.
- Violations of competition/anti-trust laws or other legal/regulatory requirements.
- Human rights concerns (including forced labour, child labour, or modern slavery risks), where applicable.
- Attempts to conceal misconduct, retaliate against a reporter, or interfere with an investigation.

If you are unsure whether something is a concern, raise it anyway.

CONFIDENTIALITY GUARANTEE

RGIS will handle reports confidentially to the extent possible and consistent with a fair and thorough review. Your identity (and the information you provide) will be shared only with those who need to know in order to assess the concern, investigate, take action, or meet legal requirements.

ANONYMOUS REPORTING

Reports may be made anonymously, where permitted by local law and the reporting channel used. RGIS will review anonymous reports in the same way as other reports, although RGIS may be limited in its ability to follow up or provide updates if no contact details are provided.

NON-RETALIATION GUARANTEE

RGIS prohibits retaliation. No one will be disciplined, demoted, terminated, harassed, or otherwise treated unfairly for raising a concern or participating in an investigation in good faith, even if the concern is not substantiated. Any retaliation (or attempted retaliation) is itself a serious violation and may result in disciplinary action, up to and including termination of employment or the ending of a business relationship.

SECTION 5

REPORTING SUSPECTED VIOLATIONS

If you believe you have experienced retaliation, report it immediately using the channels below.

HOW TO RAISE A CONCERN

You may make a report through any of the following channels:

- Your supervisor/manager (where appropriate).
- Human Resources.
- RGIS Business Ethics Hotline (email): apacethics@rgis.com
- Legal (email): generalcounsel@rgis.com | ecordier@rgis.com

Oral reports can also be made by requesting an in-person meeting with your supervisor, HR or Legal through the email channels documented above.

WHAT INFORMATION TO INCLUDE

To help RGIS assess your report, include (if known): who was involved, what happened, when and where it occurred, how it was discovered, the names of any witnesses, and any documents or evidence.

WHAT HAPPENS NEXT

RGIS will review reports promptly and take appropriate action. This may include an internal investigation led by Legal/ Compliance and, where necessary, involvement of Human Resources, Internal Audit, Security, or external advisors. RGIS may contact you for additional information if you provide contact details. RGIS will share outcome information where appropriate and permitted.

GOOD FAITH REPORTING

Reports must be made honestly and in good faith. Knowingly false or malicious reports may lead to disciplinary action.

Reporting at:

- apacethics@rgis.com

Human Resources:

- Generalcounsel@rgis.com

Legal:

- Generalcounsel@rgis.com
- ecordier@rgis.com