Solutions, Consultation, Implementation, and Managed Services

CORP POL-0015

Fraud, Waste, and Abuse (FWA) Policy

June 2026

Version 4.0



READY COMPUTING

325 Hudson Street, Floor 4
New York, NY 10013-1004

Moulsham Mill, Parkway
Chelmsford, Essex, CM2 7PX (EMEA)

CERTIFICATIONS

TABLE OF CONTENTS

1 Introduction **2**
1.1 Purpose 2
1.2 Scope 2
1.3 Audience 2
1.4 Responsibility 2
1.5 Training and Awareness 2
1.6 Confidentiality Statement 2
2 General FWA Policy and Reporting **3**
2.1 Reporting FWA (i.e., Whistleblower Policy) 3
3 Specific Policies Related to FWA **5**
3.1 Conflict of Interest 5
3.2 Anti-Bribery and Anti-Corruption Policy 6
3.3 Insider Trading Conduct 7
3.4 False Claims Act and Healthcare Program Integrity 8
3.5 DCAA Labor-Charging and Cost Accounting Integrity 8
4 Modern Anti-Slavery and Human Trafficking Policy **9**
4.1 Supply Chain Accountability and Flow-Down 9
Appendices **10**
Appendix A: Terms, Acronyms, and Definitions 10
Appendix B: Referenced Documents 10
Appendix C: Revision History 10

1 INTRODUCTION

Integrity is at the core of Ready Computing ("Company") and all its business operations. Fraud, waste, and abuse (FWA) undermine the integrity of our organization and erode public trust. This policy outlines Ready Computing's commitment to preventing, detecting, and responding to any instances of fraud, waste, or abuse, whether intentional or unintentional. All employees, contractors, and agents play a crucial role in upholding these principles and ensuring the responsible use of resources.

1.1 Purpose

The purpose of this Policy is to define the FWA requirements that all Personnel must follow.

1.2 Scope

This policy applies to all personnel, including employees, contractors, and agents, at all Ready Computing entities and locations worldwide. It governs all business operations and activities that involve Ready Computing's resources, funds, or data, with specific emphasis on activities subject to federal and state healthcare program requirements, government contracting regulations, and other applicable laws related to fraud, waste, and abuse.

1.3 Audience

This Policy applies to all Personnel.

1.4 Responsibility

All Company Personnel are expected to read, understand, and comply with this Policy. All Company Personnel are equally responsible for the prevention, detection, and reporting of FWA. Company Personnel are required to avoid any activities that could lead to, or imply, a violation of this Policy.

If anyone has reason to believe or suspect that an instance of FWA has occurred, or will occur in the future, you must refer to 2.1 Reporting FWA and follow the requirements therein.

1.5 Training and Awareness

For Ready Computing Personnel, the Company:

- Provides this Documentation in a virtual location that is accessible to all Personnel.
- Communicate the release and subsequent updates made to this Policy, at least, annually.

For those that conduct business with Ready Computing, the Company:

- Requires formal acceptance of Company Policy through flow-downs in legal contracts.

1.6 Confidentiality Statement

The information contained within this document is intended for either internal or external use but is confidential in nature. Any review, retransmission, dissemination, or other use of the information in this document by persons or entities other than approved Company Personnel is strictly prohibited. Any unintended recipient of this document is expected to immediately contact the Company and destroy any copies of this document.

2 GENERAL FWA POLICY AND REPORTING

Engaging in any form of fraud, waste, or abuse is strictly prohibited. Any Company Personnel who have knowledge of FWA, or who has good reason to suspect that such conduct has occurred, must immediately report the activity or suspicion following the guidance in the next section.

2.1 Reporting FWA (i.e., Whistleblower Policy)

The following must be used for all forms of FWA defined throughout this Policy.

2.1.1 Reporting FWA Internally

Primary Reporting Contact

- The Vice President of Compliance and Risk Management is authorized to process all FWA claims. This should be your first point of contact.
    - Compliance and Risk Management Department: quality@readycomputing.com

Secondary Reporting Contacts

These secondary contacts may also be contacted, at your discretion; but with follow-up to ensure that the report was delivered to the highest level of authority at the Company.

- Any member of Executive Leadership (i.e., CEO, CISO, COO, etc.)
- Legal Department: legal@readycomputing.com
- Human Resources: HR@readycomputing.com

2.1.2 Reporting FWA Externally

Company Personnel should make every effort to do their due diligence to report FWA or suspicion of it internally first. That said, under extreme circumstances, Company Personnel may also report it externally:

- Any international governmental body relevant to your location.
- The Department of Homeland Security and/or Health and Human Services
    - www.oig.dhs.gov / 1-800-323-8603 Toll-Free
    - www.oig.hhs.gov/report-fraud / 1-800-HHS-TIPS
- A member of Congress or a representative of a committee of Congress
- The Department of Justice or other law enforcement agency; a court or grand jury

2.1.3 Reporting FWA Anonymously

The Company is committed to an environment of open communication. While we encourage employees to engage in direct dialogue with the Compliance and Risk Management team, we recognize that certain situations require an extra layer of confidentiality.

If you wish to report concerns regarding potential fraud, waste, or abuse anonymously, you may utilize the following secure channels:

- (917) 633-4871
- (212) 877-3307 Ext. 202

These voice mailboxes are securely managed and monitored exclusively by the VP of Compliance and Risk Management.

Note: Your privacy is respected. Reports made through these channels allow you to provide information without disclosing your identity.

2.1.4 Anti-Retaliation

Anyone reporting FWA will not be retaliated against in any manner. In addition, you will not be subject to discipline for reporting a threat or cooperating in an investigation.

- If you initiate, participate, are involved in retaliation, or obstruct an investigation into conduct prohibited by this Policy, you will be subject to discipline up to and including termination.
- If you believe you have been retaliated against, immediately report it to the HR Department.

In addition to our company's zero-tolerance policy on retaliation, employees are afforded specific whistleblower rights and protections under federal law, as described in clauses such as **FAR 52.203-17**.

3 SPECIFIC POLICIES RELATED TO FWA

The following section of this document provides clear policy for the following sub-programs of our Fraud, Waste, and Abuse program.

3.1 Conflict of Interest

There are two types of Conflict of Interest relevant to Ready Computing:

- Personal Conflicts of Interest
- Organizational Conflicts of Interest

3.1.1 Personal Conflict of Interest

Personnel have a legal duty of good faith and loyalty to the Company and should always act in the best interest of the Company. To avoid potential conflicts of interest, Personnel should avoid activities that could reasonably put them in a conflicting situation. A personal conflict of interest occurs when the Personnel's financial or personal interest, or interests of a family member interferes with, or even appears to interfere with, the Company's legitimate business interests or with the Personnel's ability to perform work-related duties objectively and effectively. All potential conflicts must be formally disclosed using the *CORP FORM-0002_Conflict of Interest Form*.

Furthermore, personnel assigned to specific federal contracts may be subject to a more formal Conflict of Interest program, including mandatory training and annual disclosures, to comply with requirements such as **FAR 52.203-16**.

3.1.2 Organizational Conflict of Interest in Government Contract Work

An organizational conflict of interest may occur when the Company's past or current projects, relationships, or knowledge of non-public information gives the Company bias or an unfair competitive advantage. As a result of the other projects, relationships, or knowledge, the Company may be in danger of being unable to provide the government with objective advice, assistance, or performance of work. Therefore, Personnel involved in a government proposal and/or project are expected to immediately report any recognized, existing, or potential organizational conflicts of interest using the *CORP FORM-0002_Conflict of Interest Form* and/or any communication mechanisms provided in section 2.1.1 Reporting FWA.

3.1.2.1 Hiring Government Personnel

Special concerns apply to hiring or retaining former and current government Personnel. Additionally, special constraints apply to communication concerning the employment of procurement officials. Therefore, the Company and Personnel shall:

- Not conduct any discussions regarding, or make any offer of, future employment without first clearing such action with the Company's Founder and CEO, Chief Financial Officer (CFO), and/or Legal Department; nor
- Add a former government Personnel onto a federal contract project without first clearing such action with the Company's Founder and CEO, CFO, and/or Legal Department.
- HR Must obtain a written ethics opinion letter for covered officials (DFAR 252.203-7000).

3.2 Anti-Bribery and Anti-Corruption Policy

Ready Computing has a zero-tolerance policy regarding bribery and corruption. It is committed to acting with integrity in all its business dealings and relationships and implementing and enforcing effective systems to prevent bribery and corruption. This section establishes the mandatory rules for complying with U.S. and U.K. anti-corruption laws and the requirements of the Federal Acquisition Regulation (FAR), including **FAR 52.203-3 (Gratuities)** and **FAR 52.203-7 (Anti-Kickback Procedures)**.

Note: This Policy does not form any part of a Company Personnel's contract. The Company may amend it at any time to improve its effectiveness in combatting bribery and corruption.

3.2.1 Compliance with Laws

The Company and Company Personnel must obey all applicable laws and regulations that affect the Company's business. This Policy covers laws relating to anti-bribery and corruption in the U.K., including the Bribery Act 2010 ("UKBA"), and all associated laws and regulations in the U.S. Personnel must:

- Have a general understanding of laws governing Personnel's areas of responsibility.
- Seek guidance prior to acting if there is any doubt concerning the application of a law or regulation.
- Report any instance of, or suspicion of, anything related to this Policy.

3.2.2 Reporting Bribery and/or Corruption

The following sections provide a non-exhaustive list of things to establish commonality. Please note, that using reasonable judgment is best, but if you are ever faced with a circumstance in which you have a question, need to report bribery or corruption, or have suspicion of bribery or corruption, please reach out to any of the following departments using any of the communication mechanisms provided in section 2.1.1 Reporting FWA.

3.2.2.1 Gifts and Hospitality

Normal and appropriate gestures of hospitality and goodwill (whether given to or received from third parties) are acceptable so long as a gift meets the following requirements:

- It is **NOT** given to any recipient who works for any governmental body.
- It is not defined as anything in the section Terms and Definitions.
- It is not made with the suggestion that a return favor is expected (i.e., "quid pro quo").
- It is given in the name of the Company, not in an individual's name.
- It does not include cash or a cash equivalent (e.g., a voucher or gift certificate).
- It is appropriate for the circumstances (e.g., giving small gifts around Christmas).
- It is given or received openly, not secretly.
- It is not selectively given to a key, influential person.
- It is not above 100 USD (or the equivalent value in local currency, e.g., GBP).
- In circumstances where it may be considered inappropriate to decline the offer of a gift, as determined by the Legal Department and/or HR Department.

Important Note: The Finance Department will keep detailed and accurate records and will have internal controls in place to declare and keep a written record of gifts and/or hospitality.

3.2.3 Facilitation Payments and Kickbacks

Accepting or making any form of facilitation payment or kickback of any nature is **prohibited**.

3.2.4 Political Contributions

The Company will never make any form of political donation.

3.2.5 Charitable Contributions

The Company encourages the act of donating to charities — whether through services, knowledge, time, or direct financial contributions (cash or otherwise) — and agrees to disclose all charitable contributions it makes. Company Personnel must be careful to ensure that charitable contributions made by or on behalf of the Company are not used to facilitate and conceal acts of Bribery. The Company will ensure that all charitable donations made are legal and ethical under local laws and practices, and that donations are not offered or made without the Company approval.

3.2.6 Special/Extreme Circumstances

The Company recognizes that Company Personnel may face a situation where avoiding a facilitation payment or kickback may put their safety or that of their family at risk. Under these circumstances, Personnel must:

1. Keep any amount to a reasonable minimum.
2. Ask for a receipt detailing the amount and reason for the payment.
3. Create a record concerning the payment.
4. Report this incident as defined in section 2.1 Reporting FWA.

3.3 Insider Trading Conduct

Anyone with knowledge of material, nonpublic information about a company may be considered an "Insider" for purposes of laws and statutes which prohibit or restrict insider trading ("Insider Trading Laws"). It is a violation of Company policy, and may be a violation of Insider Trading Laws, for any Personnel to:

- Trade in any securities while aware of "material nonpublic information" concerning any company, or
- Communicate, "tip," or disclose material nonpublic information to outsiders so that they may trade securities of any company, based on that information.

To prevent even the appearance of improper insider trading or tipping, it is important that all Personnel read, understand, and comply with this policy.

3.3.1 "Material" Information

"Material Information" can be any information pertaining to a company that reasonable financial personnel would consider to be important in making any decision related to investments (i.e., buy or sell a company's securities). Below are some examples of "Material Information" that Company Personnel may encounter while performing their duties.

Note: This is a non-exhaustive list.

- A significant cybersecurity incident experienced that has not yet been made public.
- Potential mergers and acquisitions or the sale of company assets or subsidiaries.
- New major contracts, orders, suppliers, customers, or finance sources, or the loss thereof.
- Major discoveries or significant changes or developments in products or product lines, research, or technologies.
- Significant changes in management.
- Actual or potential exposure to major litigation, or the resolution of such litigation.
- Significant changes in sales volumes, market share, production scheduling, or pricing.

3.3.2 "Nonpublic" Information

Information is typically considered "nonpublic" until it has been widely disseminated to the public. This can occur through any major news service. Additional provisions state that 'the market' should also have sufficient time to digest any information from a major news source.

3.3.3 Inquiries

Please direct all inquiries regarding insider trading to:

- The Compliance and Risk Management Department: quality@readycomputing.com.

3.3.4 Penalty and Consequences

Penalties and consequences of prohibited insider trading or tipping can be severe. Violation of this Policy by any Personnel may result in disciplinary action by the Company, up to and including immediate termination for cause. Moreover, persons violating insider trading or tipping rules may also be subject to legal consequences.

3.4 False Claims Act and Healthcare Program Integrity

Ready Computing strictly prohibits the submission of false, fictitious, or fraudulent claims for payment or approval to the U.S. Government or any state healthcare program (e.g., Medicare/Medicaid), in direct compliance with the False Claims Act (31 U.S.C. §§ 3729-3733) and the Program Fraud Civil Remedies Act. Personnel involved in the development, deployment, or support of Health IT systems must ensure that no data, deliverable, or claim is manipulated to improperly secure federal funds.

3.5 DCAA Labor-Charging and Cost Accounting Integrity

In alignment with FAR Part 31 and DCAA compliance standards, the deliberate mischarging of time, labor hours, or expenses to government or commercial contracts constitutes Fraud. Personnel must accurately record time and expenses in accordance with the *Timekeeping Policy (ACC POL-0001)* and *Expense Reporting Policy (ACC POL-0002)*. Management is strictly prohibited from directing personnel to misallocate hours across projects to manipulate cost-reimbursement ceilings.

4 MODERN ANTI-SLAVERY AND HUMAN TRAFFICKING POLICY

The Company is opposed to all forms of human trafficking, slavery, servitude, forced or compulsory labor, and any other trafficking-related activities and is committed to fully complying with all applicable international human rights standards and labor laws.

Ready Computing achieves this through a multi-layered control system:

- **Training and Awareness:** A formal commitment to ethical conduct is embedded in our U.S. Employee Handbook and annual compliance training.
- **Risk-Based Monitoring:** Our Enterprise Risk Management (ERIM) Policy includes the formal monitoring of our operations and supply chain for any potential human rights risks.
- **Regulatory Intelligence:** We conduct regular reviews of laws and regulations related to this topic.
- **Third-Party Attestation:** We maintain documented participation in the **UK Modern Slavery Registry**.

4.1 Supply Chain Accountability and Flow-Down

As a condition of doing business with Ready Computing, all third-party suppliers, partners, and subcontractors must operate with the same ethical principles established in this policy and our *QMS PLN-0007_Supply Chain Risk Management Plan*.

All levels of the Company's supply chain must:

- Have effective controls to ensure that applicable laws and regulations related to Modern Anti-Slavery and Human Trafficking are followed.
- Not retaliate against anyone who, in good faith, reports potential misconduct.
- Cooperate in audits, investigations, and reviews as required.
- Promptly report any potential violations to Ready Computing.

APPENDICES

Appendix A: Terms, Acronyms, and Definitions

Refer to Ready Computing's centralized Terms, Acronyms, Definitions record (*QMS REC-0052)* on *Ready Connect* for more information.

Appendix B: Referenced Documents

To ensure data integrity and prevent conflicting versions, Ready Computing does not maintain static lists of references within individual manuals.

The **QMS REC-0001_Document Control Master List (DCML)** is the sole, authoritative index of all active Policies, Plans, Procedures, and Records within the Integrated Management System (IMS). Please refer to the DCML for the current version and status of all documents referenced in this document.

Appendix C: Revision History

Date	Version	Name	Status
12/12/2023	0.1	Director of Compliance and Risk Management	Initial Draft
12/13/2023	0.2	Compliance and Risk Management Specialist	Revised
12/14/2023	0.3	Project Manager	Revised
12/18/2023	0.4	Director of HR Director of Compliance and Risk Management	Revised Approved
12/19/2023	1.0	Director of Compliance and Risk Management	Final
11/12/2024	1.1	Quality Assurance Specialist	Revised
11/13/2024	1.2	Risk and Compliance Specialist	Revised
11/14/2024	1.3	Director of Compliance and Risk Management	Revised
11/14/2024	1.4	Director of Compliance and Risk Management	Approved
11/14/2024	2.0	Director of Compliance and Risk Management	Final
10/01/2025	2.1	Director of Compliance and Risk Management	Revised
10/07/2025	2.2	Risk and Compliance Coordinator	Revised
10/27/2025	2.3	Director of Compliance and Risk Management	Revised
11/20/2025 11/21/2025 11/21/2025 11/21/2025 11/21/2025 11/21/2025	2.4	Chief Information Security Officer Founder and CEO Chief Finance Officer Chief Operating Officer Chief Services Officer Chief Technology Officer	Approved Abstained Abstained Abstained Abstained Abstained
11/24/2025	2.5	Director of Compliance and Risk Management	Approved
12/01/2025	3.0	Director of Compliance and Risk Management	Final

Date	Version	Name	Status
04/09/2026	3.1	Risk and Compliance Manager	Revised
06/22/2026	3.2	VP of Compliance and Risk Management	Approved
06/22/2026	4.0	VP of Compliance and Risk Management	Final

Table 1: Revision History Table