RSA

How We Win: RSA Code of Conduct

March 15, 2023

OWN YOUR IDENTITY.

Table of Contents

1. Introduction.

The RSA Code of Conduct (the "Code") provides guidance on how to carry out daily activities across RSA Security LLC and affiliates ("RSA") in accordance with our culture and values, as well as in compliance with the letter and spirit of all applicable laws.

All employees must adhere to the RSA Code, and the policies and standards which flow from our Code. This includes officers, directors, shareholders and employees of RSA. Failure to do so may result in disciplinary action, up to and including termination, in accordance with local law. Employees must be familiar with the Code and the policies and standards that apply to their role. Of course, our Code and policies can't address every possible situation, so it is up to employees to use good judgment and seek help whenever they have questions or aren't sure about the right course of action. We also expect our contingent workers, agents, and all others acting on behalf of RSA to hold themselves to equally high standards.

Our Code is a global Code. RSA is based in the United States, and thus must adhere to all laws applicable to U.S. based corporations. We proudly employ team members and serve customers all over the world. As a result, we must comply with both U.S. laws and the laws of all other countries where we do business. In those rare circumstances where it appears that local law may conflict with U.S. law, contact the Legal Department or Ethics for guidance.

2. Commitment.

We all need to show commitment to our culture and values by acknowledging that we've read, understood, and agreed to abide by the Code. We are required to do this when we are hired and to renew this commitment annually. Please note, the Code is not a contract of employment, and RSA may interpret, modify, or rescind some or all of the Code provisions, as well as related policies and standards, at any time.

RSA employees commit to always use their best judgment while performing their job responsibilities.

3. Culture and Values.

Our commitment to winning with integrity requires that we commit to operating in accordance with applicable laws and regulations, and in conformity with high standards of business conduct. To foster this collective commitment, each RSA employee must act with integrity, conduct business ethically, and protect RSA's interests. Our success depends on it.

We know our culture matters in how we run the business, how we go to market and how we treat each other. It describes what we care about, the things in which we're willing to invest, and the rules that define us as a team. Our culture is defined by our values and made real every day by how we work and lead.

We believe that what we expect from our people, how we support them in achieving those expectations, and how we measure and reward them for doing so is fundamental to our success and the longevity of our culture. Our values reflect what's most important to us as a company and guide our decisions and actions.

Our values are:

5 Core Values

Focus on the customer

- Be the problem-solver and confidant that customers want
- We work for our customers—keep them present in all internal conversations
- Build trust with our customers that we keep our promises

Play and win as a team

- There's no I in RSA; we listen to and support our teammates
- We hold each other accountable, but have each other's back
- We believe in each other's abilities to deliver

Take smart risks

- We believe that innovation wins
- We support individuals and teams to try new things
- We act with a global perspective and refine as we go

Think strategically and act decisively

- We know speed wins in business
- We don't let perfection get in the way of great
- We act with a global perspective and refine as we go

Believe in RSA

- We choose RSA and our fellow team members every day
- We're excited about whatever comes next
- Together we own RSA's future

4. We Leverage the Code.

The Code isn't something you read once. It's a guide to putting our values into action. Everyone is responsible for reading and understanding how the Code applies to them and what they do at RSA. To help apply the information, each topic has a key takeaway.

If you have questions about any topic in the Code, talk to your leader or contact Human Resources or the Legal Department.

To supplement the general guidance of the Code, RSA has adopted more specific policies and standards that apply globally, geographically, or to specific business units, functions, or departments.

5. RSA Leaders.

Being a people manager at RSA comes with responsibilities. Managers have a special responsibility to lead with integrity. It is not enough for a manager to behave legally and ethically. They must also take affirmative steps to influence their team members to do the same.

To satisfy this requirement, managers must be vocal and make a visible commitment to integrity. They must not only adhere to the law, the RSA Code, and policies and standards, but they must promote adherence and ethical behavior among their team members. This means they must:

- **Be a positive role model**. Actions speak louder than words, so let actions demonstrate the belief that although business goals are important, they can never be achieved at the cost of compliance with legal requirements and ethical principles. We can do both—we can win with integrity.
- **Set the right tone**. Be comfortable talking with team members about the importance of acting legally and ethically. Explain how our Code supports our purpose and values and ensures our success. Find opportunities to review important concepts during team meetings.
- **Thoughtfully complete ethics and compliance training promptly, and make sure team members do the same**.
- **Become familiar with the Code, policies, and standards that apply to the organization**. Adopt and follow processes designed to ensure compliance.
- **Celebrate achievement**. Recognize and reward team members whose behavior exemplifies our value of integrity.
- **Create an environment where team members know they can ask questions or raise concerns without fear of reprisal**. Be available to answer team members' questions and address their concerns. Never retaliate against anyone who reports a good faith concern or cooperates with internal investigations or audits. And don't tolerate others who do.
- **Provide appropriate supervision to ensure compliance with the Code**. Report any behavior that is illegal or violates RSA's Code, policies, or standards.

6. RSA Makes Values-Based Decisions.

The PULSE model provides a simple, clear structure to use when making challenging decisions.

Pause	Use	Look	Select	Explain
Pause to reflect on your point of view Take a few minutes to consider where you are and your view of the situation. Taking time to reflect on the situation seems obvious, but obvious or not, we often rush ahead when under pressure and make snap decisions based on our goal to deal with problems quickly.	**Use our values, policies, and legal considerations to come up with a solution** Use our values, policies, and the law to consider solutions. Ask yourself: • Is it legal? • Does it comply with our policies? • Does it reflect our values and ethical principles? • Does it respect our people, shareholders, customers, partners, communities, and planet?	**Look at alternative solutions** In situations where there are identifiable risks, competing values, and fast-moving issues, never leap to the first (or most obvious) decision. Consider alternatives and think through the risks, values being applied (or not applied), and how your decision will effectively apply answers from the previous step?	**Select the option that fits best** You are now able to use your experience, training, and your intuition. But the context for selecting the best option is now based on a clear perspective of the situation, the inherent risks, and a set of alternative solutions.	**Explain your decision clearly and honestly** Take the time to explain your decision to the key stakeholders who will be affected by the decision. The knowledge that you will be explaining your decision will inevitably affect the decision you make. Transparency is a challenge we hold in mind while the PULSE process unfolds.

7. Customers

RSA customers and broader stakeholders are the reasons we exist, and they rely on us to listen and provide solutions that will help them succeed. They expect us to operate with the highest ethical standards. To earn and maintain their trust, we are committed to doing business fairly, honestly, legally, and ethically wherever we operate in the world.

8. Privacy

Most countries regulate the collection, use, storage, disclosure, deletion, and international movement of personal information. When accessing or handling personal information, RSA must comply with applicable laws and regulations, contractual obligations, the RSA Code, policies, and voluntarily adopted standards for protecting individuals' personal information.

RSA is intentional and careful with personal information. We use lawful means to access, collect, use, share, transfer or store the personal information of others, and we use personal information solely for legitimate business. Please visit our RSA Privacy Policy currently available at https://www.rsa.com/privacy/ for more information about RSA privacy practices.

Privacy Principles that RSA employees must follow whenever processing personal information:

1. Lawfulness, Fairness, and Transparency: Only process personal information lawfully, fairly, and in a transparent manner.
2. Storage Limitation: Keep personal information for no longer than is necessary for the purposes for which it was processed.
3. Purpose Limitation: Collect personal information for specified, explicit, and legitimate purposes, and do not process personal information in a manner that is incompatible with those purposes.

4. Data Minimization: Personal information shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
5. Accuracy: Keep personal information accurate and, where necessary, up to date.
6. Integrity and Confidentiality: Process personal and health information in a secure manner to protect against unauthorized or unlawful processing and against loss, destruction, or damage.
7. Accountability: RSA shall be responsible for and able to demonstrate compliance with the principles described above.

Processor vs Controller: RSA has different obligations when acting as either a controller or processor.

- **RSA is a processor** when we do not determine the means and purposes of the personal information we process. RSA is a processor when we process personal information on behalf of our clients. In this case, and among other things, RSA is not required to give notice to these individuals of how we will use their personal information. That is the responsibility of the client - or controller.
- **RSA is a controller** when we determine the means and purposes of the personal data we process. This is largely applicable, but not exclusive, to our marketing, sales, IT, and HR teams. Ask privacy compliance about the various obligations you or your team may have to meet if you are in one of these teams and process personal information. Contact us at **privacy@rsa.com**.

Whether RSA is a processor or controller, we keep personal information secure in accordance with RSA security requirements. Additional specific safeguards apply to customers' payment card and other financial information.

Collecting, Using and Sharing Personal Information: If your role requires you to have access to personal information, do not collect, use, access, or share personal information except as necessary for your job and the jobs of those with whom you share information. If you or your team initiate an activity where personal information will be collected, consult with the Privacy team at privacy@rsa.com to determine whether a privacy impact or security assessment is necessary. If you transfer personal information from one country to another, even to share with a colleague or third party in another country, make sure the transfer is an approved part of your job.

We must respect individuals' wishes if they choose to exercise their privacy rights on their own personal information. Should you get an inquiry from an individual regarding information we hold on that person, you should handle that request in accordance with RSA Privacy Policy. If you have any questions, forward the inquiry to the Privacy team at privacy@rsa.com.

When authorized to dispose of personal information, be certain to do so responsibly and in accordance with RSA policies and standards.

Information about former employees, including but not limited to periods of employment, job duties, and performance, may not be shared with any third parties except as explicitly authorized by Human Resources. Any such requests should be directed to Human Resources.

Third Parties: RSA business partners must share our commitment to protecting and appropriately using personal information. Before sharing personal information with any business partner, be sure the partner has executed the appropriate contracts, memorializing their commitment to following the law and adhering to RSA's policies and standards. For more information regarding working with our channel partners, see RSA's Supplier Principles provisions on protecting and securing customer and team member personal information.

9. Quality, Safety, and Security in our Solutions.

- RSA focuses on earning our customers' trust and loyalty by:
- Listening to, learning from, and responding to our customers
- Delivering products, services, and solutions that consistently meet expectations for quality, value and customer experience
- Driving continual process, product, and service improvements
- Measuring customer satisfaction, trust, and loyalty

We expect our suppliers to implement and maintain robust policies and procedures to avoid procuring or otherwise introducing counterfeit parts into the RSA supply chain. To the extent that you have questions regarding our purchasing (and anti-counterfeit) procedures, you should notify the Legal Department.

We are committed to compliance with the laws and regulations in each country into which our products are shipped. Our products are designed and tested to meet or exceed the appropriate worldwide standards. RSA complies with applicable environmental regulations and laws, and takes every opportunity to minimize potential harmful impacts to our planet. In addition to meeting all applicable legal and regulatory requirements, RSA strives to have safe products that are secure and dependable.

10. Unfair Competition

Virtually all countries have laws prohibiting or regulating transactions and relationships that could have the purpose or effect of limiting competition. RSA knows it must compete fairly and vigorously and in full compliance with these laws. Any violation of these laws may result in discipline and could result in civil or criminal penalties. RSA believes that a free and competitive market serves our customers best. Competition laws are complex, and employees should consult the Legal Department before entering into any discussions with competitors, customers, resellers, or suppliers about agreements or arrangements, whether in writing, oral, or implied, that could have the effect of limiting competition or that could be perceived as having such effect.

The following types of arrangements are or could be viewed as anti-competitive and can never be discussed or entered into without advance, express written consent from the Legal Department:

- Agreements to fix or control prices
- Agreements not to compete for certain business or bids, or agreements with competitors on the terms of any bids
- Agreements between companies, whether competitors or not, to not hire or solicit employees or to set employee compensation
- Boycotting specified suppliers or customers
- Agreements to divide or allocate markets or customers
- Limiting the production or sale of certain product lines
- Pricing agreements among competitors such as coordinated price increases, follow-the-leader pricing, rotation of bids or proposals, so that each competitor takes a turn in sequence as low bidder, or so that certain competitors bid low only on some sizes of contracts and high on other sizes
- Division of the market by competitors, so that certain competitors bid low only for contracts let by certain agencies, or for contracts in certain geographical areas, or on certain products, and bid high on all other jobs
- Establishment by competitors of a collusive price estimating system

- Engaging in monopolization or attempted monopolization through unfair conduct such as pricing below cost with the intent to cause a competitor's market exit (predatory pricing)
- Tying or bundling certain products in a sale, or any other agreements that would have the effect of limiting competition

Be especially careful when interacting with competitors in connection with benchmarking, industry associations, or standards setting bodies or while attending seminars or conventions. To avoid even the appearance of an agreement, avoid discussing with competitors such things as prices, terms of sale, territories, customers, bids, volumes, costs, profits, market share, salaries, hiring practices, distribution methods, relationships with suppliers, or non-public information about product or services. Competition laws are complex. Always consult with your manager and the Legal Department before entering into any discussions with competitors, customers, resellers, or suppliers about agreements or arrangements, whether in writing, oral, or implied, that could have the effect of limiting competition or that could be perceived as having such an effect.

The antitrust laws are complicated. Employees who suspect a violation of, or have questions regarding, the antitrust laws must immediately notify the Legal Department at legalnotices@rsa.com.

11. Pricing and Contracting

RSA has established policies, standards, procedures, and controls to govern the negotiation and approval of contracts. RSA ensures compliance with legal, accounting, and financial reporting requirements, and protects RSA's assets from fraud, waste, and abuse, by having established policies in place that govern the negotiation and approval of contracts between RSA and its customers, suppliers, business partners, and other stakeholders.

Authority to enter into or sign contracts on behalf of RSA has been delegated to certain team members depending on the nature, scope, and financial value of the contract involved. Employees involved in negotiating on behalf of RSA must make sure they understand and follow the contracting policies, act only within the authority delegated to the employee under those policies and related signatory authority matrices, and ensure that all necessary approvals from the Finance, Accounting, Global Procurement, and Legal Departments have been obtained.

12. Government Contract Regulations

RSA understands that contracts with government customers, or commercial transactions financed in whole or in part with public funds, have additional requirements.

We follow the rules: If an employee is involved with public customers, the employee must ensure that they understand and comply with all applicable rules. Likewise, the employee must be diligent in requiring that consultants, resellers, suppliers, or other business partners providing goods or services in connection with government or publicly funded contracts meet all qualification and performance standards and requirements. The consequences of non-compliance are serious.

We secure business the right way: Information submitted in connection with bids or tenders for government contracts must be current, accurate, and complete.

RSA will not offer bribes, kickbacks, or preferential treatment in connection with a government contract. With limited exceptions (which must be pre-approved in writing by the Legal Department), we are also prohibited from providing anything of monetary value to government employees or their family members. This includes gifts, hospitality, travel, lodging, services, discounts, and meals. Contributions to, and favorable

statements about political parties and government bodies on RSA's behalf are not permitted. The Anti-Kickback Act of 1986 prohibits kickbacks because they undermine fair competition, and the statute's civil and criminal penalties seek to ensure that we select suppliers based on merit, not because of gifts. A kickback can take the form of money, a fee, a commission, a credit, a gift, a gratuity, an item of value, or compensation of any kind. If you accept a kickback (directly or indirectly) from any vendor or subcontractor, you are subject to termination in addition to possible criminal prosecution.

Although business courtesies are commonplace in the commercial marketplace, they may constitute kickbacks in the government contracting arena. If you have a question as to whether a business courtesy constitutes a kickback, you should contact the Legal Department before accepting anything of value from a supplier, subcontractor, or teaming partner. If you suspect a violation of the kickback laws you must immediately report your concern to the Legal Department.

Federal law may prohibit you from unreasonably precluding subcontractors from making direct sales to the government of any supplies or services. RSA is not, however, precluded from asserting rights that are otherwise authorized by law or regulation. You should consult the Legal Department before imposing on subcontractors any restrictions on selling directly to the government.

For additional guidance regarding sales to the U.S. government, please contact the Legal Department.

13. Diversity, Equal Opportunity, and Respect.

RSA is committed to diversity and equality, as well as respect for the individual. We are committed to providing a safe and productive environment that fosters open dialogue, and the freedom to express ideas that are free of harassment, discrimination, and hostile conduct. We recognize a shared responsibility to create and maintain that environment for the benefit of all.

We promote equal opportunities and fair treatment for all team members, customers, business partners and other stakeholders, regardless of race, color, religion or belief, creed, national, social, or ethnic origin, sex (including pregnancy), age, physical, mental or sensory disability, HIV status, sexual orientation, gender identity and/or expression, marital, civil union or domestic partnership status, past, or present military service, family medical history or genetic information, family or parental status, protected veteran status, citizenship status when otherwise legally able to work, or any other status protected by the laws or regulations in the locations where we operate. We provide equal employment opportunities to anyone who is legally authorized to work in the applicable country and we provide reasonable accommodations to individuals with disabilities.

All team members are expected to report suspected discrimination promptly and never retaliate against anyone who raises a good faith concern that unlawful discrimination has occurred. Our commitment to these principles is essential to our success.

14. Anti-Harassment.

We treat everyone—team members, customers, business partners and other stakeholders—with dignity and respect. Everyone should be able to do their job in a safe and respectful environment without fear of harassment. Harassment is prohibited and will not be tolerated.

Harassment can include actions, language, written materials, or objects that are directed or used in a way that undermines or interferes with a person's work performance, or creates an intimidating, hostile or offensive work environment. We never target anyone for negative treatment on the basis of race, color, religion or belief, creed, national, social, or ethnic origin, sex (including pregnancy), age, physical, mental or sensory disability, HIV status, sexual orientation, gender identity and/or expression, marital, civil union or domestic partnership status, past or present military service, family medical history or genetic information, family or parental status, protected veteran status, citizenship status when otherwise legally able to work, or any other status protected by the laws or regulations in the locations where we operate.

- All forms of harassing conduct are prohibited at RSA, including without limitation:
- Unwanted sexual advances, invitations, or comments
- Visual displays such as derogatory or sexually-oriented pictures or gestures
- Physical conduct including assault or unwanted touching
- Threats or demands to submit to sexual requests as a condition of employment or to avoid negative consequences

All team members are expected to report suspected harassing conduct promptly and never retaliate against anyone who raises a good faith concern that unlawful harassment has occurred.

15. Human Rights and Anti-Slavery.

RSA respects the fundamental human rights of all persons in our value chain. We strive to ensure respect for the human rights of all team members, as well as people outside of our organization who are impacted by our value chain, such as workers in our supply chain or business partners. We prohibit the use of child, compulsory, or forced labor and trafficking of persons for any purpose. You are also prohibited from procuring commercial sex acts during the period of performance of a government contract. We expect our suppliers to follow the same standards.

If employees or third parties suspect their (or another's) rights are at risk, or are being asked to conduct business in a way that could violate another person's fundamental human rights, we encourage employees to speak up.

16. Environmental Health and Safety (EHS).

RSA team members are expected to perform their work in full compliance with all applicable health, safety, and environmental laws and regulations. The requirement applies whether the employee is working at an RSA site, a customer site, or a remote location. Additionally, alcohol, illegal drugs, and controlled substances can adversely affect safety, productivity, attitude, reliability, and judgment. Apart from lawful, moderate, and prudent alcohol consumption during legitimate business entertainment, employees are prohibited from consuming or being under the influence of alcohol, or possessing, distributing, or being under the influence of illegal drugs while engaging in RSA business. In addition, RSA team members must complete all EHS training as may be required.

RSA employees must report all accidents, injuries, unsafe work conditions, releases to the environment, and other EHS concerns immediately to their supervisor, and to others as described in the applicable procedures. If they hire and/or procure contractor or business partner work, they must ensure that each contractor and partner has an EHS program appropriate to the type of work to be performed, is made aware of other potential hazards in the work area, and follows RSA's contractor safety and environmental requirements. If an employee is working at customer or supplier/partner locations, they must follow the stricter of RSA's or the customer or supplier/partner's EHS requirements.

RSA employees are prohibited from text messaging while driving either RSA-owned or -rented vehicles or government-owned vehicles, or privately owned vehicles, when on official RSA business or when performing any work for or on behalf of the government.

17. Workplace Violence.

A workplace free of violence, weapons, and other disruptive behavior keeps team members safe.

A non-violent workplace starts with being polite and respectful. If employees disagree with a team member or other person at work, they are encouraged to resolve it calmly. Never bully, threaten, intimidate, or harm another person or their property through verbal behavior (written or oral) or non-verbal behavior (such as gestures or expressions).

Unless authorized by law or RSA policy, employees may not possess, conceal, or use weapons, including firearms, knives, clubs, ammunition, explosives, or other devices that are primarily used to inflict injury (including recreational weapons such as hunting rifles or crossbows, toy weapons, or replicas that can easily be viewed by most people to be real or authentic) while on RSA property or when conducting RSA business. This prohibition does not apply to knives or other tools which are required, permitted, or provided by RSA as part of their job assignment.

This policy applies to anyone who enters RSA property, which includes buildings, parking lots, walkways, and any other property we own, lease, or occupy.

18. Safeguarding RSA Confidential Information.

RSA confidential or proprietary information is a tremendous asset that differentiates us from our competitors and is protected by law and key agreements. Some of this information is also considered protectable trade secrets under the law. Every employee is responsible for the protection of RSA confidential or proprietary information and trade secrets. Misusing or disclosing information that RSA considers confidential or proprietary or a trade secret, whether during or after employment, is prohibited and is a violation of the Code of Conduct and employee's agreement with RSA. In certain circumstances, it may also be a violation of law. Inappropriate disclosure may also result in profound consequences to the employee and RSA. Before disclosing or distributing any confidential information, senior management approval must be obtained and the appropriate terms of use established. This often requires the execution of a written confidentiality or nondisclosure agreement, which restricts the use, disclosure, or distribution of the information.

What is RSA confidential or proprietary information?

RSA confidential information is any information that is not publicly available and/or has a level of sensitivity requiring increased protection, management, or disposition. Confidential information includes (but is not limited to) information about our company, our products, nonpublic financial information, personal information about our team members, and third-party information that has been entrusted to us to protect and is denoted by the RSA data classification standard.

What does safeguarding confidential information mean?

Both during the employee's employment and thereafter, the employee is prohibited from using RSA confidential or proprietary information for their own benefit or disclosing such information to anyone outside of RSA, without express authorization, unless permitted to do so.

All RSA confidential or proprietary information must be returned when an employee terminates employment with RSA. Any taking, downloading, disseminating, or other prohibited use or disclosure of RSA confidential or proprietary information could constitute theft of RSA property. If such RSA confidential or proprietary information is deemed a trade secret, additional laws may apply.

Additionally, an employee must take steps to prevent inadvertent disclosure of RSA confidential or proprietary information. All security rules must be followed. In addition, an employee should not discuss any non-public or confidential or proprietary information about RSA with outsiders, including family and friends, and should not discuss such information in any public place, such as an elevator, restaurant, or airplane. Even within RSA, information should be shared with others only on a "need to know" basis. For example, broadcast emails containing RSA confidential or proprietary information should be avoided. Employees should not post any RSA confidential or proprietary information when using social media tools such as blogs, internet chat boards, or social networking sites without prior express authorization. When away from RSA premises, particular care should be taken to protect RSA confidential or proprietary information, in both tangible and electronic form, to prevent inadvertent disclosure in public places.

Employees are likely to meet, talk to, or attend functions with individuals who work for RSA competitors, partners, suppliers, or customers. When employees encounter such individuals, even where the interaction seems innocent, they must be cautious about what they say. They should never discuss RSA confidential or proprietary information with competitors and must be careful to only discuss RSA confidential or proprietary information with customers, partners, or suppliers in adherence with a fully executed Non-Disclosure Agreement between RSA and the other party. In some cases, RSA has special policies or procedures in

connection with its business relationships that require heightened attention to the safeguarding of RSA confidential and proprietary information.

You should also report any attempts by outsiders to obtain RSA confidential or proprietary information by contacting privacy@rsa.com.

19. Safeguarding the Confidential Information of Others.

You may not disclose proprietary or confidential information to others within RSA who do not need to know the information to perform their jobs, or to anyone outside RSA, without prior authorization. You also must not use such information for your personal or private benefit, or for the benefit of anyone else, during or after your employment with RSA.

RSA competes vigorously, but fairly. We protect RSA's intellectual property, trade secrets, and confidential or proprietary information, and we respect the rights of others to do the same. Employees may use publicly available information about RSA competitors or other companies but may not unlawfully acquire or misuse the trade secrets or other confidential or proprietary information of any third party.

RSA prohibits the use of any means, such as cash payments, favors, or hiring a competitor's employees, to acquire confidential or proprietary information of third parties. Even if an employee receives information about another company through legitimate means, the employee needs to determine if the information is confidential or proprietary and how such information may be used. For example, check written documents for labels that designate them as private or confidential. Before using confidential information, approval from the Legal Department must be obtained and the employee must establish the appropriate terms for its use. This may require the execution of a written confidentiality or nondisclosure agreement, which restricts the use, disclosure, or distribution of information.

Once an employee has received confidential information through legitimate means, the employee should use, copy, disclose, modify, and/or distribute it only in accordance with the terms of any relevant confidentiality or nondisclosure agreement. The employee must also abide by the lawful obligations they have to their former employer(s). These obligations may include restrictions on the use and disclosure of confidential information or solicitation of former colleagues to work at RSA, or non-competition agreements.

Each of us has the responsibility to safeguard team members' personal information. We must comply with all applicable privacy and data protection laws in the countries where we operate.

Consistent with local laws, RSA may collect personal information about team members to meet legal requirements or enable effective business operations. If your role requires that you have access to team member personal information, make sure you take steps to properly secure it, and that you access or use it only when authorized by RSA for legitimate business needs and in accordance with applicable laws and RSA policies. Regardless of your role, if you gain access to a team member's personal information or other confidential data, always take care to keep it secure. Never share it with anyone—inside or outside of RSA—without the team member's permission except as necessary to meet legal or legitimate business requirements. If this information comes to you inadvertently and/or is not required as a part of your role, it is expected that you will inform Human Resources immediately.

20. Safeguarding U.S. Government Information.

You must safeguard RSA confidential and proprietary information. You also must protect sensitive information belonging to the government (classified or unclassified) or third parties that you may gain through your work on a government contract. Most importantly, we all have an obligation to protect classified National Security information.

Information Obtained During the Procurement Process

- While performing a government contract, you may receive access to non-public, sensitive information (Controlled Unclassified Information—CUI) relating either to a competitor of RSA or the government's procurement decision. You must not improperly disclose such information.
- You also must not improperly solicit competitor bid or proposal information or government source selection information. Contractor bid and proposal information consists of any information submitted to the government by a competitor in connection with a bid or proposal, such as proposals, cost or pricing information, technical solutions, or other proprietary information. Source selection information consists of non-public information that is prepared for use by a federal agency for the purpose of evaluating a bid or proposal and includes bid prices, proposed costs, source selection or evaluation plans, competitive range determinations, rankings, and evaluation reports. Any release of such information must occur (if at all) by the government and in accordance with established processes.
- If a government contract authorizes you to access contractor bid and proposal information or source selection information, you must use such information only for authorized purposes. You also must safeguard this information from unauthorized disclosure.
- If you receive bid and proposal or source selection information to which you should not have access, you must immediately take steps to limit further access to and dissemination of the information and report the issue to the Legal Department.
- If you do not know whether you should have access to information, contact the Legal Department.

U.S. classified information

- RSA must protect classified information. To that end, you must not accept or retain classified information for which you do not have the requisite security clearance. Employees with government security clearances who have access to classified information must safeguard that data according to government regulations, including applicable agency procedures. Prior to disclosing classified information, you must ensure that recipients have the proper security clearance and a "need to know."

21. Using Information Technology and Other Resources Wisely.

Employees may occasionally use RSA resources, including information technology resources, for limited personal use, but this use must be appropriate and kept to a minimum. Inappropriate use includes, but is not limited to, engaging in illegal activity, or viewing inappropriate material, including adult or pornographic sites, hate sites or sites which would put the RSA brand at risk. RSA resources should never be used excessively or to support secondary employment, outside business ventures or personal political activities. In accordance with applicable law, RSA retains the right to monitor any use of RSA provided technology, both hardware and software, and users have no implicit nor explicit right to privacy relative to such provided technology.

RSA provides information technology resources to employees to perform their roles for the company. RSA always retains ownership over the resources. Consistent with local laws, RSA reserves the right to monitor and review the use of its resources and to access all data on its resources, including its information technology resources. Where permitted by local law, employees' use of the resources constitutes consent to such monitoring and review including when utilizing encryption, which RSA reserves the right to decrypt as part of their monitoring efforts.

Each employee has an obligation to keep our information technology resources safe from viruses, malicious software programs, and intrusion attempts by following all information security policies and never tampering with or disabling the RSA managed security software on a system. Employees are responsible for all activities performed with their individually assigned user ID and their assigned IT resources. Employees must ensure that all software and hardware purchases and agreements are approved by the Information Technology Department. If an employee has access to customer information technology resources, the employee should follow policies and procedures relating to the use of such information technology resources and to information security as directed by the customer.

22. HIPAA/HITECH Privacy.

Protected health information ("PHI") is any identifiable health information that is used, maintained, stored, or transmitted by a healthcare provider, health plan or health insurer, or a healthcare clearinghouse, in relation to the provision of healthcare or payment for healthcare services.

RSA protects the privacy and confidentiality of PHI utilized by RSA. The private and confidential use of such information will be the responsibility of all employees accessing PHI in the course of their duties.

RSA has designated the following compliance officers for PHI:

- Chief Human Resources Officer—RSA's benefits plan and RSA employee's PHI
- Chief Information Security Officer—RSA's client PHI.

All RSA employees agree to:

- Not use or disclose PHI other than as permitted by RSA or as required by law
- Safeguard PHI, and prevent use or disclosure of PHI
- Report to RSA any use or disclosure of PHI not permitted by RSA of which it becomes aware, including breaches of unsecured PHI

RSA shall annually evaluate its information security-related policies and procedures to ensure that they meet the requirements of the HIPAA Security and Breach Notification Rules.

Any employee, vendor, client, or contractor found to have violated this policy may be subject to disciplinary and/or legal action.

23. Biometric Information.

"Biometric information" means any data including but not limited to retina or iris scan, fingerprints, voiceprint, scan of hand or face geometry information, or facial photographs used to identify an individual.

RSA and RSA's time and attendance vendor collect, store, and use biometric information for the purposes of identifying employees and recording time entries when utilizing biometric time clocks.

Employees understand and agree to provide biometric information to RSA as a condition of employment.

RSA will not disclose or otherwise disseminate an employee's biometric information unless:

- Authorized by the employee
- Required by local, state or federal law
- Pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction

24. Communicating Responsibly.

In the rapidly expanding world of electronic communication, social media can mean many things. *Social media* includes all means of communicating or posting information or content of any sort on the internet, including to your own or someone else's blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board or a chat room, whether or not associated or affiliated with RSA, as well as any other form of electronic communication. The same principles and guidelines found in RSA policies and basic beliefs apply to your activities online. Ultimately, you are solely responsible for what you post online. Before creating online content, consider some of the risks and rewards that are involved. Keep in mind that any of your conduct that adversely affects your job performance, the performance of fellow employees or otherwise adversely affects applicants, customers, suppliers, people who work on behalf of RSA or RSA's legitimate business interests may result in disciplinary action up to and including termination.

Employees should always communicate in ways that demonstrate RSA's values, further our purpose, and enhance our reputation and brand. Employees must avoid offensive, inflammatory, or aggressive language when communicating in connection with their role at RSA, as well as anything that would embarrass or disparage RSA. Be truthful and accurate. Do not send emails to people who do not have a legitimate need to receive them.

Unless explicitly authorized to speak on behalf of RSA, an employee must make it clear that their personal views are theirs alone and do not reflect RSA's views or represent an official company position. They must be careful not to disclose confidential or proprietary information belonging to RSA or others except to those who have a legitimate need to know and who are authorized to access the information.

Take care when using instant messaging (IM), texting, blogs, chat, social media, and other avenues for electronic or online communication. RSA supports such open communications, as long as such communications are done legally and ethically.

Inappropriate postings that may include discriminatory remarks, harassment, and threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject you to disciplinary action up to and including termination.

Be respectful

Always be fair and courteous to fellow employees, customers, applicants, suppliers, or people who work on behalf of RSA. Also, keep in mind that you are more likely to resolve work-related complaints by speaking directly with your co-workers than by posting complaints to a social media outlet. Nevertheless, if you decide to post complaints or criticism, avoid using statements, photographs, video, or audio that reasonably could be viewed as malicious, obscene, threatening, or intimidating, that disparage customers, members, employees, or suppliers, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion, or any other status protected by law or company policy.

Be honest and accurate

Make sure you are always honest and accurate when posting information or news, and if you make a mistake, correct it quickly. Be open about any previous posts you have altered. Remember that the internet archives almost everything; therefore, even deleted postings can be searched. Never post any information or rumors that you know to be false about RSA, fellow employees, applicants, customers, suppliers, people working on behalf of RSA, or competitors.

Post only appropriate and respectful content

Maintain the confidentiality of RSA trade secrets and private or confidential information. Trade secrets may include information regarding the development of systems, processes, products, know-how, customers, pricing, and technology. Do not post internal reports, policies, procedures, or other internal business-related confidential communications.

Employees may not post financial, confidential, sensitive, or proprietary information about RSA, fellow employees, applicants, customers, suppliers, or people working on behalf of RSA.

Do not create a link from your blog, website, or other social networking site to an RSA website without identifying yourself as an RSA employee.

Express only your personal opinions. Never represent yourself as a spokesperson for RSA. If RSA is a subject of the content you are creating, be clear and open about the fact that you are an employee and make it clear that your views do not represent those of RSA, fellow employees, members, customers, suppliers, or people working on behalf of RSA. If you do publish a blog or post online related to the work you do or subjects associated with RSA, make it clear that you are not speaking on behalf of RSA. It is best to include a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of RSA."

Using social media at work

Refrain from using social media while on work time or on equipment we provide, unless it is work-related as authorized by your manager or consistent with the Electronic Communication and Internet Use Policy. Do not use RSA email addresses to register on social networks, blogs, or other online tools utilized for personal use.

Retaliation is prohibited

RSA prohibits taking negative action against any employee for reporting a possible deviation from this policy or for cooperating in an investigation. Any employee who retaliates against another employee for reporting a possible deviation from this policy or for cooperating in an investigation will be subject to disciplinary action, up to and including termination.

Solicitation, Distribution, and Posting of Materials

RSA prohibits the solicitation, distribution, and posting of materials on or at RSA property by any employee or nonemployee, except as may be permitted by this policy. The sole exceptions to this policy are charitable and community activities approved and supported by RSA-sponsored programs related to RSA's products and services.

Additional Provisions

- Nonemployees may not solicit employees or distribute literature of any kind on RSA premises at any time.
- Employees may only admit nonemployees to work areas with management approval or as part of an RSA-sponsored program. These visits should not disrupt workflow. An employee must always accompany the nonemployee. Former employees are not permitted onto RSA property except for official RSA business.
- Employees may not solicit other employees during work times, except in connection with an RSA-approved or sponsored event.
- Employees may not distribute literature of any kind during work times or in any work area at any time, except in connection with an RSA-sponsored event.
- The posting of materials or electronic announcements is permitted with approval from Human Resources.

For more information
If you have questions or need further guidance, please contact the Marketing Department.

25. Speaking on RSA's Behalf.

RSA's public statements must be carefully managed to ensure accuracy, fairness, and compliance with all legal requirements, protect our reputation, and ensure consistency with our values and brand. RSA uses certain distribution channels—such as press releases, media and analyst conferences and statements on RSA.com—to communicate our company's official position to the public. Use of these channels is limited to authorized individuals and information shared must be valid, accurate, and approved for public release. Only authorized individuals can communicate the company's official position on certain topics such as financial performance, strategic business plans, legal matters, and public policy issues. Always engage Corporate Communications with questions related to speaking on behalf of RSA. Do not speak to the press or media unless you have coordinated with the Corporate Communications team. If you're asked to comment on a story or article, please decline until you have a chance to engage with Corporate Communications.

We keep our promises:

- Everything RSA tells customers and prospective customers about our products and services—in our advertising, sales and marketing communications, and otherwise—must be truthful, complete, and understandable.
- Don't mislead customers by exaggeration, by omitting vital information or by advertising products, features, or services you are not confident we can deliver.
- Make sure you comply with all internal requirements relating to the review and approval of advertising and marketing communication materials.

If you have questions or need further guidance, please contact the Corporate Communication Department.

26. Sustainable Approach.

Environmental responsibility is about incorporating sustainability into every aspect of what we do. RSA is committed to driving human progress by putting our technology and expertise to work where it can do the best for people and the planet. It is simply not enough to do “less bad.” We see technology as the key to unlocking regenerative solutions—ones that put more back into society, the environment, and the global economy than they take out. Help us uphold this commitment by incorporating sustainable thinking into every aspect of what they do. This means working to design products that utilize energy more efficiently, are made from preferable materials, or are easier to safely recycle and recover materials from at the end of their useful life. It also means streamlining our operations to minimize resource use.

Environmental responsibility is about more than creating an eco-friendly product or initiative. We partner with customers using our technology and expertise to innovate sustainable solutions that benefit our communities and the planet. We encourage employees to engage in actions that promote the health of the planet.

27. Information Lifecycle Management.

Team members, partners, contractors, and consultants are required to adhere to RSA’s information lifecycle management policies and standards. Certain RSA business, transactions and other information must be retained for a specific period in accordance with legal requirements. To adhere to those requirements, RSA has created a document retention schedule and a legal hold process. It is your responsibility to retain such information in accordance with applicable retention requirements and store it in approved, protected electronic or physical storage locations.

RSA information that is not subject to a retention schedule or legal hold or is subject to a retention schedule or legal hold but can now be disposed of because the schedule allows it or the hold has been lifted, should be disposed of in a secure manner.

28. Financial Integrity.

Our financial statements must always honestly and accurately reflect our financial and operational performance. The integrity of our financial statements and other regulatory filings is critical to the successful operation of our business, and to maintaining the confidence and trust of our shareholders, customers, business partners, and other stakeholders.

RSA does not misrepresent financial or operational performance or otherwise knowingly compromise the integrity of the company’s financial statements. We do not enter information in the company’s books or records that intentionally hides, misleads, or disguises the true nature of any financial or non-financial transaction, result, or balance, nor do we enter into any unauthorized agreements or allow any activity that could lead to that result. We follow all processes and controls designed to ensure the accuracy of RSA’s assessment and reporting of its financial results.

29. Insider Trading.

Using material non-public information for personal financial gain, or sharing it with others for their financial gain, is prohibited by company policy and potentially illegal. Employees should never use or disclose material non-public information prior to its official public release.

“Material non-public information” about a company is information that a reasonable shareholder would consider important in making a decision to buy or sell stock. Examples include yet-to-be-announced financial or company performance information, mergers or acquisitions, supplier or customer relationships, changes in senior executive management, and new products.

Insider trading occurs when an individual with knowledge of material non-public information about a company uses it to gain profits or avoid losses in the stock market. Employees may have access to “inside” information about our company or other companies, current or potential suppliers, customers, or acquisition targets. They are obligated to keep this information confidential, and the employee, their family members, and individuals with whom they have a personal relationship must never use this kind of information to trade in any company’s securities. Likewise, the employee must never provide stock tips or share inside information with any other person who might use it to trade stock. Even if the employee doesn’t intend for someone to act on the information, sharing it would violate their confidentiality obligations to RSA and could result in accusations of insider trading against them or RSA. There are serious legal penalties for insider trading and tipping, including civil liabilities and criminal sanctions (such as a possible jail sentence).

30. Anti-Bribery and Anti-Corruption.

RSA earns business because we have the best products and solutions anywhere. We don’t win business by bribing anyone, ever. Don’t accept a bribe from anyone, ever. A bribe is anything of value—such as cash, hospitality, travel, gifts, loans, charitable donations, or job opportunities—offered for an improper purpose or in order to win or keep business. RSA is committed to winning business only on the merits and integrity of its products and solutions. We do not tolerate bribery or corruption, regardless of where we are located or where we do business. Bribery and corruption are forbidden with respect to both public and private entities, both by this Code and RSA policies and standards and also, in some countries, by law.

Regardless of local practices or competitive intensity, employees must avoid all activity which could constitute bribery or corruption or could give the appearance of bribery or corruption. This is particularly the case with employees and officials of governments, state-owned or controlled entities, political parties, and international organizations. Although employees must pay particular attention when dealing with public entities and their employees, many anti-corruption laws—and this Code and RSA policies and standards—cover private entities and employees as well.

You must not offer or provide a bribe or gratuity to obtain a government contract or subcontract or to obtain favorable treatment under a contract or subcontract. Federal criminal statutes prohibit giving, offering, or promising money or anything of value, directly or indirectly, to a public official in order to influence an official act or for or because of an official act. "Items of value" can include money, gifts, favors, in-kind use of company resources, entertainment, and other items or services of value. The definitions of "public official" and "official act" are broad, and current or future procurement activity is considered an official act. These statutes carry severe penalties including fines and imprisonment.

Offering or giving a bribe or gratuity to obtain a government contract or subcontract or to obtain favorable treatment under a contract is strictly prohibited by law and this Code.

Complex rules govern the giving of gifts, hospitality, and other business courtesies to government officials and employees of governmental or quasi-governmental entities. What may be permissible for commercial customers may be illegal when dealing with the government. All payments, disbursements, rebates, marketing development funds, discounts, credits, or other exchanges of currency to a customer or third party must be for legitimate business purposes.

We comply with the anti-bribery and anti-corruption laws of the countries in which we do business, and with the U.S. Foreign Corrupt Practices Act (FCPA) as RSA is based in the United States. These laws apply to the actions of our company, our team members, and third parties who work on our behalf anywhere in the world.

Any questions related to the above should be directed to the Legal Department.

31. Trade Law Compliance.

RSA operates all over the world and complies with applicable laws regarding the import or export of goods, services, software, and technologies, including U.S. economic and trade sanctions laws and regulations, in every country in which RSA conducts business.

Trade laws provide that we cannot:

- Export products, services, technology, or software, or engage in prohibited sales to embargoed countries or to entities associated to those countries such as embassies or banks—even if the entity is located outside the embargoed country.
- Provide our products for prohibited end-uses (such as terrorist activities, missile technology and proliferation of nuclear, chemical or biological weapons).
- Provide our products to prohibited end-users (such as parties subject to comprehensive OFAC sanctions).
- Ship, transfer or release products, technology or software requiring an export license without obtaining the appropriate authorization.

When importing, we must exercise reasonable care in all customs matters to ensure that we accurately classify, value, determine country of origin, and specify all facts reportable to customs authorities. We expect our partners to demonstrate this same commitment.

RSA abides by the U.S. anti-boycott regulations, which prohibit us from cooperating with any request concerning a boycott not initiated by the U.S. government. You must not enter into an agreement, provide any information, or take any action that would cause RSA to support an illegal foreign economic boycott. You must immediately report all requests to engage in any such activity to the Legal Department. For additional information regarding trade compliance, please see the Export Compliance Manual that can be obtained through the Legal Department.

32. Theft and Fraud.

RSA will not tolerate theft and fraud. We all know that theft is taking something that doesn't belong to you without permission. It can include physically taking something like money or property, or it can be done through other means like forgery, embezzlement, or fraud. Fraud is a type of theft by deception. It is making someone believe (by words or conduct, or by concealing important information) something that isn't true, with the intent of having them take (or refrain from taking) some action that results in them suffering economic harm.

Anyone who engages in or assists others with theft or fraud in connection with their roles at RSA will be subject to disciplinary action up to and including termination and may also be subject to prosecution. Help safeguard RSA's assets and reputation by watching for any kind of fraudulent activities against RSA, our team members, customers, shareholders, business partners, or other stakeholders and report suspicious activity immediately.

33. Money Laundering and Terrorist Funding.

RSA takes steps to prevent illegal use of its business activities for money laundering and terrorist financing by identifying our customers, their business activity, and the origin of their funds, and by reporting suspicious transactions. We abide by all applicable laws designed to deter criminal enterprise and protect the national security of the countries where we do business.

Money laundering is the process by which funds generated from criminal activity such as drug trafficking are moved through legitimate businesses to hide their criminal origin. Terrorist financing refers to funding for terrorist activities and can come from legitimate or criminal sources. Employees must never knowingly facilitate either money laundering or terrorist financing and must take steps to prevent inadvertent use of RSA's business activities for these purposes. Employees must be vigilant and exercise good judgment when dealing with customers or business partners. Know who they are, what kind of business they are in, and where their funds come from.

Employees should immediately report any unusual or suspicious activities or transactions such as attempted payment in cash or from an unusual financing source, arrangements that involve the transfer of funds to or from countries or entities not related to the transaction or customer, unusually complex deals that do not reflect a bona fide business purpose, or attempts to evade record-keeping or reporting requirements.

34. Travel and Expense Responsibly.

RSA funds may only be used for legitimate business purposes. Employees must follow company policies regarding expense limits, the use of corporate credit cards, preferred travel vendors, necessary management approvals, receipts, expense reports, and other travel-related matters. Employees are expected to truthfully, accurately, and completely record travel and hospitality expenses.

Reimbursement expense claims must be honest and accurate. RSA will not use RSA funds for personal travel or entertainment, or to supplement personal income. While engaged in RSA business, employees should not go to places that would negatively reflect on RSA, or that are not in alignment with our values, such as a sexually oriented business. Expenses incurred at these establishments will not be reimbursed. These venues are not acceptable for business entertainment even if expenses are not submitted for reimbursement.

35. Conflicts of Interest.

RSA requires its employees avoid any activity or personal interest that creates or appears to create a conflict between their interests and the interests of RSA or that might impair, or appear to impair, their ability to perform work objectively and effectively.

Common Areas of Conflicts of Interest

- **Personal relationships**: You should not be involved in any employment-related decisions —such as hiring, compensation, evaluation, or promotion—regarding a family member or someone with whom you have a romantic relationship.
- **Outside employment, business ventures and investments**: Secondary employment, outside business ventures, or other commercial or financial activities must not take away from your responsibilities to RSA. You must never engage in any outside employment or other activity that competes with RSA, violates your confidentiality or other obligations to RSA, or that is illegal, immoral, or would otherwise reflect negatively on RSA.
- **Contracting**: We always select vendors and business partners who will serve RSA's best interests. You must not participate in any decisions relating to current or potential business relationships between RSA and your secondary employer, personal business ventures, or entities in which you or a relative has a significant financial investment or serve in a governance position.
- **Outside board memberships and governance roles**: RSA team members are not permitted to serve on the boards of outside for-profit companies, whether publicly traded or private, with the rare exception that members of RSA's Executive Leadership Team and certain Senior Vice Presidents may request to serve on a for-profit board in strict adherence to RSA's Global Conflicts of Interest Policy and with the approval of RSA's Chief Executive Officer. Service on the board of a non-profit entity is generally permitted but must also adhere to RSA's Global Conflicts of Interest Policy.

Conflicts of Interest in Government Contracts

- **Personal conflicts of interest**: A personal conflict of interest may exist where the government expects objective judgment from you, and you have a financial interest, personal activity, or relationship that may impair your ability to act impartially and in the best interest of the government when exercising that judgment. The following interests may give rise to a personal conflict:
    - Conflicting financial interests of you or close family or household members (including business ownership interests, stock holdings, real estate investments, etc.)
    - Other employment or financial relationships (including job negotiations, consulting relationships, business referral relationships, research funding, etc.)
    - Gifts
- **Organizational conflicts of interest**: In addition to preventing personal conflicts of interest, we each must ensure that RSA does not have any actual or apparent organizational conflicts of interest in connection with RSA's performance of government contracts. An organizational conflict of interest may arise if RSA is unable or potentially unable to render impartial assistance, service, or advice to the government because the objectivity of RSA or our employees is impaired, or RSA has an unfair business advantage. These types of conflicts can arise if:
    - RSA or an RSA employee participates in the development of a statement of work for a procurement on which RSA intends to compete (and excluding circumstances in which the government seeks industry comment or participation)
    - A statement of work requires RSA or its partners to evaluate or assess work performed by RSA or its partners on a government contract.

    - RSA gains access to non-public proprietary information from its performance of a government contract that may give RSA an unfair business advantage in another procurement (and excluding traditional incumbent advantages).
- **Hiring of former government employees**: "Revolving door" laws and regulations impose restrictions on government employees and companies in the private sector regarding the solicitation for employment and hiring of former government employees. Some government employees retire with post-government employment restrictions. These should be examined carefully to ensure any position offered remains suitable. Although RSA recognizes and values the highly developed and often times unique skills held by government employees, RSA takes great care in the hiring process to ensure that the company neither violates laws nor creates conflicts of interest. To that end, you must consult with the Legal Department before responding to or initiating any contact with a current or former government employee concerning present or future employment opportunities at RSA.

If you believe that you may have a personal conflict of interest with respect to your work on a government contract, you must notify the Legal Department.

36. Gifts and Hospitality.

Gifts and hospitality must be given and received in a responsible manner and may never be used to influence a business decision.

Reasonable gifts, hospitality, and other business courtesies may be appropriate to foster goodwill but should never be used to influence a customer's business decision or undermine the integrity of our business relationships.

Accepting Gifts:

Although nominal gifts and business courtesies (but never cash or cash equivalents) are acceptable under certain limited circumstances, RSA will not solicit or accept tangible or intangible personal benefits of any kind that are given—expressly or implied—in exchange for securing RSA business or providing favorable business terms. We will not accept gifts or hospitality that are illegal, immoral, or would reflect negatively on RSA.

Giving Gifts:

Gifts may only be given as appropriate business courtesies to enhance relationships and never to inappropriately influence business decisions. When appropriate to give gifts, employees should only offer gifts and hospitality to partners, customers, or other third parties for legitimate business purposes and when the gift, hospitality, or business courtesy is reasonable in amount, in good taste, and in accordance with RSA's Global Gifts and Hospitality Policy. Gifts, hospitality, and business courtesies may never be in the form of cash or cash equivalents and may only be given to those individuals who are permitted to accept the gift under the laws and policies applicable to them.

More restrictive rules often apply when giving gifts to certain types of customers, like officials or employees of governmental or quasi-governmental entities, which can include certain healthcare, utility, or education customers. The rules relating to doing business with government entities impose strict limitations on what government officials may accept in "gifts" from contractors such as RSA. As a general matter, you must not, directly or indirectly, give, offer, or promise anything of value (for example, entertainment, meals, refreshments, gratuities, or gifts) to any government official, however innocent the purpose and regardless of whether you seek reimbursement from RSA. Applicable laws may allow the giving of some small courtesies (less than $20) in specific situations. Employees must always follow the most restrictive rules applicable and reach out to the Legal Department when in doubt.

37. Political Activity.

Team members are encouraged to be responsible citizens and participate in civic and political activities, as appropriate in your home country and community, provided your activities are lawful and respectful. Activities must be conducted on your own time and at your own expense. RSA funds or assets, including facilities, equipment or trademarks may not be used in connection with personal political activities or interests.

Team members must use care not to give the impression that RSA supports or endorses any candidate, campaign, or policy issue with which you are personally involved. Follow all laws as they relate to the ability of corporations and individuals to make political contributions or engage in lobbying or other government communications and political campaign activities.

RSA does not make corporate political contributions, even when it is legal to do so. RSA's Legal Department team coordinates RSA's activities with government officials and policy makers in compliance with applicable laws. Accordingly, you must not communicate with public officials regarding RSA-related policy matters or otherwise claim to represent RSA with policy makers except as authorized or directed by the Legal Department. Furthermore, use of federally appropriated funds to influence federal transactions such as the award of a federal contract, the making of a grant or loan, entering into any cooperative agreement, or extending, continuing, renewing, amending, or modifying any federal contract, grant, loan, or cooperative agreement, is strictly prohibited by law except under limited circumstances. If you believe that RSA is expending federally appropriated funds in support of such activities, you must immediately notify the Legal Department. Whenever you have a question about an RSA related public policy or political matter, please contact the Legal Department first.

38. Ethics Investigations.

RSA takes ethics investigations seriously. All investigations and any resulting corrective action will be conducted in compliance with applicable local law and applicable RSA policies and standards. The Legal Department is responsible for overseeing internal investigations into suspected ethics and compliance-related misconduct, under this Code and related policies and standards. Employees must not interfere in internal investigations or engage in their own fact-finding. Rather, they should promptly raise ethics and compliance questions and cooperate fully in any company-authorized internal investigation.

All investigations and any resulting corrective action will be conducted in compliance with local law, applicable RSA policies and standards, and any required workers' representative consultation requirements. Employees are expected to cooperate in internal investigations, audits, accounting reviews, or directions from RSA's lawyers in connection with lawsuits or government proceedings.

RSA takes all reasonable efforts to keep information related to an investigation confidential and the employee must keep investigation information confidential and not share such information beyond the investigation team unless specifically authorized in writing. Retaliating against any RSA team member for reporting an ethics issue or participation in an authorized company investigation is strictly prohibited and will not be tolerated. Team members, suppliers, partners, or vendors engaging in such retaliatory behavior will be subject to discipline, up to and including termination.

39. Speaking Up.

RSA encourages employees and third parties to speak up and report concerns if they have ethics concerns or suspect that someone is behaving illegally or unethically. Employees can talk to their leaders, submit an online report via email to **ethics@rsa.com**, or report anonymously (where allowed by law) to **reports@lighthouse-services.com**. Additionally, RSA does not tolerate retaliation against anyone who initiates or participates in the Ethics process, asks questions, or raises concerns in good faith. Team members and leaders are required to cooperate and be truthful in company investigations and follow the instruction of the Legal Department, Human Resources, and SRO during such investigations.

If you know of or suspect a violation of applicable laws or regulations, of this Code or any policy, or suspect unethical, illegal, or suspicious behavior, you must promptly report it. Failure to report a known violation may subject the employee to disciplinary action up to and including termination.

In some instances, the law or the terms of a government contract may require RSA to report misconduct. Employees must report suspected violations of federal criminal law involving fraud, conflict of interest, bribery, gratuity violations, or the Civil False Claims Act immediately so that RSA can comply with its legal obligations. Timely reporting permits timely review and timely conduct adjustment where required. Failure to report suspected violations may itself violate the Code.

There are many ways for you to ask questions or raise concerns:

- Your leader
- A member of management
- Human Resources
- Legal Department
- Internal Ethics inbox via e-mail to **ethics@rsa.com**
- Ethics Helpline telephone and e-mail contact information at **reports@lighthouse-services.com** to report your concern confidentially or anonymously, where the law allows

RSA does not tolerate retaliation against anyone who reports suspected misconduct or assists with an investigation or audit in good faith. If you think you are being retaliated against, or that an investigation is being conducted inappropriately, you should report it immediately using any of the reporting avenues listed above.

Ethics Helpline:

- Website: https://www.lighthouse-services.com/rsa
- E-mail: **reports@lighthouse-services.com**
- Toll-Free Telephone:
    - Direct Dial
        - English-speaking USA and Canada: 833-489-0009
        - Spanish-speaking USA and Canada: 800-216-1288
        - French-speaking Canada: 855-725-0002
        - Spanish-speaking Mexico: 01-800-681-5340
    - AT&T USA Direct
        - All other countries: 800-603-2869
        - (Must dial country access code first click here for access codes and dialing instructions)

(Note: You must include RSA's company name with report.)