SECCURACY

# CODE OF BUSINESS CONDUCT

CENTRO 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundos Europeus Estruturais e de Investimento

# A Message from Our Chief Executive Officer

At Seccuracy, we provide a platform that give our clients the control and transparency of everything. Our achievements have been driven by the way we do business, including our commitment to honest, ethical business practices. Competing on the merits of what we have to offer builds trust and reputation. A strong reputation and our dedication to earning the trust of our customers, partners, and each other leads to long-term success.

Our Code of Business Conduct summarizes some of our most important policies, sets expectations for ourselves, and outlines our responsibilities to other members of the Seccuracy community to act ethically, with integrity, and inclusively.

The Code applies to all employees, officers, directors, and contingent workers of Seccuracy and our global subsidiaries around the world. We are all responsible for upholding its principles, promptly communicating suspected violations, and asking clarifying questions. Speaking with honesty and courage is essential to creating a fulfilling work environment that rewards teamwork and respects diverse work styles, lifestyles, and cultural differences. This will enable us to continue to deliver the incredible tools our customers use to make a better and safer maritime Seccuracy industry.

RUBEN DOS REIS
CHIEF EXECUTIVE OFFICER,
STRONGHOLD SECCURACY.

# 1. We Take Ethics and Compliance Seriously

SECCURACY'S VISION IS TO HELP CREATE A STANDARD MARITIME SECURITY INDUSTRY.

Our platform contains innovative features that improve the standardization, productivity and compliance of all key maritime security stakeholders.

A large part of our success stems from our commitment to doing business honestly and ethically. This commitment involves everyone in the Seccuracy family, including employees, officers, directors, and contingent workers. A fundamental part of being a member of the Seccuracy team is respecting and following this Code and Company policies. Some of the Company policies are listed in this Code. You can find other policies and guidelines on Seccuracy's internal platform.

We expect you to know your legal obligations relating to your job and to conduct yourself with integrity in all your business interactions. Many Seccuracy policies include or reflect legal or regulatory requirements and there may be additional laws and regulations that apply to your job. You must comply with all of these laws and regulations. Violations can create significant liability for Seccuracy, could threaten our ability to do business, and may lead to termination of your relationship with Seccuracy.

If you believe there is a conflict between Portugal or local laws and this Code, please contact your Legal Business Partner for guidance.

We are counting on you to recognize potential problems and ask questions if you are ever unsure.

One way to determine whether something is appropriate is to apply the "front-page test" by imagining your actions on the front page of tomorrow's newspaper with all of the details, including your name and picture. If you are uncomfortable with the idea of this information being made public, think again about your course of action.

Whenever you are unsure about the appropriateness of an event or action, ask your manager, Finance, Human Resources, or Legal Business Partner.

## Managers as Role Models

Managers at all levels have a special responsibility as role models for ethical behaviour. Additionally, all managers must ensure that employees under their supervision understand and comply with this Code and Seccuracy's policies and practices. This includes making sure that all required training is completed. It is important that managers:

- Read and understand the Code;
- Regularly reinforce and discuss the Code with team members;
- Seek guidance from Legal Business Partners with questions about the Code;
- Ensure compliance with the Code and all applicable policies and guidelines.

# Q&A

Q- ARE THERE ANY POLICIES OR GUIDELINES THAT REQUIRE SPECIFIC MANAGEMENT COMPLIANCE?

A: Yes. Managers are required by certain policies and guidelines to conduct proactive reviews of employee activity and escalate issues as needed. Managers must evaluate and approve each entry on an employee expense report under the T&E policy, for example, to ensure that they are within standards. Managers must also investigate any disputed charges or issues.

Q: Where can I find information about other relevant policies and guidelines?

A: There are various policies and guidelines that support the Code. These policies and guidelines can be found on Seccuracy's internal website, or platform. If you ever have a question regarding whether a policy or guideline exists or is applicable, ask your manager, Finance, Human Resources, or Legal Business Partner.

# 2. We Ask Questions and Report Violations

WE ENCOURAGE YOU TO RAISE CONCERNS AND ASK QUESTIONS.

## Reporting Possible Violations

If you believe that this Code, the law, or any of our other policies are being violated, you have an obligation to report the suspected violation. Do not conduct your own investigation; instead, report the suspected violation immediately.

We make many resources available for you to ask questions or to report possible violations. You may choose the one you are most comfortable with:

- Your manager or anyone in senior management;
- Your Legal Business Partner or any attorney with Seccuracy;
- Your Human Resources Business Partner or anyone else in Human Resources management;
- Your Finance Business Partner or anyone else in Finance management;
- Audit & Advisory Services;

Where permitted by applicable law, you can contact the Hotline, by phone or online, and decline to provide your name. You can also send a letter to:
Audit & Advisory Services or the Chief Legal Officer,
Rua da Gandarada, n39
3450-133 Mortágua
Portugal

**A SPECIAL NOTE FOR EMPLOYEES LOCATED IN THE EUROPEAN ECONOMIC AREA (EEA)**

**Hotline Reporting**

EU law and regulations allow EEA employees to seek guidance or report through the Hotline ONLY if the matter falls into certain areas of concern.

To determine what areas of concern can be reported through the Hotline, see the applicable Data Protection Notice for your EEA location.

Reports made through the Hotline by EEA employees will be treated confidentially and your identity will not be revealed to any third parties, except when required by law. For more detailed information regarding Hotline procedures as they apply to EEA employees, click here.

**Other Reporting**

You may report concerns using any of the other reporting channels outlined in this section. The data related to those concerns or reports will be retained in compliance with applicable law.

## Non-Retaliation and Disciplinary Action

If you have questions or concerns of any kind, you should feel free to ask questions or make a report without fear of retaliation.

We will not tolerate retaliation (in some places, this is called "victimization") against anyone who reports a suspected violation in good faith or cooperates in an investigation. Anyone who engages in any form of retaliation will be subject to disciplinary action, which may include termination of employment. If you believe that you have been subject to retaliation as a result of reporting a suspected violation in good faith, please report it immediately to any of the available resources listed in this section.

In cases in which you report a suspected violation in good faith and are not engaged in the questionable conduct, Seccuracy will keep its discussions with you confidential to the extent reasonably possible. In the course of its investigation, Seccuracy may find it necessary to share information with others on a "need to know" basis.

# Q&A

Q: IF I MAKE A REPORT BY CALLING THE HOTLINE OR BY SUBMITTING IT THROUGH THE INTERNET, CAN I REMAIN ANONYMOUS?

A: Yes, all reports to the Hotline, either by telephone or by web, are confidential and may be made anonymously subject to regional exceptions.

Q: What if I make a report about a suspected violation and I am wrong?

A: If you made the report in good faith and believe that the information provided is accurate, you will not be subject to disciplinary action. You do not need to be right—but you do need to provide truthful information.

# 3. We Promote a Respectful Workplace

WE VALUE INTEGRITY, HONESTY, RESPECT FOR OTHERS, AND TEAMWORK

At Seccuracy, we want work to be enjoyable and meaningful for every employee. We want to give everyone an opportunity to shine.

For these reasons, we strive to create a respectful workplace where each of us is committed to maintaining an employment environment free from any form of discrimination or harassment. There are different countries, cultures, gender and religions. We therefore need to respect and recognize diverse work styles, lifestyles, and cultural differences.

You can find more information regarding Seccuracy's policies in your employee's Seccuracy portal Admin and from your Human Resources Partner.

## Equal Opportunity

We value the individuality and diversity in our workforce and are committed to making employment decisions—including hiring, promotions, and terminations—based on qualifications, skills, and merit.

## Discrimination and Harassment

We value respect for others and are committed to providing equal employment opportunity for all of our employees and applicants for employment. We will not tolerate discrimination against or harassment of employees, contingent workers, or customers based on age, gender, race, national origin, citizenship, disability, medical condition, religion, gender identity, gender expression, sexual orientation, marital status, military and veteran status, genetic information, or any other basis protected by local law ("Protected Attribute").

Discrimination means treating a worker adversely in connection with his or her work because he or she has a Protected Attribute. Harassment means engaging in conduct against the worker which is unwelcome by the worker and would be viewed as offensive, hostile, or intimidating by a reasonable worker.

If you witness, are informed of, or experience discrimination or harassment, please report it immediately to any of the available resources listed in Section 2 Reporting Possible Violations.

## Maintaining Health and Safety

Seccuracy is committed to maintaining a healthy, safe, and productive workplace. If you have any health or safety concerns you should contact the

Environmental, Health, Safety & Security (EH&S) department at EH&S@seccuracy.com, by calling +351 231 927042 or by using any of the reporting procedures mentioned in **Section 2**. Emergencies and imminent threats of harm should immediately be reported to the police or other emergency personnel. For further information, please consult the Seccuracy Environmental Health, Safety & Security pages including the Emergency Reporting & Response page. Outside of the EU, please refer to local policies and guidelines, as applicable.

## Drugs, Controlled Substances, and Alcohol

Employees are not permitted to be under the influence of drugs (including inappropriate use of lawful medications), controlled substances, or alcohol while at work.

Drugs and alcohol can impair your ability to do your job and may put other employees at risk. For further information, please consult the Drug and Alcohol Policy.

Outside of the EU, please refer to local policies and guidelines, as applicable.

## Weapons and Violence

Seccuracy does not tolerate intimidation, harassment, threatening behaviour that raises reasonable and significant concerns of bodily harm, or actions of actual or threatened violence against employees, visitors, contingent workers, or any other persons who are either on company premises or have contact with employees in the course of their duties. Firearms, explosives, or weapons of any kind are not allowed in the workplace, or while conducting workplace activities, even if you have a license to possess them or a permit to carry them in a concealed manner. Weapons are also prohibited at off-site locations where Seccuracy business is conducted or at Seccuracy-sponsored events. For further information and ways to report related concerns, please consult the Workplace Violence Prevention Policy.

# Q&A

Q: HOW CAN I RECOGNIZE IF SOMEONE'S BEHAVIOR IS ACTUALLY A FORM OF UNLAWFUL HARASSMENT?

A: Unlawful harassment can include any behaviour that creates an intimidating, hostile, or offensive work environment and is based on protected personal characteristics.

All forms of harassment are unacceptable at Seccuracy and will not be tolerated. Examples of unlawful harassment include, but are not limited to:

- Derogatory comments including gestures, slurs, epithets, or jokes, based on a legally-protected characteristic such as gender, race, religion, or sexual orientation;
- Sexual advances;
- Verbal or physical threats;
- Physical conduct including blocking or impeding another person's movement, isolating a person because of certain characteristics, leering, stalking, or touching;
- Offering employment benefits in exchange for sexual favours;
- Displaying or distributing material that is derogatory, demeaning, sexually suggestive, or offensive regarding race, gender, or any other protected characteristic.

Harassing conduct can take place in many forms. For example, sending inappropriate messages via email or text/SMS, displaying offensive screen savers, or sharing offensive material that has been downloaded from the internet can all be considered harassing conduct.

# 4. We Avoid and Disclose Conflicts of Interest

IT IS YOUR RESPONSIBILITY TO AVOID AND DISCLOSE SITUATIONS WHERE A CONFLICT OF INTEREST COULD OCCUR WITH RESPECT TO YOUR OBLIGATIONS TO SECCURACY.

A conflict of interest arises when you have an activity or interest outside of your work at Seccuracy which interferes with, may interfere with, or may be perceived as interfering with your professional judgment or responsibility to Seccuracy. A conflict can even arise from the work or activities of someone with whom you have a close personal relationship. We can help ensure that your outside interests do not become impermissible conflicts of interest for Seccuracy - but only if we know about them.

Outside interests you must disclose include:

- **A Business Relationship with Seccuracy.** Any direct business relationship you, or any person with whom you have a close personal relationship, have with Seccuracy.

- **Interests in Competitors and Business Partners.** Any interest you, or any person with whom you have a close personal relationship, have with one of our competitors, customers, resellers, distributors, suppliers or other business partners. This interest can include your performing services for, having a financial interest (for example, a significant investment, ownership, or creditor interest) in or volunteering for one of these entities.

## EXAMPLES INCLUDE...

With whom do you have a close personal relationship?

- A family member
- A spouse
- A domestic partner
- A member of your household
- An in-law
- A close friend if that friendship has the potential to influence or impact your obligations to Seccuracy.

- **Additional Employment.** You want to be an employee of another entity at the same time you are employed by Seccuracy.

- **Board Representation.** You want to be a member of an advisory board or board of directors (unless it is a non-profit organization whose primary purpose is educational, religious, or charitable and it has no plans to do business with Seccuracy). Please refer to the Corporate Policy Regarding Board Representation.

Beyond these, you should disclose to your supervising manager and Human Resources Business Partner any other outside interest that may reasonably be viewed as interfering with, potentially interfering with, or that could be perceived as interfering with your professional judgment or responsibility to Seccuracy. When in doubt, disclose your outside interest.

Examples of outside interests that you should disclose if they interfere, may interfere, or may be perceived as interfering with your work for Seccuracy include:

- Other Work. You want to work elsewhere as a consultant, contingent worker, or volunteer.
- Publication. You have contributed or want to contribute to a third-party publication outside of your work for Seccuracy.
- IT Development. You want to develop software, apps or other intellectual property outside of your work for Seccuracy.

# Remember that…

Whether a conflict of interest is apparent or actual, your personal reputation and Seccuracy's reputation can be damaged. Here are some factors to consider in determining whether a conflict may exist:

- Does the outside interest affect how I do my job?
- Could the outside interest affect the decisions I make?
- Are others likely to think that the outside interest might affect the decisions I make?
- Do I have a divided loyalty between the outside interest and my job?
- Will this outside interest divert my attention away from my work for Seccuracy?
- Would I be embarrassed if someone inside Seccuracy knew about the outside interest?
- Would a customer or supplier question whether they have been treated fairly?

If the answer to any of these questions is yes - or even maybe - it could be a conflict of interest, and you should discuss it immediately with your manager or Human Resources Business Partner.

# You Should Know…

**Certain Corporate Opportunities.** A business opportunity in which Seccuracy has or might have an interest, or which is closely related to Seccuracy's business or its anticipated plans.

**Financial Interests.** Financial interests in other companies or businesses.

If you think you might be faced with a conflict of interest, it is important to address the situation immediately. Talk to your manager or your Human Resources Business Partner and remove yourself from any decision-making responsibilities that are related to the conflict.

Some activities are never allowed while you are working for Seccuracy, including:

- Working for or serving on the Board of one of our competitors;
- Receiving gifts (and other personal benefits) because of your status as an Seccuracy employee, except as described under the Gifts and Entertainment section;
- A line of management reporting relationship with a member of your family or another person with whom you have a significant relationship. If you find yourself in one of these relationships, Human Resources can assist you in resolving any potential conflicts. See Seccuracy's policy on Employment of Family Members, Relatives, and Significant Others for additional information.

# 5. We Protect Confidential Information

SECCURACY'S CONFIDENTIAL INFORMATION AND TRADE SECRETS ARE AMONG ITS MOST VALUABLE ASSETS AND WE ALL MUST PROTECT THEM.

## Seccuracy Confidential Information

Seccuracy Confidential Information means any information that Seccuracy does not make or want to make publicly known at a given time.

Seccuracy Confidential Information may include (Without limitation):

- Computer programs, software or hardware products, product roadmaps, and development plans;
- Code, documentation, algorithms, know-how, trade secrets, formulas, processes, procedures, ideas, research, inventions, and schematics;
- Personal Data, Behavioural Data, and Unique Identifier Data, which are defined in the Data Protection Definition Set;
- Network and security information;
- Contracts or proposals, merger, acquisition, and divestiture plans;
- Internal investigation matters, litigation matters, government inquiries, and investigations;
- Other technical, business, financial and marketing information, forecasts, and strategies.

*It is your duty to abide by Seccuracy's Confidentiality Principles.*

## Confidentiality Principles

We have adopted the following Confidentiality Principles for working with Confidential Information:

- Use Confidential Information only in permitted ways;
- Identify and label types of Confidential Information accurately;
- Practice responsible collection, maintenance, and storage of Confidential Information belonging to third parties;
- Limit internal sharing only to people authorized to receive the Confidential Information;
- Make disclosures of Confidential Information outside of Seccuracy only with appropriate approvals;
- Be accountable for enforcement of these Confidentiality Principles.

You are expected to safeguard all Confidential Information to which you may have access during the course of your work. Your obligations to safeguard Confidential Information are in effect during your employment or engagement with Seccuracy and continue even after you are no longer an employee of or engaged by Seccuracy.

SECCURACY RESPECTS THE RIGHTS OF OTHER PEOPLE AND OTHER COMPANIES TO PROTECT THEIR CONFIDENTIAL INFORMATION AND TRADE SECRETS.

## Confidentiality Obligations to Third Parties

Third Party Confidential Information is information owned or controlled by a Third Party, which is entrusted to Seccuracy under an obligation of confidentiality.

Just as Seccuracy protects its own confidential materials, Seccuracy respects the rights of other people and companies to protect their confidential information and trade secrets by practicing responsible collection, maintenance, and storage of Third-Party Confidential Information, and by using it only in permitted ways, as more fully described in the Confidentiality Policy.

## Confidentiality Obligations to Previous Employers

Do not use or reveal to Seccuracy any information that might reasonably be considered the confidential or trade secret information of a former employer – including materials from your former employer – without prior written authorization from the owner of the information.

For additional guidance on these issues, please see the Confidentiality Policy.

# Q&A

Q: What are examples of confidential information?

A: The following are examples of information that may be confidential, although this list is not exhaustive:

- Personnel records and personally identifying information of employees;
- Names and lists of customers and resellers;
- Contracts or proposals related to non-public business plans;
- Product plans, roadmaps, and designs;
- Marketing strategies;
- Pricing policies;
- Proprietary software information or source code;
- Information concerning potential or future mergers, acquisitions, or divestitures;
- Financial information;
- Internal email and other communications;
- Information concerning litigation matters and government inquiries and investigations.

# 6. We Respect Privacy and Personal Information

WE ARE COMMITTED TO PROTECTING AND RESPONSIBLY USING PERSONAL INFORMATION OF EMPLOYEES, CUSTOMERS, AND OTHER THIRD PARTIES.

Privacy laws deal with personal data (also known as personal information), which generally means information that can be used to identify, contact, or locate an individual. This may include personally identifiable and, in some cases, behavioural data (information concerning an individual's activities). Like confidential information, personal data requires special care.

You are required to follow all Seccuracy policies, processes, and standards when involved in a business process or when using applications/ systems that involve the collection, use, transfer, storage, or disposal of personal data. You and the vendors you engage are required to follow all Seccuracy principles and operational guidelines regarding data analytics. This helps create an environment of trust and integrity with our customers and the business community and helps ensure that Seccuracy maintains its compliance with applicable global data protection and privacy laws.

Effective as of November 02, June 2021, Seccuracy, comply with the principles of the EU-U.S. Privacy Shield Framework (GDPR) which govern the collection, use, and disclosure of personal information.

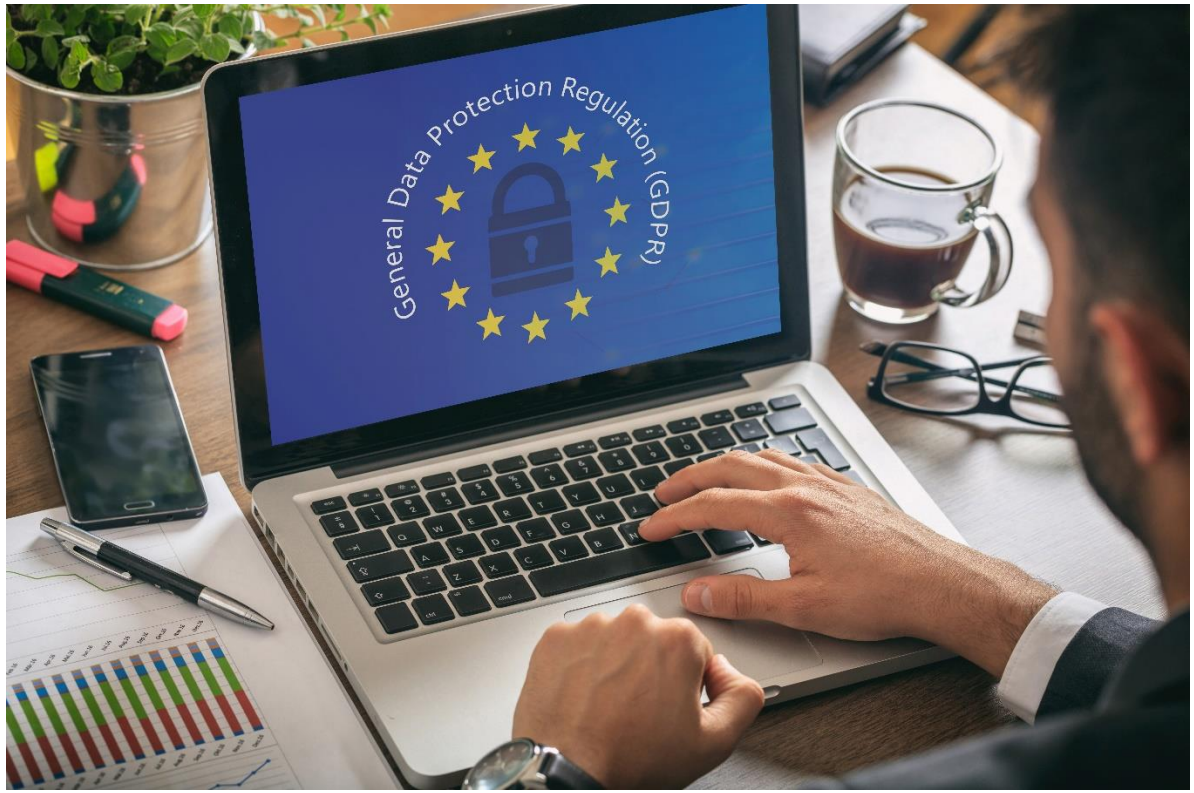
Seccuracy strives to abide by the following Privacy Principles:

- Be transparent about our actions and intent;
- Present individuals with clear and actionable choices;
- Practice purposeful collection, use, and retention of data;
- Use data only for the purposes for which it was collected;
- Only share data with third parties in limited and approved ways;
- Respect rights of access, correction, and objection where provided by local law;
- Be accountable for enforcement of these Privacy Principles.

For further information, please review the Privacy Shield Notice, Privacy Policy, Privacy Statement and Worker Data Protection Policy.

## Privacy and Your Use of Seccuracy Resources

Seccuracy respects the privacy rights and interests of its employees, contingent workers, customers, and business partners. However, as permitted by local law, information created, accessed, transmitted, or stored using Seccuracy technology resources, such as email messages, computer files, telephone messages, or websites in your browsing history, are Seccuracy resources and assets. We may access, monitor, or inspect Seccuracy resources, assets, and property at any time without notice or consent to the extent permitted by law. This can include monitoring and retrieving information that is stored or transmitted on Seccuracy's electronic devices, computer equipment, and systems. For further information, please consult the Acceptable Use Policy.



# 7. We Protect Intellectual Property

OUR DEDICATION TO INNOVATION IS WHAT MAKES US SUCCESSFUL AND SETS US APART FROM OUR COMPETITORS

## Seccuracy Intellectual Property

At Seccuracy, we are extremely committed to protecting our intellectual property, which includes our trademarks, copyrights, trade secrets, patents, software code, designs, inventions, know-how, databases, and business processes. Seccuracy's intellectual property is one of Seccuracy's most valuable assets and is vital to Seccuracy's continued success. As with Confidential Information, we expect you to protect our intellectual property. Seccuracy intellectual property may be used only for Seccuracy's business purposes and in accordance with the relevant policies or guidelines.

Maintaining the confidentiality of Seccuracy's trade secrets and other Confidential Information is an important element of protecting Seccuracy's intellectual property. Your obligations to safeguard such information continue even after you are no longer an employee of or engaged by Seccuracy.

For further information, please consult the Confidentiality Policy, Trademark Guidelines, Employee Publications Policy, and Source Code Policy.

## Intellectual Property of Others

We are dedicated to respecting the intellectual property rights of others. All software used by employees to conduct Seccuracy business must be appropriately licensed and authorized. Making or using unauthorized copies of software or devising ways to obtain unauthorized access to software services is not permitted and may expose you and Seccuracy to civil and criminal liability.

Works published in hard copy or on the internet, such as technical papers, product information, reference works, newsletters, blogs, imagery, or photographs are generally protected by copyright and their unauthorized use may constitute copyright infringement. Do not make copies of these materials or incorporate them into Seccuracy products or materials, or services without first consulting your Legal Business Partner.

Music, film or video clips, and other similar material available on the Internet are likewise generally protected by copyright and their unauthorized use may constitute copyright infringement. Do not use these materials, or any portion of them, in Seccuracy presentations or promotional materials, or at trade shows or Seccuracy events without first consulting your Legal Business Partner. In addition, using Seccuracy's systems, devices, or network to unlawfully stream or download entertainment content is prohibited and may expose you and Seccuracy to civil and criminal liability.

If you are contacted by someone who wants to sell or license any invention, patent, design, process, software, trade secret, or other intellectual property to Seccuracy, consult with your Legal Business Partner before entering into any substantive discussions.

# 8. We Communicate Appropriately with Others

SECCURACY DESIGNATES SPECIFIC EMPLOYEES TO SPEAK WITH THE MEDIA AND FINANCIAL ANALYSTS REGARDING SECCURACY MATTERS, AND COMMUNICATES IN WAYS THAT COMPLY WITH LEGAL REQUIREMENTS

## Advertising and Marketing

All businesses have a legal responsibility to ensure that advertising and marketing is truthful and not deceptive, and to comply with consumer protection and other regulations. Seccuracy is no exception. We strive to comply with all applicable policies and laws pertaining to the advertising and marketing of products and services. If you publicly endorse any Seccuracy product or service, disclose your Seccuracy affiliation and state your own independent views.

## Media Requests

Unless you are a designated employee, refer all inquiries from the media or other third parties to Corporate Communications or the Head of Public Relations and all inquiries from financial analysts to Investor Relations or the Chief Financial Officer.

You should refer any government inquiries about Seccuracy to the Chief Legal Officer or your Legal Business Partner.

## Social Media

You may not disclose confidential, private, or proprietary information about Seccuracy in any public forum such as conferences, industry events, social media sites, blogs, or any other online forum. If you have any questions about whether information is confidential, private, or proprietary, please check with your manager prior to sharing it. In addition, you are required to abide by the rules and guidelines set forth in the Social Media Policy.

## Law Enforcement / Government

If any Seccuracy documents or property are requested by a government or law enforcement officer, you must promptly notify and consult with your Legal Business Partner prior to providing any Company documents or property. In all matters, you are encouraged to notify your Legal Business Partner before speaking to government or law enforcement officials regarding Seccuracy or Seccuracy's business activities to ensure that the appropriate Seccuracy representative responds to any inquiries.

# 9. We Use Seccuracy Assets Appropriately

WE ALL HAVE A RESPONSIBILITY TO ENSURE THAT SECCURACY ASSETS ARE NOT MISUSED, MISAPPROPRIATED, SHARED WITH UNAUTHORIZED EMPLOYEES OR OTHER THIRD PARTIES, OR SOLD WITHOUT APPROPRIATE AUTHORIZATION.

Seccuracy assets may be tangible or intangible. Examples of tangible assets include computers, equipment, files, office supplies, fax machines, and photocopiers. Examples of intangible assets include software, trademarks, intellectual property rights, trade secrets, copyrights, and other Seccuracy Confidential Information. For information about protecting intangible assets, see the Confidentiality Policy.

## Computer and Other Equipment

Always care for Seccuracy resources, assets, and equipment and use them responsibly. If you use

Seccuracy equipment at your home or outside of

an Seccuracy facility, take precautions to protect it from theft or damage, just as if it were your own. If you leave Seccuracy employment for any reason, you must immediately return all Seccuracy resources, assets, and equipment in normal operating condition.

## Use of Email and Other Forms of Electronic Communication

When using Seccuracy email and communication systems (e.g., texting, tweeting, etc.) ensure that usage is appropriate for Seccuracy business purposes. Follow simple rules of etiquette and common sense when preparing, sending, and forwarding such communications. Please remember that the email system, Company communication devices (e.g., a Company-provided mobile device), and Company information sent to/ from personal devices are owned by Seccuracy, and may be subject to monitoring and inspection by Seccuracy even if protected by password, as permitted by applicable laws. For further details please consult the Information Security Policy.

Use of Third-Party Technology Services (including Cloud – SaaS, PaaS, IaaS)

When using Third Party Technology Services to support an Seccuracy business process, you must ensure that the Third-Party Service protects Seccuracy Confidential Information. For further details please consult the Third-Party Information Security Policy.

## Use of Internet

Internet use that is not strictly Company-related should be minimized at the workplace and during business hours. You may never use Seccuracy resources, assets, systems, or equipment for any illegal purpose. Seccuracy may monitor employee Internet usage/web browsing history while using Seccuracy resources, assets, systems, or equipment as permitted by local law. For further information, please consult the Information Security Policy.

# 10. We Keep Accurate Business Records

KEEPING ACCURATE BOOKS AND RECORDS AND RETAINING THEM FOR RETRIEVAL IS AN IMPORTANT PART OF OUR DAILY BUSINESS.

## Integrity of Our Books and Business Records, Financial Disclosure and Reporting

Seccuracy's policy is to provide full, fair, accurate, timely, and understandable disclosure in reports and documents that we file with public communications. We have careful disclosure and internal control processes that are designed to ensure that reported information is recorded, processed, summarized, and filed within the time periods required. In addition, we have established internal control processes to provide reasonable assurance regarding the reliability of our financial reporting and the preparation of our financial statements for external purposes in accordance with generally accepted accounting principles.

At Seccuracy, we must support Seccuracy's disclosure controls and procedures and internal controls for financial reporting. You must make sure that any financial information provided by you is accurate and that you understand and comply with Seccuracy's Finance Policies.

In addition, all members of the Finance organization must understand and comply with applicable laws and accounting and tax rules and regulations.

If you have concerns regarding accounting or auditing matters, you should report them as specified in Section 2 We Ask Questions and Report Violations. For further information, please consult the Procedures for the Submission of Complaints or Concerns Regarding Accounting or Auditing Matters.

## Managing and Retaining Business Records

Keeping business records, and retaining them for retrieval, is an important part of our daily business. In fact, various laws require that we keep certain records for minimum periods of time.

It is equally important to know when to periodically dispose of documents that are no longer useful or do not need to be retained. However, if litigation is pending or threatened, you must retain all pertinent documents in accordance with instructions received from the Legal Department.

Local laws regarding record retention and disposal may vary. Please consult the Records and Information Management Policy for more information.

# Remember that…

Common examples of business records include:

Expense reports;

- Invoices;
- Time records;
- Financial reports;
- Journal entries;
- Personnel files;
- Business plans;
- Contracts;
- Customer lists;
- Marketing information.

Depending on its content, an email may be considered a business record. If you are unsure whether something is a business record, please contact Legal.

# 11. We Employ Ethical Business Practices

WE EXPECT YOU TO ACT HONESTLY AND ETHICALLY IN ALL DEALINGS WITH CUSTOMERS, SUPPLIERS, BUSINESS PARTNERS, AND GOVERNMENT OFFICIALS

## Free and Fair Competition

Most countries have well-developed laws, rules, and regulations designed to encourage and protect free and fair competition.

We are committed to competing vigorously, always doing so in compliance with all applicable antitrust and competition laws throughout the world. While these laws and their application to particular situations can be complex, we expect you to have a basic knowledge of what may constitute a violation and to know when to contact your Legal Business Partner for guidance.

Laws regarding competition regulate Seccuracy's relationships with customers, suppliers, and channel partners. These laws cover pricing, discounts, rebates, margins, credit terms, promotions, unfair contract terms, discrimination, exclusive dealing and distribution, exclusive purchasing and supplying, restrictions on carrying competing products, terminating relationships, and many other practices.

Competition laws also govern relationships between Seccuracy and its competitors. Communications with and about competitors should be made only for legitimate business purposes and be in accordance with competition principles. You should consult with your Legal Business Partner before communicating or engaging with a competitor, attending a meeting where our competitors might be present, or joining any trade associations or other industry groups that

### REMEMBER THAT…

Fair Competition or antitrust laws prohibit agreements, understandings, and even sharing information with competitors related to competitively sensitive topics, including, but not limited to, the following:

Pricing practices including discounts and rebates, margins and costs, credit terms, promotional allowances;

Bid information, sales proposals, customer data, or other information related to the timing or scope of competition for customers and potential customers;

Non-public business plans and forecasts, R&D analyses, product development roadmaps, and other strategic plans and information.

In addition, there are also restrictions on what may properly be discussed with suppliers, channel partners, and even customers. For more details, please refer to the Seccuracy Guide to Fair Competition.

could include competitors. If a questionable situation arises during a meeting with competitors, you should immediately record your objection, leave the meeting, and contact your Legal Business Partner.

For more information, please consult the Seccuracy Guide to Fair Competition.

## Insider Trading

From time to time, you may have access to "material information" about Seccuracy's business that has not been disclosed to the public (i.e., Material Non-public Information). Material Non-public Information is non-public information that a reasonable investor would likely consider significant to a decision to buy or sell. Material Non- public Information also includes information about other companies engaged in business or contemplating a transaction with Seccuracy (e.g., customers, vendors, suppliers, or channel partners).

Seccuracy, like many public companies, has adopted specific trading restrictions to guard against insider trading, in addition to those restrictions imposed by law. Do not confuse these Seccuracy -imposed trading restrictions with the broader prohibition on trading when in possession of Material Non-public Information otherwise imposed by law.

### REMEMBER THAT

You are never permitted to pass along Material Non-public Information to any other person (including family members) who may buy or sell securities based on that information. Nor may you make recommendations or express opinions as to trading in any company's securities on the basis of Material Non-public Information. This is referred to as "tipping;" it violates the securities laws of many countries, and it subjects both parties involved to criminal prosecution.

# Q&A

Q: What are some examples of Material Non-public Information?

A: Examples of Material Non-public Information include, but are not limited to, the following types of information:

- Non-public financial results (including restatements of financial results or material impairments, write-offs, or restructurings);
- Projections of future earnings or losses;
- New products or changes in product prices;
- Significant changes in business strategy, senior management, or directors;
- News of pending or proposed strategic transactions or dispositions, including significant acquisitions;
- Major events involving Seccuracy's securities;
- New equity or debt offerings;
- Significant litigation matters and government inquiries and investigations.

For additional examples, please consult the Insider Trading Policy.

## Anti-Corruption (Anti-Bribery)

We expect you to act with the utmost honesty, integrity, and transparency in all dealings on behalf of Seccuracy, and we are committed to complying with all anti-corruption/anti-bribery laws, everywhere in the world. Seccuracy prohibits bribery and all other corrupt conduct, no matter what form it takes. In particular, you may not offer or receive bribes, kickbacks, or anything of value to or from any individual or entity, whether that individual or entity is a government official or a private party (like a customer, supplier, or other business partner) to inappropriately influence a business decision.

Our zero-tolerance policy applies equally to employees and to all others acting on Seccuracy's behalf (whether third-parties, channel partners, agents, consultants, or intermediaries). In short, our partners cannot do what Seccuracy is itself prohibited from doing. You are responsible for reviewing and being fully familiar with and abiding by Seccuracy's Anti-Corruption Policy and related Policies, including the Government Affairs Policy and the Global Travel and Entertainment Policy.

If you have any questions or concerns, contact your Legal Business Partner because the stakes are significant. Violations of these requirements can subject the company and individuals involved to lasting reputational damage and to serious criminal, civil, and other penalties.

# Remember that…

When selecting a consultant, sales representative or third party, always watch out for suspicious business practices. Warning signs may include:

- Requesting payments in a different country or to a third party;
- Requesting cash or untraceable funds;
- Failing to disclose an affiliation with a government official;
- Lack of relevant qualifications or having no prior professional experience;
- Lack of necessary staff or facilities to perform the services in question;
- Lack of adequate financial record-keeping.

A gift can be an item, but it also can include event tickets or the provision of services when the gift provider is not otherwise involved in the event or service.

Entertainment is distinguished from a gift as it typically involves meals, events, or other forms of entertainment where the provider participates in the meal, event, or other form of entertainment.

Permissible gifts and entertainment include those that:

- Are given openly and directly;
- Come with no strings attached;
- Are NOT solicited;
- Are NOT in the form of cash or a cash equivalent, such as a cash or gift card;
- Are NOT significant in value;
- Are NOT accepted as part of or during a business negotiation;
- Comply with all applicable laws and with all policies of both the giver and recipient; and
- Would NOT reflect poorly on Seccuracy.

## Gifts and Entertainment In a Business Context

Seccuracy policy and practice requires moderation and the use of good judgment when giving or accepting gifts (or anything else of value) or entertainment in business settings.

## GOVERNMENT

Transactions with government entities involve an increased risk for corruption - or the perception of corruption—so Seccuracy's Global Travel and Entertainment Policy and Government Affairs Policy impose strict limits on (and in some cases prohibit altogether) what may be offered and provided to officials of governments. It is your responsibility to be familiar with these Seccuracy policies and the special rules that apply to dealings with government officials.

## NON-GOVERNMENT (PRIVATE OR COMMERCIAL ENTITIES)

When dealing with non-government parties, extending or receiving common courtesies, such as small gifts or business meals, in connection with legitimate business activities generally is acceptable within the parameters set forth below, provided the courtesy is not intended in any way to influence a business decision or to obtain an improper advantage and does not give the appearance of impropriety

- **Gift Limits and Prohibitions -** Extending or receiving occasional gifts having a maximum retail value of $250 over the course of any one calendar year to or from the same person as a gesture of goodwill is acceptable. Gifts in the form of cash payments are not allowed, regardless of amount. Gifts in the form of tickets to sporting events and other forms of entertainment that exceed a $250 value may be acceptable under certain circumstances but require the pre-approval of your manager and the Chief Financial Officer.

- **Entertainment Limits and Prohibitions -** Extending or receiving entertainment (including meals) should be moderate and reasonable, not expensive or extravagant. Any expensive or extravagant entertainment expenses require prior written approval of your manager and the Chief Financial Officer.

# Remember that…

Anything of value may include:
Meals and entertainment; Cash;
Gifts; Travel; Favours, such as helping someone secure a job, an internship, or obtain admission to a school;
Charitable contributions.

# Q&A

Q: Who are government officials?

A: Who counts as government officials under the law and our policies is broad and includes (i) officers, employees, representatives, or agents of officers and employees of any national, regional, local, or other government entity, government-owned or government-controlled enterprises, or public international organizations; and (ii) political parties, party officials, and candidates for public office. Government officials can include administrative employees, such as clerks, secretaries, or assistants, as well as higher-level officials.
A U.S. Official under the law and our policies is a government official in the United States and broadly includes federal, state, and local elected and appointed officials, civil servants, agents, and other representatives, of any branch of U.S. government (executive, legislative, or judicial), as well as political parties and candidates for governmental office. A U.S. Official can also include officials who are associated with governmental institutions such as public hospitals, state universities, government laboratories, and the military, among other institutions.
When in doubt about whether an individual is considered a government official or a U.S. Official, consult your Legal Business Partner.

## Special Rules Relating to EU Officials

EU laws, as well as Seccuracy's Government Affairs Policy and Anti-Corruption Policy impose strict rules when dealing with EU Officials. Who counts as a "EU Official" under the law and our policies is broad and includes federal, state, and local elected and appointed officials, civil servants, agents, and other representatives and employees, of any branch of EU government (executive, legislative, or judicial), as well as political parties and candidates for governmental office. Violations of these rules can result in significant civil fines and/or criminal penalties. If you have any questions, ask your manager, your Legal Business Partner or the Government Affairs team. For more information, see Seccuracy's Government Affairs Policy.

## Political Contributions

You may not use Seccuracy's funds or assets or request or accept reimbursements from Seccuracy for contributions to state, or local candidates, political committees, or political party committees. Contributions to ballot initiatives anywhere in the world require the prior written consent of the Chief Legal Officer. For more information on political contributions, please consult Seccuracy's Government Affairs Policy.

## Working with Government Customers

When a government entity is our customer or our ultimate end customer (for example, when Seccuracy is a subcontractor), we are subject to different and stricter requirements than when we work with commercial customers. Whenever your work involves a government entity as a customer, you are responsible for knowing and complying with applicable requirements. Discuss these requirements with your manager, your Legal Business Partner, or the Government Affairs team before engaging with the government customer or bidding work for the government. A violation of these requirements can lead to serious financial and reputational harm, and can result in Seccuracy being prohibited from doing business with the government.

# Remember that…

Government officials can include:

- Police, military, customs, or immigration officers;
- Executives and other employees of a government-owned or government-controlled business, such as a national oil company, state-owned refinery, national airline, or national railway;
- Individuals who work for public international organizations, such as the United Nations, International Monetary Fund, or the World Bank;
- Employees and administrators of state-funded universities and research institutes;
- Any person acting in any official, administrative, or judicial capacity for or on behalf of any government or quasi-governmental organization like a political party;
- Lower-seniority administrative personnel, including clerks, secretaries, and assistants.

For additional examples of who may be a government official, refer to Seccuracy's Anti- Corruption Policy and Government Affairs Policy

# 12. We Promote Social Responsibility

CREATING A BETTER WORLD IS MORE THAN JUST A VISION, IT'S WHAT WE DO EVERY DAY.

## Environmental Protection

Seccuracy, like many of its customers, is committed to environmental sustainability. We work to comply with all applicable environmental laws and continually improve the environmental performance of our business operations and our partnerships with suppliers. We help our customers design a better world through our products, partnerships, and educational initiatives. For more information, see Seccuracy Environmental Policy.

## Human Rights

Seccuracy is committed to corporate responsibility and protecting and promoting human rights wherever it does business. We expect our business partners to support internationally recognized human rights and comply with all applicable laws and regulations regarding health and safety in the workplace, the eradication of human trafficking and slavery, the elimination of child labor, and responsible sourcing of minerals. In addition, we expect our partners to support fair labor practices, including the freedom to associate, and a work environment that is free from harassment and discrimination. We uphold the principles in the International Bill of Human Rights and the ILO Declaration of Fundamental Principles and Rights at Work. For more information, see Seccuracy's Human Rights Policy.

## Giving Back

Supporting the causes that Seccuracy employees care most about is central to our culture. We demonstrate that support by contributing to important causes and by matching employee contributions of both time and money through the Seccuracy Foundation. We do not contribute corporate or matching donations to support religious activities, organizations that are discriminatory, lobbying or advocacy groups, or government officials. For more information, see Seccuracy's Donation Policy and Volunteer Policy.

At Seccuracy, we are working to a better world so that all people can live well and within the limits of the planet. As part of our culture of impact, don't forget to ask yourself – does this action help to create a better world?

# 14. Waivers and Amendments

We are committed to regularly reviewing and updating our policies and procedures, including this Code. Any amendments to this Code will be posted on our Company's website.

For directors and executive officers, exceptions to this Code require written approval by the Board of Directors and require public disclosure under applicable law. For employees who are not executive officers, material exceptions to this Code require review by Seccuracy's Chief Legal Officer and approval in writing in accordance with appropriate policy.

At Seccuracy, we value your commitment to being an honest and ethical member of the Seccuracy team. Part of that commitment is to follow the guidelines within this Code as well as Seccuracy policies and the law. If you are ever unsure about what to do, ask someone. We are all responsible for asking questions and reporting any suspected or actual violations of the Code or Company policies.

Contact the following people with any Code-related questions or concerns you may have:

- Your manager or anyone in senior management;
- Your Legal Business Partner or any attorney with Seccuracy;
- Your Human Resources Business Partner or anyone else in Human Resources management;
- Your Finance Business Partner or anyone else in Finance management;
- Audit & Advisory Services;
- for international phone numbers, click here
- By web: Visit www.Seccuracy.com
- Where permitted by applicable law, you can contact the Hotline, by phone or online, and decline to provide your name. You can also send a letter to Audit & Advisory Services or the Chief Legal Officer,
  Rua da Gandarada, n39
  3450-133 Mortágua, Portugal

For concerns or complaints regarding accounting or auditing matters, you should report them as specified in the Procedures for the Submission of Complaints or Concerns Regarding Accounting or Auditing Matters located on Infosys.

**A SPECIAL NOTE FOR EMPLOYEES LOCATED IN THE EUROPEAN ECONOMIC AREA (EEA)**

## Hotline Reporting

EU law and regulations allow EEA employees to seek guidance or report a matter through the Hotline ONLY if the matter falls into certain areas of concern.

To determine what areas of concern can be reported through the Hotline, see the applicable Data Protection Notice for your EEA location.

Reports made through the Hotline by EEA employees will be treated confidentially and your identity will not be revealed to any third parties, except when required by law.

## Other Reporting

You may report concerns using any of the other reporting channels outlined in Section 2. The data related to those concerns or reports will be retained in compliance with applicable law.

For additional information, you can find a list of the Seccuracy's policies.