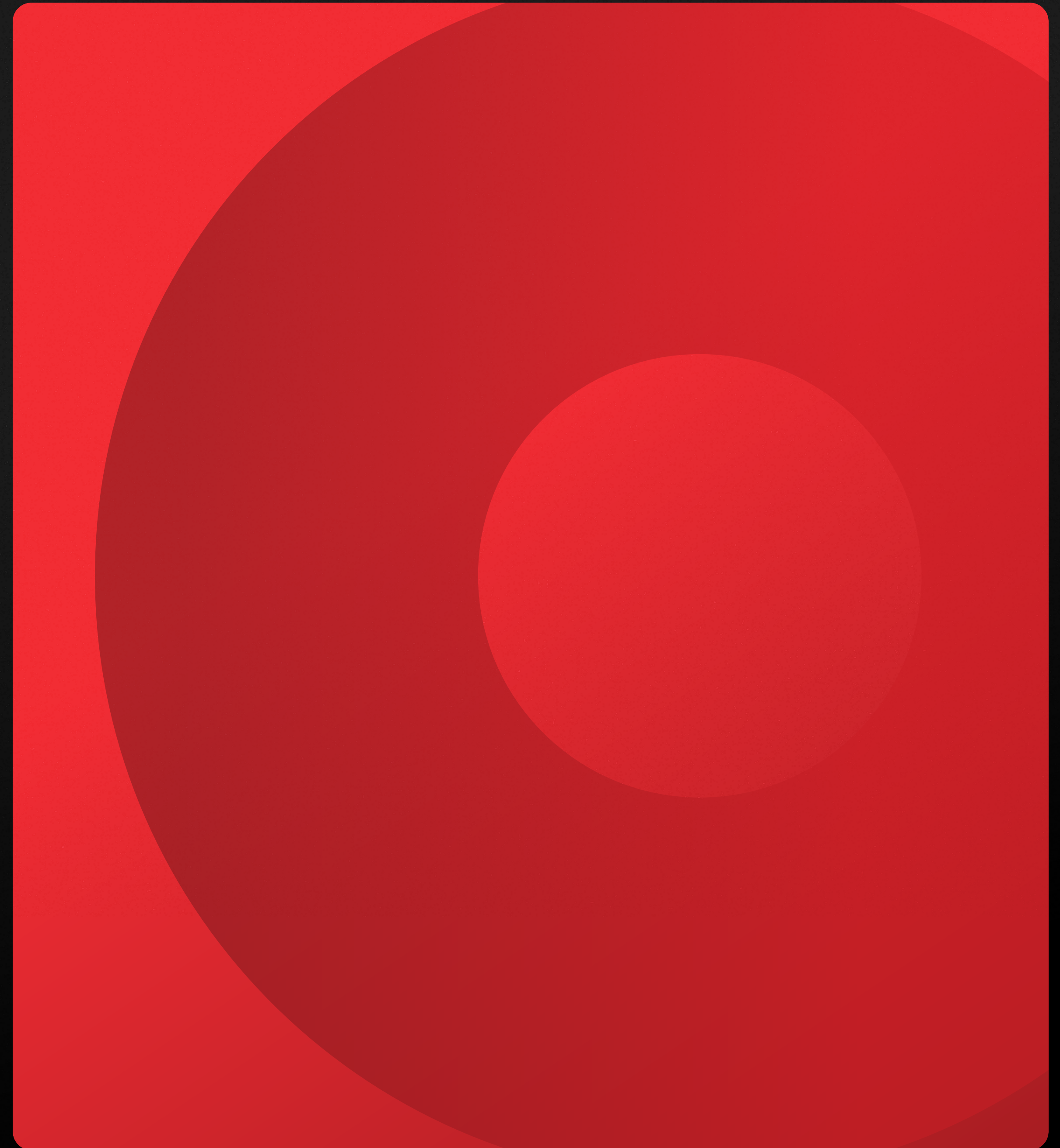


Code of Business Conduct and Ethics





A message from our CEO

At OutSystems, we believe lasting success is measured not only by what we achieve, but by how we achieve it. Our accomplishments reflect that commitment, as does the trust customers place in us to help them succeed in an AI-driven world.

Earning that trust requires more than innovation. It depends on the integrity, accountability, and respect we bring to our daily interactions with our customers, partners, and community. It requires us to innovate responsibly, stay aligned around customer outcomes, and uphold the highest standards in how we work and make decisions.

Our Code of Business Conduct and Ethics outlines the Company’s principles and sets expectations for our business conduct. It applies to everyone at OutSystems and its subsidiaries, including employees, officers, directors, and contractors worldwide. Each of us is responsible for understanding this Code, exercising good judgment, and speaking up when something does not feel right.

As technology evolves and new possibilities emerge through AI and intelligent systems, our commitment remains the same: to build trust through the way we work together and help enterprises innovate with confidence.

Woodson Martin, CEO

Purpose

Every person makes a difference. This Code of Business Conduct and Ethics sets forth the guiding principles by which OutSystems and its subsidiaries (“OutSystems” or the “Company”) conducts its business. OutSystems promotes honesty and the highest standards of integrity. Our commitment to the principles and ethical standards by which we work every day provides the foundation for strong and successful relationships with each other, our customers, investors and all who have a stake in OutSystems’ success.

Who must follow this Code?

We expect all of our employees, the members of the Board of Directors, officers, and all individuals serving as independent contractors of the Company (collectively “OutSystems Personnel” or “you”), to follow the letter and spirit of this Code.



What if I have a Code-related question or concern?

If you have a question, doubt or concern, please speak up. If you have an issue to report, do so with appropriate urgency. No matter how small the situation or concern, we do not want to let anything fester. We encourage honesty and openness so we can address our issues early and keep our Company safe and strong.

There are several avenues you can use to direct your questions:

- Your manager, or another manager you trust
- OutSystems Compliance Officer
- [OutSystems SpeakUp Helpline](#)

Good faith reporting and non-retaliation

If you have a good faith complaint or concern about a suspected or actual violation of this Code, Company policy or law, you should report it promptly. OutSystems prohibits retaliation against any employee with respect to such reports, and if you believe you are being retaliated against, please contact the People Team. Anyone who engages or attempts to engage in retaliatory action will be subject to disciplinary action up to and including termination.

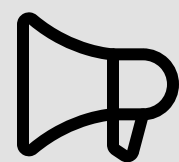
Please consult the OutSystems Whistleblower and Complaint Policy for additional guidance.



Expectations for Managers

Expectations for Managers

OutSystems Personnel in managerial positions have a special responsibility as leaders in our Company to set the right tone and model our commitment to integrity and honesty at OutSystems.
Doing the right thing as a manager includes:



Speaking up when you see a problem, never discouraging and always encouraging others to do the same.



Ensuring those who report to you understand this Code and know the laws, regulations and policies that apply to their work and areas of responsibility.



Always being receptive to questions and comments and directing issues and areas of concern with appropriate urgency to people who can help.



Our Principles

Customer Success and Serving Our Customers

Our customers come first. We achieve this by excelling in our work, building company value, and holding ourselves to the highest standards of integrity. Because we deliver exceptional products and services, our customers trust us. We protect and earn that trust every day by living the principles outlined in this Code of Conduct.



Respect in our Workplace and Supporting Each Other

Diversity and Equal Employment Opportunity

A diverse, inclusive workplace is essential. Our teams' varied perspectives drive creativity and new solutions, empowering us to challenge the status quo in a safe, supportive environment.

Our employees have the opportunity at OutSystems to reach their fullest potential and are expected to do their best to create a supportive work environment free of harassment, intimidation, bias and unlawful discrimination. We are firmly committed to equal opportunity in all aspects of employment and will not tolerate any harassment or discrimination of any kind including on the basis of race, color, religion, gender, sex, age, sexual orientation, gender identity, national origin, disability, genetic information, pregnancy status, or any other protected characteristic as established by applicable law. The types of characteristics protected by law vary across our global locations.

Safe Workplace, Harassment and Bullying

The Company strives to provide OutSystems Personnel with a safe, secure and healthy work environment. We do not tolerate violence and threatening behavior. Discrimination, harassment and bullying in any form, verbal, physical, sexual or otherwise, through any means is prohibited.

Each of you has the responsibility for maintaining a safe, secure and healthy work environment. If you have a good faith complaint or concern about a suspected or actual violation of this Code, you should report it promptly. For further guidance, consult the OutSystems Global Policy Prohibiting Workplace Discrimination, Harassment, and Bullying.



Health and Safety

Individuals are expected to follow all health and safety rules. OutSystems Personnel should report to work in a condition to perform their duties, free from the influence of illegal drugs or alcohol. The use of illegal drugs or inappropriate or excessive use of alcohol in the workplace will not be tolerated. Possession and use of weapons are not permitted in the workplace.

If you see something suspicious or unsafe, speak up and say something by reporting accidents, injuries, and unsafe equipment, practices, or conditions.

Modern Slavery and Human Trafficking

OutSystems is committed to conducting our business in a manner consistent with all applicable employment and human rights laws, rules, and regulations wherever we operate. We have a zero-tolerance policy for the use of child labor, forced or indentured labor, or for human trafficking practices. You must not knowingly do business with partners, vendors or suppliers who engage in these practices. OutSystems Personnel are expected to abide by such restrictions and are required to report any potential violations of labor or human trafficking laws of which they become aware.



Transparency, Fairness, & Integrity

Conflicts of Interest

At OutSystems, we look out for the Company’s best interests. A conflict of interest happens when your personal relationships or outside activities influence or appear to influence your ability to make objective, effective decisions in the course of your job responsibilities. You should be scrupulous in avoiding situations that present a potential or actual conflict of interest. You owe a duty to OutSystems to advance its legitimate interests when the opportunity to do so arises.

Conflicts of interest may arise if you or a family member receives an improper personal benefit because of your role in the Company. You must avoid participating in any business decision that could personally benefit you, your family, or a close connection. Conflicts aren't always obvious or easy to resolve, and it would be impossible to list every situation in which a conflict of interest may arise.

The following are examples of situations that may give rise to a potential or actual conflict of interest:

- Financial interests, especially in competitors, customers or suppliers of OutSystems
- Outside work, advisory roles, board seats, starting your own business
- Developing or helping to develop outside inventions that relate to or compete with existing or reasonably anticipated OutSystems products and services
- Taking advantage personally of business or investment opportunities that are discovered through the use of corporate property, business or information
- Working with or for family members

Sometimes conflicts of interest or the appearance of a conflict of interest will develop accidentally or unexpectedly. If you believe you may have a potential conflict of interest, discuss it with your manager right away for assistance in managing the conflict. It is your responsibility to act appropriately until the situation has been addressed. In some cases, the situation presenting a conflict of interest will require review and approval from your manager and the General Counsel.

Please note that such disclosure, which is consistent with your general obligation to act in good faith toward OutSystems, does not include personal or private information that is not strictly necessary and relevant to your ability to perform your duties to OutSystems.



Gifts and Entertainment

Exchanging gifts and entertainment (also referred to as business courtesies) can help build good working relationships with our customers and business partners. In some cases, accepting gifts, entertainment and other business courtesies can create the appearance of a conflict of interest or bias that could influence business decisions or even be seen as a bribe.

As a reminder,

- Cash gifts are prohibited.
- Decline gifts or hospitality from current or potential suppliers/vendors when involved in the selection or negotiation process.
- Gifts of nominal intrinsic value and business courtesies that are modest, infrequent and do not create the appearance of impropriety are likely appropriate.
- All payments, gifts and hospitality must be recorded accurately and completely.

Before giving or accepting any gift or courtesy, consult with the OutSystems Gifts and Entertainment Policy and follow the guidelines and procedures set forth therein. This policy should be read in conjunction with the Finance Policy and the Anti-Corruption Compliance Policy especially when business courtesies involve Government Officials. Be aware that you may need to obtain prior approval, and in all circumstances, use good judgment.



Anti-Corruption, Bribery and Kickbacks

OutSystems strictly prohibits all forms of bribery, kickbacks, and corruption. Regardless of local customs, all OutSystems Personnel must comply with global anti-corruption laws, including the U.S. Foreign Corrupt Practices Act, the U.S. Anti-Kickback Act, Portugal’s General Regime on Corruption Prevention, and the UK Bribery Act 2010.

You are prohibited from offering or giving anything of value to, or for the benefit of, any government official or commercial customer for the purpose of obtaining or retaining business, securing any improper advantage, or to request, accept or agree to receive bribes, kickbacks, or other improper payments. A kickback is the return of a sum already paid or due to be paid as part of a legal contract, serving as a reward for making or fostering business arrangements.

OutSystems does business with government entities in many countries and we must be committed to the highest standards of integrity in all public procurement and government contracting activities. If you interact with government officials or their representatives on behalf of the Company, you must be especially careful and understand the limits and rules regarding gifts, entertainment and hospitality provided to them. No funds shall be used to influence the official acts of foreign government officials, political parties, or candidates in a manner that violates relevant anti-corruption and lobbying disclosure laws, including the U.S. Foreign Corrupt Practices.

Relevant laws and regulations are very strict and can subject you and the Company to civil and criminal penalties. Familiarize yourself with the OutSystems Anti-Corruption Compliance Policy and follow all policy and guidelines therein. If you have reasonable grounds to believe a violation has occurred, you must promptly report it. If you have any questions or concerns, contact the Compliance Officer or General Counsel.



Third Parties and Government Contracts

OutSystems utilizes agents, distributors, resellers, and other third-party intermediaries (collectively, “Business Partners”). Prior to engagement, you should conduct appropriate due diligence to ensure that the prospective Business Partner does not have a history or reputation of unethical or illegal practices or could otherwise cause reputational harm to the Company.

Our commitment to integrity is stringent and this awareness and need for caution is heightened when doing business in the public sector, which is highly regulated. Government contracting laws are complex. In particular, because OutSystems operates in the U.S. Federal market, we must ensure that all company and employee political or public policy activities comply with applicable laws and avoid even the appearance of impropriety. Improper conduct can result in severe penalties, including price reductions, contract cancellation, and suspension or debarment from future government opportunities.

You are prohibited from unauthorized representation of the Company to government officials, using Company resources for lobbying or partisan political activities, and engaging in lobbying activities. All contacts and communications with elected or appointed government officials on behalf of OutSystems must be pre-approved in writing by the General Counsel to ensure they are coordinated, authorized, and compliant with legal reporting requirements.

You are responsible for ensuring that you do not engage in prohibited lobbying. If you have questions about relevant laws and how they apply to you in your dealings with the government customers or government officials, contact the Legal Team.



Competition and Fair Dealing

OutSystems is committed to vigorous, open, and fair competition which shall be based solely on the merits of our competitive offerings. Integrity in the competitive process requires adherence to all relevant antitrust and unfair competition laws as well as applicable procurement and acquisition regulations and laws.

All OutSystems Personnel must deal fairly with the Company's customers, suppliers, competitors, and other employees. No individual should engage in manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other unfair dealing practice. You must ensure that all communications and representations to prospective clients, suppliers, and partners are accurate and truthful.

Part of maintaining integrity is being mindful of the flow of information and data. OutSystems Personnel must protect confidential information. If you have access to another company's proprietary information, competitively sensitive information, or non-public customer bid, proposal or source selection information, and you do not believe you have permission to access it, you must not disclose, discuss, or use such information. If you receive another company's confidential or proprietary information by mistake, return or destroy it. If you have any doubts or concerns, promptly contact the Legal Team.

Doing business with governments and government-owned entities present special legal, regulatory and contractual requirements that apply to government contracting, including procurement integrity requirements and compliance with the US Procurement Integrity Act. You must not disclose or use any unauthorized confidential contractor bid or proposal information, e.g., proprietary information submitted by the bidding entity, or source selection information, e.g., information prepared or used by a federal agency for evaluating bids or proposals to enter into a procurement contract.

Antitrust and fair competition laws worldwide protect consumers by prohibiting anti-competitive behavior that restricts a free market. All OutSystems Personnel are expected to uphold these standards and follow the law. Because compliance can be complex, always consult the Legal Team with any questions regarding these laws and your responsibilities.



Maintain Trust and Protect our Assets

Protecting Confidential and Proprietary Information

One of our most important assets is the Company’s confidential and proprietary information. Failure to protect this information could be harmful to OutSystems’ continuing success and useful to our competitors. You must safeguard the Company’s proprietary and sensitive business information, including all confidential and proprietary knowledge, data, or information about OutSystems, its subsidiaries and affiliates. Unauthorized use or distribution of proprietary information violates this Code and other OutSystems policies. It could also be illegal and result in civil or criminal penalties.

By way of illustration, confidential and proprietary information includes, but is not limited to: business plans or strategies; product designs and concepts; financial results; prices and costs; sales and marketing plans; information regarding customers, potential customers and business partners of OutSystems, including customer lists, names, representatives and any non-public information concerning them;

employee and supplier information; computer software and programs; any data, reports, analysis, techniques, algorithms, processes, technical information, ideas, trademarks, copyrights, know-how, trade secrets, patents, patent applications or inventions and any other proprietary technology and all of OutSystems proprietary rights therein.

OutSystems Personnel must not disclose, use, lecture on, or publish any OutSystems confidential or proprietary information, unless it is required for your work at the Company. Additionally, you must obtain written approval from the Company before publishing or submitting any material (written, verbal, or otherwise) that incorporates this information. are expected to take all reasonable precautions to prevent the inadvertent or accidental disclosure of such information.

You are to take reasonable precautions to prevent accidental or inadvertent disclosures.

All OutSystems Personnel must, upon termination of employment or relationship with OutSystems, return all confidential information to OutSystems, including originals and copies, regardless of format (e.g., electronic, paper.) In some cases, the disclosure of any confidential information, even after termination of employment or other relationship, may result in civil liability to the individual.



Confidential Information of Others

OutSystems Personnel must maintain the confidentiality of information, including any Protected Health Information (“PHI”) and Personally Identifiable Information (“PII”), entrusted to them by OutSystems customers, suppliers, business partners, and prospective business partners, except when disclosure is either expressly authorized by OutSystems or otherwise required or permitted by law. It is essential that you protect this information.

Protection and Proper Use of Assets

OutSystems provides you with tools and equipment needed to do your job effectively and relies on you to be responsible with them. All OutSystems Personnel should endeavor to protect OutSystems assets and ensure their efficient use. Specifically with respect to the use of AI, OutSystems Personnel must refer to the the Company’s AI policy which governs the internal use of third-party artificial intelligence tools (e.g., GitHub Copilot, Google Gemini) and the internal development of AI tools and features.

Theft, carelessness, and waste have a direct impact on the profitability of OutSystems. You are strongly encouraged to immediately report any suspected incident of fraud or theft to your manager or to the Compliance Officer for investigation. Company equipment should not be used for non-Company business, although incidental personal use may be permitted. OutSystems Personnel must adhere to best security practices when using or interacting with Company-owned or managed resources. Consult the Company’s Security Policies for further information and guidance or contact the Security Team with any questions or concerns.



Data Privacy

Customer data, personal data and the systems that process such data must be protected and handled in accordance with all relevant laws, regulations, and all Company security and data privacy policies. The Company safeguards confidential customer data and personal data and limits access only to those people who need it to do their job. If you have any questions or concerns contact the Privacy Office.

Communications and Social Media

OutSystems Personnel are expected to use good judgment. Your communications, including online and social media posts, should be respectful and must not disclose confidential or proprietary Company or employee information. Your online conduct must adhere to our anti-harassment policies.

When acting in your professional capacity on behalf of the Company, always take steps to protect OutSystems’ reputation and follow our branding guidelines. Before speaking on behalf of the Company, communicating with the press or participating in public speaking engagements, contact your manager for guidance and approval as required.



Financial Integrity – Statements and Accounting

All OutSystems books, records, accounts, and financial statements must be maintained in reasonable detail, accurately and fairly record information, and properly reflect OutSystems’ transactions and business activities. The Company’s financial, accounting and legal teams are responsible for procedures designed to ensure proper internal and disclosure controls, and everyone must follow these procedures. These records must conform to applicable legal requirements and to the OutSystems system of internal controls. Unrecorded or “off the books” funds or assets are prohibited.

Records Management and Retention

All OutSystems Personnel are responsible for the accuracy and integrity of the Company’s documents and records. Documents and records must be retained and destroyed in accordance with the law and the OutSystems Records Management Policy.



Follow the Law

All OutSystems Personnel must understand and comply with the laws, regulations, and company policies that apply to their roles. This Code complements these requirements rather than replacing them. OutSystems Personnel are responsible for working with their managers to determine the relevant regulations governing their role and any required training. Should there be any conflict between this Code and applicable local laws, the local law shall prevail.

Anti-Money Laundering

OutSystems prohibits Personnel from engaging in any activity that facilitates money laundering or the funding of terrorist or criminal activities. Please consult the OutSystems Export Control, Trade Sanctions, and Anti-Money Laundering Compliance Policy for additional guidance.

Export Controls and Trade Sanctions

OutSystems is subject to the trade laws of the countries where it operates or conducts business, including the U.S. export control laws and trade sanctions. OutSystems Personnel must comply with all such applicable laws. When delivering products or services internationally you should keep in mind that there may be additional local legal and regulatory requirements. Please consult the OutSystems Export Control, Trade Sanctions, and Anti-Money Laundering Compliance Policy for additional guidance.

Insider Trading

Trading while in possession of material information that is not known to the public (“inside information”) is illegal. OutSystems Personnel who have access to such inside information may not use or share that information for stock trading purposes or for any other purpose except conducting our business. All non-public information about OutSystems is to be considered confidential information. To use non-public information for personal financial benefit or to "tip" others who might make an investment decision based on this information is not only unethical, it is also illegal.





**Asking
Questions,
Doing The Right
Thing**

Asking Questions, Doing The Right Thing

This Code cannot anticipate every situation you may encounter. You are expected to always use good judgment and common sense. When in doubt, ask. If you are unsure whether a decision or action aligns with our values, please discuss it with your manager. In the rare case where it may not be appropriate to discuss an issue with your manager, or where you do not feel comfortable approaching your manager with your question, reach out to the Compliance Officer or use the OutSystems SpeakUp Helpline available 24/7.



Violations

Violation of this Code and its Appendix (applicable to employees in certain specified countries and attached hereto) is grounds for sanction up to and including termination of employment or contractual relationship with just cause or for gross misconduct. Such action is in addition to any civil or criminal liability that might be imposed by any court or regulatory agency.



Related Documents

- Anti-Corruption Compliance Policy
- AI Policy
- Gifts and Entertainment Policy
- Whistleblower and Complaint Policy
- Records Management Policy
- Export Control, Trade Sanctions, and Anti-Money Laundering Compliance Policy
- Business Partner Compliance Guide
- Global Policy Prohibiting Workplace Discrimination, Harassment, and Bullying
- IMS Glossary
- Control of Documents Policy

Document History

Version	Change Description	Date
8.0	- Enhancements for more direct, plain language & updated statutory and policy references - Template and grammatical updates - Annual review	May 20, 2026
7.1	Update included change in leadership	May 20, 2025
7.0	- Update referencing Gifts and Entertainment Policy - Update adding Appendix per Portuguese General Regime for the Prevention of Corruption (“RGPC”) - Annual Review	April 3, 2025
6.0	Annual Review	March 26, 2024
5.0	Annual Review	March 10, 2023



Appendix

Framework

This appendix is an integral part of OutSystems' Code of Conduct and applies to all OutSystems – Software Em Rede S.A. employees.

Pursuant to article 7, paragraph 2, of the General Regime for the Prevention of Corruption ("RGPC") (approved by Decree–Law No. 109–E/2021 of 9 December), the Code of Conduct must specify the disciplinary sanctions that may be applied under the law in the event of non–compliance with the rules contained therein, as well as the criminal sanctions associated with acts of corruption and related offenses.

Crimes of corruption and related offenses and criminal sanctions

According to the RGPC, corruption and related offenses include the crimes of corruption, improper receipt and offer of advantage, embezzlement, economic participation in business, extortion, abuse of power, malfeasance, influence peddling, money laundering, fraud in obtaining and diverting subsidies, grants, or credit.

However, since OutSystems – Software Em Rede S.A. is a private entity, and its employees do not have the status of public officials for the purposes of the Portuguese Penal Code, only the crimes identified in the table below could lead to its liability:



Legal Type	Description/Penalties
Active Corruption Article 374 of the Penal Code	Whoever, by themselves or through another person, with their consent or ratification, gives or promises to an official, or to a third party by indication or with the knowledge of the official, a material or non-material advantage, for the practice of an act or omission in the exercise of their functions, even if the action or omission does not imply a violation of the duties of the position. Punishable by imprisonment for up to 5 years or a fine of up to 360 days (€1,800 - €180,000), for individuals. The legal entity can be sentenced to a fine of up to 600 days, between €60,000 and €6,000,000.
Active Corruption with Detriment to International Trade Article 7 of Law No. 20/2008, of April 21	Whoever, by themselves or, with their consent or ratification, through another person, gives or promises to an official, national, foreign or of an international organization, or to a holder of a political office, national or foreign, or to a third party with the knowledge of those, a material or non-material advantage, which is not due, to obtain or maintain a business, a contract or another undue advantage in international trade. Punishable by imprisonment from 1 to 8 years, for individuals. The legal entity can be sentenced to a fine of up to 960 days, between €96,000 and €9,600,000.
Passive Corruption in the Private Sector Article 8 of Law No. 20/2008, of April 21	Whoever [private sector worker], by themselves or, with their consent or ratification, through another person, solicits or accepts, for themselves or for a third party, without being due, a material or non-material advantage, or its promise, for any act or omission that constitutes a violation of their functional duties. Punishable by imprisonment for up to 8 years or a fine of up to 600 days (€3,000 - €300,000), for individuals. The legal entity can be sentenced to a fine of up to 960 days, between €96,000 and €9,600,000.
Active Corruption in the Private Sector Article 9 of Law No. 20/2008, of April 21	Whoever, by themselves or, with their consent or ratification, through another person, gives or promises to a private sector worker, or to a third party with the knowledge of that worker, a material or non-material advantage, which is not due, for the practice of an act or omission that constitutes a violation of their functional duties. Punishable by imprisonment for up to 5 years or a fine of up to 600 days (€3,000 - €300,000), for individuals. The legal entity can be sentenced to a fine of up to 600 days, between €60,000 and €6,000,000.
Undue Offering of Advantage Article 372 of the Penal Code	Whoever, by themselves or through another person, with their consent or ratification, gives or promises to an official, or to a third party by indication or knowledge of that official, a material or non-material advantage, which is not due, in the exercise of their functions or because of them. Punishable by imprisonment for up to 3 years or a fine of up to 360 days (€1,800 - €180,000), for individuals. The legal entity can be sentenced to a fine of up to 360 days, between €36,000 and €3,600,000.
Influence Peddling Article 335 of the Penal Code	Whoever, by themselves or through another person, with their consent or ratification, solicits or accepts, for themselves or for a third party, a material or non-material advantage, or its promise, to abuse their real or supposed influence with any public entity; or whoever, by themselves or through another person, with their consent or ratification, gives or promises a material or non-material advantage to the aforementioned persons. Punishable by imprisonment for up to 5 years or a fine of up to 240 days (€1,200 - €120,000) for individuals. The legal entity can be fined up to 600 days, between €60,000 and €6,000,000.



Legal Type	Description/Penalties
Money Laundering Article 368–A of the Penal Code	Whoever converts, transfers, assists, or facilitates any operation of conversion or transfer of advantages obtained, by themselves or by a third party, directly or indirectly, with the aim of concealing their illicit origin or avoiding criminal prosecution for the crime(s) committed. Punishable by imprisonment for up to 16 years in the case of individuals. The legal entity can be fined up to 1920 days, between €192,000 and €19,200,000.
Fraud in Obtaining a Subsidy or Grant Article 36 of Decree–Law No. 28/84, of January 20	Whoever obtains a subsidy or grant: a) By providing the competent authorities or entities with inaccurate or incomplete information about themselves or third parties and related to important facts for the granting of the subsidy or grant; b) By omitting information about important facts for its granting; c) By using a document justifying the right to the subsidy or grant or important facts for its granting, obtained through inaccurate or incomplete information. Punishable by imprisonment from 1 to 8 years in the case of individuals. The legal entity can be fined up to 960 days, between €96,000 and €9,600,000 or even face dissolution.
Fraud in Obtaining a Credit Article 38 of Decree–Law No. 28/84, of January 20	Whoever, when presenting a proposal for the granting, maintenance, or modification of the conditions of a credit intended for an establishment or a company: a) Provides written information that is inaccurate or incomplete to accredit it or important for the decision on the request; b) Uses documents related to the economic situation that are inaccurate or incomplete, namely balance sheets, profit and loss accounts, general descriptions of assets, or appraisals; c) Conceals the deteriorations of the economic situation that have occurred since the credit request and that are important for the decision on the request. Punishable by imprisonment for up to 5 years or a fine of up to 200 days (€1,000 – €100,000) for individuals. The legal entity can be fined up to 600 days, between €60,000 and €6,000,000, or even face dissolution.
Misappropriation of Subsidy, Grant, or Subsidized Credit Article 37 of Decree–Law No. 28/84, of January 20	Whoever uses benefits obtained as a subsidy, grant, or subsidized credit for purposes other than those legally intended or as provided in the credit line determined by the legally competent entity. Punishable by imprisonment for up to 6 years or a fine of up to 200 days (€1,000 – €100,000) for individuals. The legal entity can be fined up to 720 days, between €72,000 and €7,200,000 or even face dissolution.

The risks of exposure of OutSystems – Software Em Rede S.A. to crimes of corruption and related offenses are included in the Risk Prevention Plan for Corruption and Related Offenses.



Disciplinary sanctions

In addition to the criminal sanctions that may result from the violation of the rules set forth in the Code of Conduct, the following disciplinary sanctions may be applied, depending on the severity of the violation(s) and the employee's level of culpability:

- a) Reprimand.
- b) Recorded reprimand.
- c) Financial penalty.
- d) Loss of vacation days.
- e) Work suspension with loss of salary and seniority.
- f) Dismissal without compensation or severance pay.

For each violation of the Code of Conduct, a report will be prepared identifying the rules violated, the sanction applied, and the measures adopted or to be adopted.