PNC | Supply Chain Management

Supplier Code of Conduct

March 2025

Summary & Overview

This Supplier Code of Conduct ("Supplier Code") outlines principles that are consistent with PNC's strong commitment to ethics and integrity, as established in PNC's Code of Business Conduct and Ethics ("Code") and core Values. Together, they convey our strengths and create a solid foundation of principles such as legal and regulatory compliance, ethical business practices, human rights, and environmental, and social responsibility. The principles outlined within this Code are consistent with our company policies and aim to leverage other internationally recognized norms, including the International Labor Organization's Fundamental Conventions, the United Nations Universal Declaration of Human Rights, the United Nations Guiding Principles on Business and Human Rights, and the United Nations Global Compact.

All firms or individuals that provide products or services to PNC, either directly or through another entity ("Supplier"), are subject to the provisions of this Supplier Code. As such, all Suppliers must understand and implement its requirements, operate in accordance with its principles, and stay up to date on any changes. These same requirements apply to any vendor that a Third Party outsources work to.

In addition to the direct link provided above, a copy of the Code can be obtained from www.pnc.com under "Corporate Responsibility." If there are questions about this Supplier Code or what is expected of our Suppliers, please refer to the PNC Supplier Self Service Center.

Legal and Regulatory Compliance

PNC Suppliers must comply with all applicable laws, rules, and regulations, which may include anti-trust and fair-trade policies, anti-money laundering and anti-terrorist financing laws, anti-bribery and corruption laws, restrictions related to economic sanctions, environmental laws, and employment laws, including those that address wages, forced labor, child labor, modern slavery, trafficked labor, indentured labor, involuntary labor, forced overtime, equal pay and non-discrimination, and occupational health and safety, in the countries in which they operate.

Suppliers must also provide reasonable assistance so that PNC can meet all applicable legal and regulatory requirements where we do business. This includes cooperating with regulatory inquiries and investigations related to outsourced services. If any provision of this Supplier Code would result in a violation of statutory, regulatory, or other legal obligations, including any applicable agreement with PNC, Suppliers must follow the statute, regulation, or other legal obligation.

Human Rights, Environmental and Social Responsibility

As conveyed in our Human Rights Statement, PNC is committed to a positive, safe, and healthy workplace environment, which fosters respect and inclusiveness among team members, and expects the same of our Suppliers. As such, Suppliers should provide an inclusive and supportive working environment, free of harassment and discrimination, in which all employees are valued and empowered to succeed. PNC also encourages Suppliers to share in our commitment to providing accessible digital experiences to our customers, including through embracing accessibility guidelines and standards, such as the Web Content Accessibility Guidelines (WCAG).

Environmental Sustainability

PNC's Climate Action Strategy reflects our long-term commitment to reducing environmental impact throughout our value chain, including our internal operations. Through this commitment, PNC has committed to reducing emissions, energy, and water use in its own operations, and to procuring electricity from renewable sources. Consistent with this commitment, PNC encourages Suppliers to identify their and their subcontractors' greatest environmental impacts and to implement practices, guidelines, and policies to help mitigate these impacts, as appropriate to their business. PNC also encourages Suppliers to inform PNC about any environmentally friendly products or services that they offer and that may be appropriate for PNC.

Community Investments

PNC believes that it is important to be a meaningful part of the community. That's why working to strengthen and serve our communities is at the heart of our everyday business. PNC has a long-standing commitment to help drive impact and bolster economic opportunity for low- and moderate-income (LMI) communities. Also, as part of PNC's philanthropic commitment, PNC engages with nonprofits in the communities where we have a significant presence to enhance educational opportunities, with an emphasis on early childhood education, and to promote community growth through economic development. Finally, PNC includes small and diverse-owned businesses in our sourcing processes and encourages Suppliers to consider doing the same. PNC encourages Suppliers to regularly engage with and apply their resources to help strengthen their own communities.

Contract Workers

Each of the individual workers with whom a Supplier engages to perform tasks on behalf of PNC ("Contract Workers") is responsible for becoming familiar with and adhering to the Code, living the Ethical Standards expressed in PNC's Values, and complying with this Supplier Code. At a high level, Contract Workers must adhere to the highest standards of integrity in their respective business dealings and:

- Be familiar with and follow the Code and related ethics policies and refer to them whenever an ethical question arises;
- Never do something, even at the request of a PNC employee, or permit or ask a PNC employee, contractor, or anyone acting on behalf of PNC to do something that potentially violates the Code;
- Refrain from any form of illegal activity or unethical practices, ranging from but not limited to corruption, extortion, bribery, and discrimination.
- Promptly inform PNC if the Supplier or its employees become aware of any conduct-related issues to their work at PNC that are potentially illegal, deceptive, dishonest, unfair, abusive, unethical, or that is likely to result in harm to PNC customers or PNC's reputation; and
- Ask questions of, or raise concerns with, the appropriate individuals at PNC. The resources available to help with questions or concerns about this Supplier Code, the Code, or other business ethics and conduct issues are as follows:
    - The Contract Worker's PNC Resource Manager
    - PNC's Corporate Ethics Office at 412-768-8507
    - The PNC Business Conduct and Ethics Hotline, where individuals may remain anonymous, available at 866-785-9753 or an online reporting tool on the Ethics site of the PNC Intraweb
    - The Corporate Ethics Office Mailbox at Corporate.Ethics.Office@pnc.com

If a Contract Worker informs the Supplier, instead of PNC, of a violation or potential violation of this Supplier Code or the Code, the Supplier has the obligation to report the matter to PNC's Corporate Ethics Office via the means set forth above.

Discrimination, Bias, Harassment, Sexual Harassment, and Other Inappropriate Conduct

PNC will not tolerate discrimination, bias, harassment, intimidation, coercion, threats, actions leading to bodily harm, or other inappropriate conduct by a manager, supervisor, employee, Contract Worker, customer, client,

vendor, or visitor. It is never acceptable to treat people differently because of their race, color, religion, national origin, gender, sexual orientation, gender identity/gender expression, age, ancestry, marital status, genetic information, family medical history, disability, veteran status, or any other basis prohibited by law.

Sexual harassment is defined as any unwelcome conduct of a sexual nature that unreasonably interferes with an individual's work performance or creates an intimidating, hostile, or offensive working environment. Sexual harassment may take various forms, including but not limited to verbal (*e.g.*, sexual innuendo, sexual propositions, threats, suggestive or insulting comments, or jokes of a sexual nature); non-verbal (*e.g.*, sexually suggestive pictures or objects, graphic commentaries, obscene gestures, or sexually demeaning or pornographic pictures displayed on a workplace computer or cell phone); and physical contact (*e.g.*, unwelcome physical contact such as touching, pinching, grabbing, or hugging).

PNC will take appropriate action against those who engage in harassment or inappropriate conduct and against those who fail to timely report it. Contract Workers will be protected from any retaliation for good faith reporting or testifying about illegal harassment or inappropriate conduct while working on behalf of PNC. PNC will promptly and fairly investigate all such complaints by speaking to the parties and witnesses involved and will keep the investigation confidential, to the extent possible.

Protection from Retaliation

Retaliation occurs when a negative action is taken against PNC employees or Contract Workers, because they have made a good faith report to management or to a regulatory authority of an alleged violation of the Code, PNC policies, regulations, or law. PNC does not tolerate retaliation, in any form. Suspected retaliation must be reported to the PNC Corporate Ethics Office, using one of the methods provided above.

Being Honest

Honesty in dealing with PNC, our colleagues, and PNC's customers and shareholders is the foundation of who we are at PNC. Contract Workers are expected to be honest when performing work at or on behalf of PNC. Dishonesty, in any form, jeopardizes both the Supplier's and PNC's trustworthiness and reputation.

Specifically, PNC employees and Contract Workers must create honest and accurate business records, in accordance with applicable legal and accounting principles. Business records include any type of record that a Contract Worker creates or modifies while working on behalf of PNC. Suppliers must ensure that PNC business records are made secure and readily available to those with a need to know the information.

Avoiding Conflicts of Interest

Contract Workers must avoid any actual, potential, or perceived conflicts of interest prior to engaging in any relationship with PNC, or if they later become aware of a conflict of interest, they must promptly disclose it. Conflicts of interest can take many forms, occurring anytime a Supplier's interests oppose the interests of PNC or our clients. Some common examples for Contract Workers include multiple assignments or multiple clients at the same time while performing work on behalf of PNC, outside interests, personal investments, personal or business relationships, the exchange of gifts, political engagement, etc., any of which are contrary to PNC's interests.

Anti-Bribery and Anti-Corruption

PNC takes a zero-tolerance approach to our employees and others working on behalf of PNC engaging in or tolerating bribery or any other form of corruption. As such, we expect Suppliers to follow all anti-corruption practices that are disclosed in both the Code and PNC's Enterprise Anti-Bribery and Corruption ("ABC") Policy. Consistent with this obligation, Contract Workers, and those acting on their behalf, may not promise, authorize, recommend, give, solicit, offer, or receive anything of value, such as a gift, that could reasonably appear as intended to influence improper action or to obtain an improper advantage. What follows are a few of the categories of

conduct that are prohibited under anti-bribery laws:

- Bribing another party: Contract Workers must never offer, promise, or give another party anything of value with the intent to obtain or retain business, whether for PNC or the Supplier. This includes anyone with whom PNC conducts business, including employees, officers, or directors of a PNC vendor, a government employee or government official, a business partner or agent of PNC, or a PNC client.
- Accepting a bribe: Contract Workers may never accept money or anything of value in return for performing their business functions or to reward them for already having done so.
- Failing to prevent a bribe: Contract Workers must never use other persons, such as other contractors, to pay a bribe on PNC's behalf or to do anything that would violate PNC policy.

All Suppliers and Contract Workers must:

- Report to PNC's Corporate Ethics Office, directly to PNC Compliance, PNC Human Resources, PNC Legal, or the ABC Officer, any suspected potential or actual payment or acceptance of a bribe while assigned to perform work at or on behalf of PNC or anyone who solicits a bribe or threatens loss of business or other adverse action against PNC for failure to pay a bribe.
- Receive approval from PNC's Corporate Ethics Office before a gift or anything of value is given or an invitation is provided.
- Refer any regulatory inquiries to their PNC Resource Manager.

Evaluating Gifts and Entertainment

Gifts or entertainment provided on behalf of PNC to PNC's current or potential customers or vendors must be reasonable and customary and should never be intended to influence a business decision or be lavish or excessive. Specifically, no person may provide any form of gift or entertainment to government employees/officials in connection with their work for PNC before seeking approval from PNC's Corporate Ethics Office. If a Supplier or Contract Worker wants to provide a gift or entertainment on behalf of PNC, approval in writing must be obtained via email from PNC's Corporate Ethics Office before the gift is given or the invitation extended.

Protecting PNC Information

Supplier and their Contract Workers may have access to, and use of, confidential information about PNC and PNC's customers, shareholders, directors, employees, and suppliers, that is not publicly available. It may include, but is not limited to:

- Customer/client lists, prospect lists, and any listing of shareholders, employees, and suppliers.
- Customer account or personal financial information.
- Strategic business, marketing, project and financial information, and plans.
- Information relating to mergers and acquisitions; contracts under negotiation.
- Information about PNC's products and services, technologies, and processes
- Computer programs, system documentation, special hardware, software, and technology developments, manuals, formulas, processes, methods, machines, compositions, ideas, improvements, inventions, and other proprietary information and trade secrets.
- Reports written to or by regulatory agencies.
- Information designated as confidential, private, or privileged; security information, such as passwords, personal identification numbers (pins), and electronic keys.
- Employee payroll, benefit, health, performance, and other non-public information that is personal to the employee.
- Inside information.
- All other non-public information that might be of use to outside parties, or harmful to PNC or our customers, if disclosed.

"PNC Information" includes: 1) All data created, received, modified, or stored using PNC technology, whether for

personal or business reasons; and 2) All information of or relating to PNC business, regardless of where it is created, received, modified, or stored. All PNC Information belongs to PNC. There is no personal expectation of privacy or confidentiality in PNC Information. All PNC Information may be reviewed by PNC, our attorneys, and/or our regulators without further notice. Contract Worker use of PNC technology or electronic media and/or their creation, sending, modification, or receipt of PNC Information constitutes their consent to any interception, monitoring, retrieval, and recording of activity and communications. Use of any personal device to create, receive or store PNC information could subject that device to review by PNC, our attorneys, or regulators. For the protection of PNC Information, all Contract Workers must not allow PNC Information to leave PNC, except through authorized, official processes. All confidential data must be protected and shared only with proper authorization and a legitimate business need.

At PNC, we take our customers' data privacy and security seriously. As such, Suppliers and Contract Workers have a responsibility to protect PNC customer data, among other confidential data, in accordance with applicable laws, contract terms, and prevailing industry practices. To that end Contract Workers must:

- Only use PNC client, customer, and employee information for the reasons for which the information was gathered or for other reasons allowed by PNC.
- Never disclose PNC confidential information to anyone unless they have a legitimate business need to know.
- As a general rule, assume all information learned while working with PNC is confidential.
- Only use technology (such as laptops and other equipment) that is approved by PNC's technology team.
- Ask their PNC Resource Manager about PNC procedures on securing, retaining, and disposing of confidential information and follow them.
- Not email customer information (in any form) to an account outside of PNC, as sending customer information outside of PNC's firewall exposes the information to significant security risk from Internet hackers and thieves.
- Not allow data to leave PNC except through appropriate and authorized official processes. This prohibition includes the use of any third-party service provider, including personal email.

PNC employs various Data Loss Prevention software programs to alert managers and systems security personnel of customer information that is either printed or e-mailed outside of PNC. Further, Contract Workers are not permitted to send any PNC Confidential Information or proprietary material to a personal email account, including but not limited to internal documents and presentations, customer or client lists, and any information or materials that are not public.

Proper Use of PNC Assets

Contract Workers may have access to PNC assets, which include, but are not limited to, PNC's facilities, office supplies, files and documents, intellectual property, technology platforms, application systems, electronic media, and physical devices, to help them do the job for which they have been contracted. Contract Workers must only use PNC assets for legitimate business purposes.

For the protection of PNC Assets, all Suppliers and Contract Workers must:

- Not misuse computer systems or networks, including accessing any PNC Information, servers, or accounts, without both authorization and a legitimate business need
- Not use PNC technology or electronic media to initiate or participate in any malicious, unauthorized, or fraudulent use of company resources. Software must always be downloaded from an approved and protected channels within PNC (the Software Center).
- Comply with any policies of the PNC business unit and manager for whom they are working.
- Never use PNC technology and electronic media to initiate, download, create, save, or send items that may be perceived as hostile, harassing, offensive, threatening, or otherwise inappropriate.

- Never conduct PNC business using non-PNC email, text messaging, social media accounts, or any other applications that have not been approved by PNC (*e.g.*, WhatsApp, WeChat). Non-PNC personal devices may be used **only** to arrange meetings and calls, advise colleagues about business hours and scheduling, and for other non-core business related activities. Any questions about whether a specific use is appropriate should be directed to the Contract Worker's PNC manager.
- Never attempt to create, connect, or bridge networks or network segments, except through official mechanisms approved by Security and Network Engineering.
- Never attempt to access or utilize non-approved screen sharing applications or screen sharing websites or utilizing any technology to enable unauthorized access to (including viewing of) systems or data.
- Never attempt to utilize or access file sharing sites, such as coding forums, free file movement applications, or any other service that enables a user to bypass PNC approved applications.

Social Media – Proper Usage

PNC maintains and operates certain social media for our official use. In addition, PNC employees and Contract Workers utilize social media in their professional and personal lives to interact with family, friends, coworkers, and the general public. However, the use of social media carries with it certain responsibilities and risks when such use relates to the business or impacts the reputation of PNC.

Contract Workers must NEVER do any of the following on social media, unless specifically authorized:

- Comment on PNC's products or services.
- Disclose confidential information or discuss PNC's customers or clients.
- Use PNC trademarks, logos, or identifying marks in their personal activities.
- Post, solicit, seek, or provide PNC business-related recommendations, endorsements, or referrals to other employees, former employees, customers, suppliers, or other business contacts.
- Create personal social media profiles, accounts, or content that might create the perception that they are authorized or approved by PNC.

Likewise, under the sections of the Code related to Discrimination, Bias, Harassment, Sexual Harassment, and Other Inappropriate Conduct, social media activity that is discriminatory, harassing, offensive, threatening, or otherwise inappropriate will not be tolerated. This includes social media activity that occurs outside the PNC workplace to the extent it relates to or impacts the business or reputation of PNC.

Violation of the Code

PNC will take all necessary actions to enforce this Supplier Code. A Supplier's or Contract Worker's failure to adhere to this Code may result in the termination of any applicable agreements with the relevant Supplier or Contract Worker. Violations of this Supplier Code may also constitute violations of law, which may expose PNC, the Supplier, or the Contract Worker to criminal or civil penalties. PNC may require reimbursement for any costs associated with a violation of this Supplier Code.

This Code was reviewed and approved by the Responsible Business Strategies (RBS) Committee, a management committee that reports to the Management Executive Committee and approves voluntary corporate responsibility public disclosures, new commitments or goals, and new signatory relationships produced by or on behalf of the Corporate Responsibility Group.