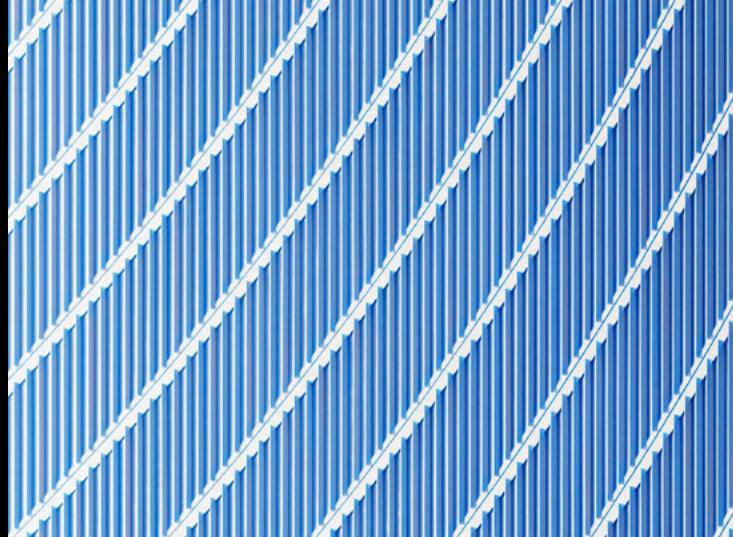


Business Conduct Guidelines

Integrity Comes First

Table of Contents



1. Integrity Means We Commit to Ethics and Compliance

- 1.1. Our Values and the Business Conduct Guidelines
- 1.2. The Importance of Integrity and Compliance
- 1.3. Speaking Up – Where and How to Report
- 1.4. Cooperation
- 1.5. No Retaliation
- 1.6. External Inquiries, Contacts and Communications
- 1.7. Speaking Publicly and Social Media

2. Integrity Means We Protect IBM Employees, IBM Assets and the Assets Belonging to Others

- 2.1. Maintaining a Safe and Productive Work Environment
- 2.2. Protecting and Using IBM Assets and Those Owned by Others
- 2.3. Sharing and Receiving Proprietary and Confidential Information
- 2.4. Avoiding Inadvertent Disclosure
- 2.5. Guarding Against Cyberthreats
- 2.6. Protecting Assets, Business Interests and Employees
- 2.7. Managing Personal Information
- 2.8. Leaving IBM

3. Integrity Means We Respect Intellectual Property Rights

- 3.1. Protecting IBM Intellectual Property
- 3.2. Using Third-Party Software, Apps, Cloud-Based Services and Data
- 3.3. Using Open Source Software
- 3.4. Developing Applications for Mobile Devices
- 3.5. Protecting Trademarks and Domain Names

4. Integrity Means We Are Honest, Accurate and Complete

- 4.1. Be Honest
- 4.2. Reporting and Recording Information
- 4.3. Understanding Financial Controls and Reporting
- 4.4. Making Commitments and Obtaining Approvals
- 4.5. Retaining Records



5. Integrity Means We Compete, Win Business and Treat Others Ethically

- 5.1. Working with Organizations Outside of IBM
- 5.2. Working with Government Entities and GOEs
- 5.3. Working with Suppliers
- 5.4. Working with IBM Business Partners, Resellers and Others
- 5.5. Dealing with Competitors
- 5.6. Competing Ethically
- 5.7. Acquiring and Using Information About Others

6. Integrity Means We Meet Our Legal Obligations

- 6.1. Protecting Against Corruption
- 6.2. Giving and Receiving Business Amenities and Gifts
- 6.3. Avoiding Money Laundering and Funding Terrorist Activities
- 6.4. Selling in the Public Sector
- 6.5. Lobbying
- 6.6. Visiting IBM Property – Government Officials and Candidates for Public Office
- 6.7. Complying with International Trade Requirements
- 6.8. Complying with Antiboycott Requirements
- 6.9. Meeting Cross-Border Travel Requirements
- 6.10. Protecting the Environment

7. Integrity Means We Separate Our Personal Interests from Our Business Responsibilities

- 7.1. Acting on Your Own Time
- 7.2. Avoiding Conflicts of Interest
- 7.3. Steering Clear of Insider Trading
- 7.4. Participating in Public Service and Political Activity

8. Notice of Certain Additional Rights; Resources

- 8.1. Other IBM Policies, Directives and Guidelines

Letter from Arvind



If we think of IBM's values as our ethical compass, then the Business Conduct Guidelines are our roadmap. They are inspired by IBMers' core value of "trust and personal responsibility in all relationships." They govern our interactions with clients, business partners, suppliers, developers, investors, teammates and communities. They support us as we strive to operate with integrity at all times.

As you review the current Business Conduct Guidelines, I ask you to take a moment to reflect on how they apply today to your individual role at IBM. Think about their relevance to the products you develop. To the regulatory environments you encounter. And to the daily interactions you have with others, both inside and outside our company.

Our commitment to the responsible stewardship of IBM's values is part of what makes us a unique and enduring company. Our longstanding reputation for ethics and integrity – built over more than a century – provides a foundation to continue IBM's essential role in business and society, today and in the years to come. We are all keepers of this important legacy. Your thorough understanding and application of our Business Conduct Guidelines is one of the most critical ways we can uphold this responsibility.

Thank you for your dedication to these principles, and for everything you do to make IBM the world's most trusted technology partner.

Arvind Krishna

Arvind Krishna,
Chairman and Chief Executive Officer

1



Integrity Means

We Commit to Ethics
and Compliance

1.1 Our Values and the Business Conduct Guidelines

IBM has long been recognized as one of the world's most ethical companies. For more than one hundred years, we've repeatedly reinvented ourselves to meet new challenges. What always has remained unchanged is our unwavering commitment to integrity.

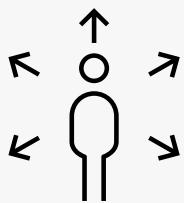
Our IBM Values serve as a solid foundation for the business choices we make. The Business Conduct Guidelines (BCGs) provide general guidance for resolving a variety of legal and ethical issues.



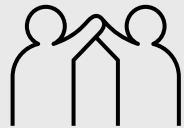
IBM's Values



Dedication to every client's success



Innovation that matters—for our company and for the world



Trust and personal responsibility in all relationships

1.2 The Importance of Integrity and Compliance

Integrity and compliance are vital to IBM's success – and yours. Our integrity, reputation and brand are in your hands, and we rely on you to protect them!

No matter where your workplace is – whether you work with IBMers, clients, Business Partners, suppliers or other parties in person, over the phone, online or by any other means – follow our Values, the BCGs and other applicable IBM corporate directives, such as IBM policies, corporate instructions and guidelines (**Corporate Directives**). And comply with all laws and regulations that apply to IBM's business.

Always use good judgment in your work. If you have questions about interpreting or applying the BCGs, Corporate Directives, or laws and regulations applicable to IBM, don't guess. Ask for help. It's your responsibility to consult your manager or IBM Counsel, or use one of the IBM Communication Channels.

Watch out!



As our business continues to transform, you may find yourself working in exciting new areas like healthcare, financial services, education or mobile application development, some of which are highly regulated. Any change in your work responsibilities may carry new responsibilities under the BCGs or new legal requirements.

If you violate the BCGs, other Corporate Directives or the law, IBM may take any action regarding your employment, including termination of employment, subject to applicable law. Failing to comply with laws could also result in fines, lawsuits, loss of business privileges and, in some cases, imprisonment.

1.3 Speaking Up – Where and How to Report

IBM expects IBMers like you to report potential wrongdoing – whether a violation of the BCGs or other unethical or unlawful conduct involving IBM. IBM will promptly review your report of actual or potential violations of the BCGs or other unlawful or unethical conduct. IBM will not tolerate threats or acts of retaliation against you for making any reports.

To report a concern (or raise an allegation), contact:

- › **IBM Employee Concerns:** for concerns or allegations relating to potential violations of the IBM Business Conduct Guidelines, including without limitation non-inclusive or inappropriate behaviors (such as bullying, harassment or discrimination) or financial recording and reporting, business process violations and inappropriate use of assets, or management decisions which personally affect you or the broader IBM population.
- › **IBM Corporate Security:** for threats or acts of violence, loss or theft of IBM assets (including trade secrets and other intellectual property), or violation of law on IBM premises.
- › **IBM Cybersecurity Incident Response Team:** for cybersecurity or data incidents, potential or actual system and data breaches and inadvertent disclosures.
- › **IBM Global Real Estate Safety:** for work-related safety issues.
- › **IBM Corporate Health:** for work-related health issues.

1. Integrity Means We Commit to Ethics and Compliance

If you are unsure how to raise a concern or allegation, the following resources and communication channels are also available:

- > [Talk It Over @ IBM](#)
- > [AskHR](#)
- > A [Compliance Officer](#)
- > [Corporate Assurance and Advisory Services](#)
- > Your Manager
- > [The Legal Department](#)

Take note!



IBM's Global Insider Trust Program

empowers employees to safeguard our organization's integrity and security. By adhering to the Business Conduct Guidelines (BCGs) and recognizing that insider threat is a shared responsibility, it is imperative that we all contribute a culture of transparency and accountability, thus ensuring the protection of our IBM equities. It is every IBMer's duty to report any activity that risks IBM data, personnel, facilities, or intellectual property, including risks from other IBMers.

Did you know?

You can raise concerns or report potential wrongdoing through the [IBM Employee Concerns page](#). Concerns may be raised online, by regular mail or by phone, are handled discreetly, and may be raised anonymously. Also, an employee is not prohibited from reporting possible violations of law or regulation to a government agency, as permitted by law.

Did you know?

Allegations that may fall under the EU Whistleblowing Directive can be raised through Employee Concerns as well as other IBM Communication Channels.



1.4 Cooperation

IBM needs your cooperation to conduct investigations and audits for IBM's internal controls and to respond to inquiries, audits or investigations by clients, regulators or others. You must fully cooperate in these matters. For example, promptly, completely and truthfully comply with all IBM requests; participate in meetings and interviews in a timely manner when requested; and provide and keep all relevant information (electronic or otherwise) as directed by IBM.

1.5 No Retaliation

IBM prohibits threats or acts of retaliation for (1) reporting in good faith potential wrongdoing or inappropriate behavior, (2) refusing to act in violation of the Business Conduct Guidelines, **Corporate Directives** or law, or (3) cooperating with an investigation. If you believe you have been retaliated against or received threats of retaliation, report it through one of the IBM Communication Channels, and IBM will take appropriate action.



1.6 External Inquiries, Contacts and Communications

IBM's business is monitored by journalists, consultants, IT and securities analysts, investors, regulators and others. These people may see you as having valuable expertise, and they may ask you to give your insights to them, with or without compensation. If contacted, do not respond to them for IBM, whether in person, online through social media, by telephone or otherwise. Instead, promptly notify the contacts below to identify both the appropriate person to respond and the appropriate response:

- › IBM Communications, if contacted by journalists or bloggers
- › IBM Analyst Relations, if contacted by consultants or IT analysts
- › IBM Investor Relations, if contacted by securities analysts or investors
- › IBM Chief Sustainability Office, if contacted by environmental groups, government agencies, business associations, or individuals about any matter involving environmental policy, declarations, principles, practices, or programs
- › IBM Government and Regulatory Affairs, if contacted about public policy or lobbying matters
- › IBM Counsel, if you receive a request for information, a legal notice or an audit request related to IBM's business from a client, attorney, investigator, law enforcement or other government official or if you are asked to testify on behalf of IBM in a legal proceeding or before an agency, legislative or other public hearing

Nothing in the BCGs prohibits you from communicating directly with any government agency or entity, without prior consent of, or notification to, IBM to the extent permitted by law and applicable rules of professional responsibility, and you are not prohibited from talking about your terms and conditions of employment.

1.7 Speaking Publicly and Social Media

When you speak out in a public forum or on social media, you must make it clear that you do so as an individual. Do not give the appearance of speaking or acting on IBM's behalf – only certain people are authorized to do so. Anything said or written in public – from the town square to social media sites – will remain accessible longer than you intended, and may be read at any time by anyone – whether a client, competitor, colleague, journalist, investor or regulator.

When using social media, follow IBM's **Social Computing Guidelines**. Follow the **IBM-Owned Social Media Guidelines** authorization process and obtain your manager's approval before submitting a request for a social handle using IBM's name, trademarks or product names.

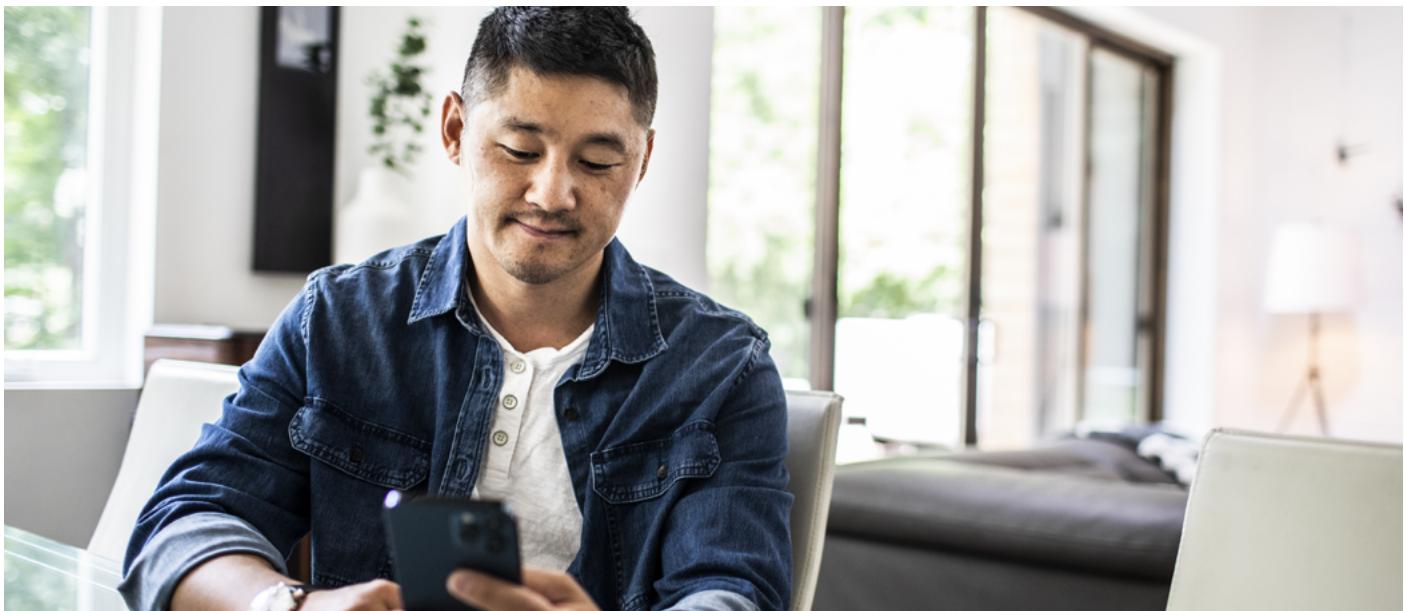
Take note!



If you, as an IBMer, wish to, or are asked to speak at an event:

- › contact your business unit's Communications support or email ibmpress@us.ibm.com before you agree or commit to the opportunity.
- › where investors or analysts will be the target audience or are likely to attend (for example, trade shows or client-sponsored events), contact Investor Relations to determine whether IBM's participation is appropriate and, if so, who should participate on IBM's behalf.

Even if you are simply attending an event (not as a speaker), be aware that you are not authorized to speak on IBM's behalf to the media or analysts/investors in attendance. Forward any inquiries you receive to IBM Media Relations or IBM Investor Relations, respectively.



2



Integrity Means

We Protect IBM Employees, IBM Assets
and Assets Belonging to Others

2.1 Maintaining a Safe and Productive Work Environment

IBM strives to maintain for its employees a healthy, safe and productive work environment free from discrimination and harassment, whether based on race, color, religion, gender, gender identity or expression, sexual orientation, pregnancy, national origin, caste, genetics, disability, age or any other factors that are unrelated to IBM's legitimate business interests, subject to applicable law. IBM will not tolerate sexual advances or comments, racial or religious slurs or jokes, or any other conduct, such as bullying, that creates or encourages an offensive or intimidating work environment. Familiarize yourself with **Corporate Policy 117**, which demonstrates our commitment to fostering a work environment where every IBMer is able to thrive because of their differences, not in spite of them. Be mindful of **Corporate Instruction HR 116**, addressing harassment and bullying in the workplace, and be respectful and considerate of others when communicating your viewpoint or otherwise using social computing tools, such as Slack channels.

Take note!



IBM is committed to the use of inclusive language. Your words matter. Avoid racial and cultural bias by following the **Inclusive IT Terminology Guidelines**.

IBM does not tolerate acts of violence in the workplace. Workplace violence may include incidents in the environment where we work and live. Refer to IBM's **Workplace Violence Program** for additional training and support.

Other prohibited conduct, because of its adverse impact on the work environment, includes the following:

- › Threats or violent behavior
- › Possession of weapons of any type
- › A manager having a romantic relationship with a subordinate
- › Discrimination against any employee on the basis of any element of diversity
- › Use, distribution, sale or possession of illegal drugs or any other controlled substance, except for approved medical purposes
- › Being under the influence of illegal drugs, controlled substances used for non-medical purposes, or alcoholic beverages in the workplace
- › Consumption of alcoholic beverages on IBM premises, unless approved in advance by your manager

If you believe you are the victim of or are concerned about a risk of prohibited workplace conduct, contact the **Talk it Over @ IBM** team or report it using one of the IBM Communication Channels.

If IBM management finds that your conduct on or off the job adversely affects others or your ability to perform your job, IBM may take any action regarding your employment, including termination of employment, subject to applicable law.

When using Slack, exercise good judgment and follow the BCGs, the Social Computing Guidelines, and guidelines for Slack usage found [here](#).

Remember



You play a critical role in identifying, eliminating and controlling health and safety risks. Take reasonable care for your health and safety and that of others.

- Maintain accurate emergency contact information, including your mobile phone number, in the **IBMer Safe Program**, so that IBM may contact you in the event of an emergency.
- Report unsafe conditions, accidents and near misses through your local process at **Global Real Estate Safety**.

You must use IBM assets, including IBM premises and facilities and physical assets and systems, only for IBM's legitimate business purposes. IBM's physical assets and systems include devices such as laptops, tablets and smartphones, information and communication systems, and connections to the Internet. Incidental personal use of physical assets and systems is permitted, however, if it is limited in duration, does not violate company policies, and does not affect your productivity or the productivity of others.

Do not use IBM assets in ways that violate the law, that are inconsistent with IBM's business interests or to visit Internet sites that feature sexual content or gambling, or that advocate intolerance of others.

Use assets belonging to others, including clients, only to the extent permitted by the other party; make sure you fully understand and follow the other party's terms and agreements as well as any laws that may restrict access to the assets based on privacy, citizenship or other requirements.

Did you know?

IBM is committed to high standards of corporate responsibility across all functions of our business and that includes respecting and protecting human rights. As a global company, IBM recognizes its role in promoting an equitable and safe future for its employees, suppliers, clients, and the communities where we operate. IBM's commitment to respecting all human rights is represented by the "IBM human rights principles" which can be found on the Reports and Policies page of the **IBM Impact site**.

2.2 Protecting and Using IBM Assets and Those Owned by Others

IBM has extensive assets of great value. They are critical to IBM's success in the marketplace, and you must protect them and cooperate with IBM's efforts to do so.

IBM's assets include, for example, physical assets and systems that IBM makes available to IBMers for work, IBM facilities and premises, IBM's proprietary and confidential information and IBM intellectual property. Our business may also require us to access and use assets belonging to others, such as their proprietary and confidential information, intellectual property, systems, data or tools.

2.3 Sharing and Receiving Proprietary and Confidential Information

IBM's proprietary information and intellectual property are IBM assets. They are the result of the hard work and innovation of many IBMers, and they give IBM a competitive advantage.

Some IBM proprietary information is confidential; often, such information is also subject to copyright, patent, trademark, trade secret or other intellectual property or legal rights. You may not share IBM confidential information with, or accept confidential information from, another party unless your manager has approved and IBM and the other party have signed a confidentiality or other suitable agreement approved by IBM Counsel.

Remember



IBM proprietary information is any information that IBM owns, including:

- Information about current and future products, services, research and development, or associated internal policies and processes
- Business plans or projections, such as potential acquisitions or divestitures, or unannounced strategies or prospects
- Earnings and other financial data
- Software in object or source code form
- Information in our online repositories and databases

Improper disclosure of IBM proprietary or confidential information could threaten IBM's competitive advantage or create security issues. Follow all IBM safeguards for protecting that information and share it only as authorized by IBM.

2.4 Avoiding Inadvertent Disclosure

Be careful to avoid inadvertent disclosure of proprietary and confidential information, whether owned by IBM or others. Do not discuss this information with, or in earshot of, any unauthorized person, including family members or friends. They might – innocently or otherwise – pass the information on to someone else.

Take note!



Audio and visual recordings could result in inappropriate disclosure of proprietary or confidential information, violate applicable law and/or infringe the privacy of others. Subject to local applicable laws, you may not, unless expressly authorized by law, make audio or visual recordings of IBM confidential or proprietary information, business discussions or any other type in the working environment, unless you have a legitimate business need to make the recording and it is previously approved by management, unless you can use the video conferencing recording functionality according to video conferencing recording rules [here](#). Never record any conversations (live, telephone, video conferencing or otherwise) secretly or without notice to all participants.

What should I do if I receive unsolicited proprietary or confidential information?



Proceed with caution to prevent any accusation that IBM misappropriated or misused the information. If you have a question about what to do if you receive an unsolicited email that includes proprietary information, contact IBM Counsel and be sure not to forward the email.

2.6 Protecting Assets, Business Interests and Employees

We rely on you to protect IBM's and others' assets.

IBM does not consider your use of IBM assets to be private. Therefore, you should not keep any personal items, messages or information that you consider private anywhere in IBM assets.

To protect IBM employees, IBM assets and IBM business interests and subject to applicable laws, IBM reserves the right at any time to:

- Inspect your use of IBM assets and personally owned electronic devices (BYO devices), such as smartphones and portable storage media used to conduct IBM business or store IBM assets, your office or workspace and your personal property, such as briefcases and bags, located on or being removed from an IBM location

2.5 Guarding Against Cyberthreats

Third parties, like our clients, trust IBM with their data and other assets, and we rely on you to protect them – as well as IBM's own data and assets.

Violating IBM's information security policies puts IBM assets, and assets belonging to others, like client data, at risk. Even well-intentioned actions, such as creating workarounds and shortcuts to improve service delivery or downloading unapproved third-party software, can violate IBM and client security policies and result in IT or data security breaches.

If you are aware of or suspect an IT or data security issue or incident, or any loss of assets, including data, belonging to IBM or others, report it to the

Cybersecurity Incident Response Team (CSIRT)
immediately.



- › Inspect, monitor, intercept and recover through technical or other means and review any employee communications (including any and all telephone conversations or transmissions, e-mails, texts, Slack messages and other instant messages on collaboration platforms or internet access or usage), records, files and other items in any electronic device or system, including but not limited to, computers, telephones and other systems, whether IBM assets or BYO devices, at any and all times and by any lawful means for any purpose
- › Terminate your use of, or access to, IBM assets at any time, including access through BYO devices

You are expected to cooperate with such inspections and IBM actions. IBM may share information and data with others, including its outside counsel, other advisors or law enforcement, subject to applicable law. Do not access another employee's workspace, including e-mail and electronic files, without prior approval from your manager or the employee.

For additional information on access to IBM assets and employee personal property, refer to **Access to Property and Information**.



Take note!



To protect IBM assets, including data and proprietary and confidential information, and assets belonging to others, take the following precautions:

- › Follow **IBM's information security policies**, controls and processes.
- › Never share passwords.
- › Register all devices used for IBM business purposes, such as laptops, mobile phones, servers and personally owned electronic devices, such as smartphones and portable storage media, as required by **IBM policy**.
- › Follow the special legal or other requirements that apply to certain types of data, like health information.
- › Participate in scheduled IBM cybersecurity training.
- › Except as may be provided in another IBM policy, do not use any personal accounts (email, Instant messaging, social media, cloud storage, videotelephony, etc.) to conduct IBM business.
- › Maintain accurate and up-to-date employee and contractor records to help ensure access credentials are appropriate.
- › Remove a supplier's access to IBM data or delete the data yourself (or direct the supplier to delete it), as soon as the supplier's need to access the IBM data ends.

2.7 Managing Personal Information

IBM takes your privacy seriously. Not all countries have data protection laws, but IBM has **Privacy and Data Protection** policies intended to protect personal information wherever we use, process or store it. Always comply with applicable privacy laws and IBM privacy policies.

IBM's business processes, management and systems cross country borders. To run its business and manage the employment of its personnel, subject to applicable data protection laws:

- › IBM and IBM-authorized companies and individuals collect and use personal information about employees, such as compensation, skills, use of IBM assets, and medical and benefit information.
- › IBM may share this information with those who have a need to know, such as health insurers.
- › IBM and IBM-authorized companies may transfer personal information about you, as an IBM employee, to IBM-authorized companies or individuals in any country where we do business.

If, as part of your work, you have access to personal information of others, you may use such personal information only to the extent necessary to do your job and according to instructions issued by management and other Corporate Directives that apply. When compiling personal information, make it anonymous, when possible, to minimize risk.

- › Some personal information, such as health or financial information, is particularly sensitive and is subject to more stringent regulatory requirements, with which you must comply.
- › Do not disclose personal information to anyone who does not have a legitimate need to know such information, within or outside of IBM, either during or after your employment.

If you are aware of or suspect that personal information has been misused, lost, stolen or accessed inappropriately, report it to the **Cybersecurity Incident Response Team (CSIRT)** immediately.

2.8 Leaving IBM

IBM assets and materials belong to IBM and you may not use them for personal purposes or in any subsequent employment you may have. Assets and materials include software, hardware, data and any other information or material (such as employee data, financial information, marketing data, code, project files and product or program designs) you develop or work on during the course of your employment.

If you leave IBM for any reason, including retirement, you must return all IBM assets and materials to IBM, including IBM assets and materials that are on BYO devices. Upon your departure, you may not remove any IBM assets or materials from IBM, either physically or through any digital means. Do not, for example, transfer IBM assets or materials from any IBM repositories to a personal device or personal online storage.

Never disclose or use IBM assets or materials for any purpose that violates the BCGs or otherwise in support of any subsequent employer. IBM continues to own intellectual property that you create as an IBM employee even after you leave IBM.

3



Integrity Means

We Respect Intellectual
Property Rights

3.1 Protecting IBM Intellectual Property

IBMer have access to, and may develop, IBM intellectual property. Intellectual property includes such things as inventions, software, publications, know-how and other related materials. We value our intellectual property; it helps provide protection, credibility and value to our development and innovation efforts for both open source project contributions and proprietary solutions.

As an IBMer, you assumed specific obligations relating to intellectual property by virtue of applicable law and the employee agreement between you and IBM. This includes assigning to IBM rights in intellectual property relating to IBM's current or anticipated business activities you develop while an IBM employee, unless otherwise approved by management in accordance with our **On Your Own Time – Guidelines for Developing IP**. Talk with IBM Counsel before you file for a patent or other intellectual property rights.



May I participate in external standards development organizations?



Engaging in external standards activities like the World Wide Web Consortium or the International Organization for Standardization – either on new projects with organizations IBM is already involved in or with new organizations altogether – could result in antitrust risk or loss of intellectual property rights. Follow **the Standards Activity Review (SAR) Process** before participating in standards activities.

3.2 Using Third-Party Software, Apps, Cloud-based Services and Data

To protect our employees and our business, IBM restricts IBMers' use of third-party software products (including apps), open source software, cloud-based services, **generative AI tools**, and data (together, third-party products).

Some third-party products (including those available for "free" or at no charge such as open source software, external online language translation apps or tools) may not meet IBM security requirements or may contain malware that could threaten IBM's network. They may have licenses and terms IBM cannot comply with, which can expose IBM to audits, license fees and other intellectual property claims by others.

Whether you are using an IBM-provided device (laptop, tablet or smartphone) or a BYO device, make sure you use third-party products for IBM business purposes only if IBM

What is the right way to acquire a third-party product to use for IBM business purposes?



You can:

- Purchase it through Procurement, using established Procurement procedures; or
- Obtain it from an approved IBM source on w3 or through an external app store, as directed by IBM.

has approved their use and IBM has been granted a license to use them in the ways you intend. If you're using open source software, follow IBM's **Open Source Participation Guidelines** as well. Some third-party products may be approved for certain uses, but not for others. Make sure you understand any applicable restrictions.

Watch out!



The default settings on some third-party products are set at "public" – which means that anything you do or post can be visible to others on the internet. This could result in the loss of proprietary or confidential information belonging to IBM or others. Make sure you follow IBM security guidelines and use the proper security and privacy settings.

3.3 Using Open Source Software

IBM has a strong history of contributing to and consuming open source projects. There are many benefits to IBM and our clients gained from engaging in open source, but it must be done responsibly according to IBM guidelines to maximize value and manage both cybersecurity and intellectual property risks. All IBMers who are consuming or contributing to open source software, such as software developers, offering managers, program managers, researchers and others, must follow IBM's **Open Source Participation Guidelines**.



3.4 Developing Applications for Mobile Devices

Follow the [IBM Mobile Development Guidelines](#) if you create IBM applications for mobile devices. The rules for distributing applications on certain devices are strict. Make sure you know what is allowed. Obtain prior approval from your manager before using development kits or other tools that have not been approved.

Did you know?

Content, images or other files may be easy to download from the Internet and may be free, but beware – they are likely still subject to license restrictions. Make sure you fully understand and follow the terms and conditions associated with any downloaded content, images or other files.

3.5 Protecting Trademarks and Domain Names

Trademarks are words, names, symbols or designs used to identify and distinguish a company and its products or services, and they are valuable assets. Use IBM's and other companies' trademarks properly and acknowledge the trademarks of others, when appropriate. For guidance, refer to [IBM's Copyright and Trademark Information](#).

Do not develop or use a word, name, symbol or design as a trademark without first going through the [Naming Tool Process](#). In addition, you may not, directly or through another party, register domain names on IBM's behalf or create websites for IBM that will be available on the Internet (outside of IBM.com) without approval from the [Corporate Webmaster](#).

4



Integrity Means

We Are Honest, Accurate and Complete

4.1 Be Honest

The rules are simple: never make misleading or dishonest statements to anyone, and never engage in activities that could be considered unethical, fraudulent or otherwise unlawful.

4.2 Reporting and Recording Information

As IBMers, we regularly provide to IBM and others information and data, such as requests for reimbursement of business expenses, hours worked on client projects, or certifications.

We rely on IBMers like you to record and report accurate, complete and honest information.

Under various laws, IBM is required to maintain accurate books and records. Misrepresentation can lead to civil and criminal penalties for both you and IBM, and the loss of business privileges, such as the right to bid on business, export or import products or even remain in business.

Remember



Both making false statements and omitting important facts are wrong.

Record and report only accurate, complete and honest information. Never report information in a way that is intended to mislead or misinform those who receive it.

If you are unsure about the accuracy or completeness of any information, don't guess. Ask for help.

If you believe any information you've recorded or reported to IBM or others is incorrect or has been misunderstood or if you're reviewing information submitted by others that appears to be incorrect, promptly notify your manager and IBM Counsel to determine the appropriate next steps.

Watch out!



Some examples of dishonest or fraudulent reporting include:

- › Submitting false or inaccurate expense reimbursement requests
- › Inaccurately recording the number of hours worked or failing to report time (or overtime in accordance with IBM guidelines) worked, whether or not charged to a client
- › Submitting inaccurate information to IBM's tools or processes
- › Providing inaccurate or incomplete information to IBM or other parties, including during investigations, audits or other reviews
- › Making false or misleading statements in (or omitting material information from) external reports or other documents submitted to government agencies

Did you know?

Always be accurate and honest when labor claiming – whether reporting hours to be billed to a client or to measure against internal goals. Never over or under report. Report accurately. If you don't understand the proper way to claim your time, ask your manager or visit **AskHR**.

Watch out!



Do not make verbal arrangements or commitments, or enter into unapproved written commitments or side deals.

Violating accounting and financial reporting laws can result in significant fines, penalties and imprisonment.

The rules for accounting and financial reporting require the proper recording of, and accounting for, revenues, costs, expenses, assets, liabilities and cash flows. If you have responsibility or involvement in these areas, you must understand and follow these rules. These rules also prohibit you from assisting others to record or report any information inaccurately, make false or misleading financial reports or evade tax. Never provide advice to others, including clients, suppliers or IBM business partners, about how they should record or report their own revenues, costs, expenses, assets and liabilities.

If you are aware of or suspect any improper or unethical accounting or financial reporting, immediately inform IBM Accounting, Corporate Assurance and Advisory Services or IBM Counsel, or report it through one of IBM's other Communication Channels.

Take note!



IBM must recognize revenue accurately. Be sure to discuss with IBM Accounting, your manager or CFO team all factors that could impact revenue recognition, such as deviations from standard IBM payment terms, non-standard warranties, contingencies in deals or deviations from customary ordering procedures.

4.4 Making Commitments and Obtaining Approvals

IBM has established approval processes and delegation levels to help us protect our assets, maintain appropriate controls and run our business effectively.



Understand and follow the approval processes and delegation levels that apply to your role. Do not make business commitments, including modifications to pricing, contract or service terms, without appropriate approvals or contrary to delegation limits. All commitments must be reported to IBM Accounting to ensure the accuracy of IBM's books and records.

4.5 Retaining Records

Our records are valuable assets. Always follow the **IBM Worldwide Records Management Plan** and document retention orders issued by IBM Counsel for retaining and disposing of IBM records. The Plan applies to information in any media, including hard copy and electronic records, e-mail, wikis, blogs, apps and records in collaboration tools (whether on the IBM network or one operated by others).

Take note!



IBM's internal processes and controls are implemented to help ensure we do business the right way. Make sure you understand which IBM processes and controls apply to what you do. If you're unsure, ask! If you think a process or control is unclear or could be improved, talk about it with your manager, the process owner, or the Compliance and Investigations Team.

Don't bypass a process or control without an authorized exception, and if you see others bypassing, say something. If a client or other third party asks you to bypass IBM's (or their own) controls, or assist them in doing so, notify your manager.

5



Integrity Means

We Compete, Win Business and
Treat Others Ethically

5.1 Working with Organizations Outside of IBM

Whether you are selling, buying or representing IBM in any other capacity, you must be ethical and lawful in your business dealings. Your actions can directly affect IBM's competitiveness, reputation and compliance with applicable laws.

IBM regularly works with other organizations – subcontractors, suppliers, consultants, agents, IBM Business Partners and competitors – and frequently has multiple relationships with these companies. You must understand these relationships and act in accordance with our guidelines.

Working with other parties can present risks – IBM can be held liable for the misconduct of others, such as agents, consultants or IBM Business Partners. For example, if we know or have reason to believe a Business Partner will offer or accept a bribe or kickback, IBM may be held accountable, even if IBM does not authorize or condone it. We require other parties with whom we interact to comply with many IBM guidelines and meet our high standards of integrity in their work for us. If you are aware of or suspect another party is acting unethically or illegally, immediately report your concern to IBM Counsel or through one of IBM's Communication Channels.

5.2 Working with Government Entities and other GOEs

IBM engages with government-owned or -controlled entities (which we refer to as GOEs) in many ways – for example, as IBM clients, suppliers, consultants or IBM Business Partners. GOEs include both government entities and state-owned enterprises.

Government entities are government agencies, departments, branches, instrumentalities and public enterprises, whether regional, national, or local, as well as:

- › Government-owned or -controlled schools, hospitals, utilities and other organizations that provide public services;
- › Public international organizations, such as the United Nations or World Health Organization; and
- › Entities that procure under public procurement laws and regulations.

State-owned enterprises can be any other type of entity, even those that are privately held or publicly traded, that are owned, controlled, organized, or sponsored by a GOE or a government official. A government official is an officer or employee of a GOE as well as any private individuals or entities acting in an official capacity on behalf of one.

Dealing with GOEs, their representatives and government officials or their family members raises unique business and compliance issues, and you must follow IBM's established processes and controls to

Did you know?

Ownership alone does not determine the status of an entity. Ask yourself:

- › Are the employees of the entity public officers or civil servants?
- › Does a government entity or GOE "control" the entity, for example, through the ability to appoint directors or senior management or through regulations?
- › Are its activities financed by a government entity?

If the answer to any of these questions is yes, it is likely that the entity is a GOE.

address them. Before you engage in any business activity, including marketing or sales activities, it is your responsibility to determine if the party you are dealing with is a GOE or a government official (or a family member of one). If you are uncertain, don't guess.

5.3 Working with Suppliers

IBM works with many suppliers worldwide, purchasing both for its internal use and in support of client engagements. In general, all purchases from suppliers must be negotiated, signed, and managed by IBM Global Procurement, unless a delegation is in place.

In deciding among competing suppliers, whether you are a procurement professional or a business person involved in a purchasing decision, we weigh the facts impartially to determine the best supplier, regardless of whether it is a large or small purchase.

You must not exert or attempt to exert influence to obtain special treatment for a particular supplier. Even appearing to do so can undermine the integrity of our established procedures. Similarly, avoid conflicts of interest in a procurement transaction by following the principles in Section 7.2.

As a general principle, IBM does not buy or sell on a reciprocity basis. To maintain the high standards of our products, we should base our purchasing decisions on quality, price and supplier reliability. Also, reciprocity may be unlawful in some situations.

Of course, IBM clients can also be suppliers to IBM, and it can be appropriate for IBM to consider its other relationships with a supplier in some cases. For example, when IBM divests part of its business, IBM often buys products in the divested business area from the acquiring company. Direct questions about reciprocity to **IBM Procurement**.

5.4 Working with IBM Business Partners, Resellers and Others

To help market and install IBM solutions, IBM has relationships with many other parties, such as IBM Business Partners, Independent Software Vendors, resellers and systems integrators.

If you work with these parties, you must follow the sales, marketing and services guidelines that apply, including the **Guidelines for Working with IBM Business Partners**. You must also understand and abide by any specific requirements for IBM Business Partners and other similar parties when dealing with government entities and other GOEs.

5.5 Dealing with Competitors

Competition laws, also known as monopoly, antitrust, fair trade or cartel laws, are intended to prevent interference with the functioning of a competitive market system and exist in almost all countries where we do business.

Watch out!



Exchanging competitive information with employees of a competitor can be a crime in certain circumstances.

Prohibited conduct may include: colluding with others to fix prices or divide territories, illegally monopolizing an industry or unlawfully abusing a dominant position.

Contacts with competitors require extra care. Avoid discussion of or collaboration on proprietary or confidential information, including pricing policies, contract terms, costs, inventories, marketing and product plans, market surveys and studies, production plans and capabilities, and allocating clients or territories. Such discussions may be illegal.

If a competitor raises a prohibited subject, stop the conversation immediately and inform the competitor that you will not discuss these matters. If the competitor continues to discuss the prohibited subject, leave the meeting and immediately report the incident to IBM Counsel.

Collaborating with competitors creates risk. It is your responsibility to understand the rules that apply to such activities and to avoid prohibited subjects. Obtain prior approval of your manager and seek advice from IBM Counsel before collaborating with competitors, including competing IBM Business Partners.



Are any communications with competitors acceptable?



Yes. IBM and its competitors may attend conferences or trade association meetings where subjects of general interest are discussed without violating the law. Other acceptable contacts include sales to and purchases from other companies in our industry and approved participation in joint bids. IBMers may also participate in Open Source communities and Standards Development Organizations with competitors, provided proper care is taken with IBM proprietary information.

5.6 Competing Ethically

IBM sells its products and services on their merits. You should compete vigorously for business, but always ethically and in compliance with our policies and the law, no matter how competitive the environment.

Never make false or misleading statements about IBM and its products and services or other companies, including competitors and their products and services. Always be accurate, complete and honest. Be sure all comparisons to competitors are substantiated. In certain countries, comparative advertising is prohibited or limited.

Watch out!



If you receive a competitor's confidential information (such as a pricing proposal), by mistake or intentionally, from a client or other party, do not review it, distribute it or otherwise use it. Instead, immediately call IBM Counsel or the Compliance and Investigations Team for guidance on how to proceed.

pay a competitor's employees to obtain such information. Do not accept or use information if you have reason to believe it may have been obtained improperly or illegally.

Treat information about other organizations and individuals with sensitivity and discretion. Use it in the proper context and consistently with the purpose for which you were provided access. Share it only with those who have a legitimate need to know. Whenever possible, aggregate or anonymize information to avoid disclosing the identity of organizations or individuals.

Take note!



IBM manages valuable data of our clients. Trust, transparency, privacy, and ethics as outlined in the **IBM Principles for Trust & Transparency** must guide both our handling of client data and insights and our responsible development and deployment of new technologies, including artificial intelligence products and services. Adhere to the **Tech Ethics by Design Corporate Directive** in the design, procurement, development, delivery and operational lifecycle of applicable IBM products, services, and internal activities.

5.7 Acquiring and Using Information About Others

In today's highly competitive environment, it is critical that IBMers know and understand our competitors' offerings. Follow **Corporate Instruction IPL 130** when acquiring information about our competitors' offerings. IBM may also acquire information about individuals or organizations, including competitors, that we do business or engage with. IBM properly gathers this kind of information from legitimate sources for legitimate purposes, including extending credit, evaluating suppliers and evaluating our own products, services and methods.

Do not engage in or facilitate any improper or illegal practices, such as wiretapping, surveillance, hacking, bribery, theft, trespassing, misuse of social platforms or pretexting, to gather intelligence or obtain trade secrets or confidential or sensitive information. Do not hire or

6



Integrity Means

We Meet Our Legal Obligations

6.1 Protecting Against Corruption

IBM prohibits bribery and kickbacks of any kind. Never offer or give anyone, or accept from anyone, anything of value that is, or could be viewed as, a bribe, kickback or other improper benefit, and never improperly attempt to influence that person's or entity's relationship with IBM, whether to obtain or retain business or get some other benefit. And do not make such payments or offer such benefits through others, such as agents, contractors, consultants, IBM Business Partners, trade associations or suppliers.

Likewise, we expect everyone we interact with – including suppliers, IBM Business Partners, agents, contractors and consultants – not to accept or offer bribes or kickbacks.

What is “anything of value”?



Anything of value means just that: *Anything*, including money, meals, gifts, entertainment, transportation, travel, accommodations, event entrance fees, charitable contributions and even employment or internships (paid and unpaid).

Watch out!



When working with IBM Business Partners, suppliers or others, watch for warning signs of corruption and bribery, such as:

- › Discrepancies in records or unexplained payments
- › Deep discounts, high margin or abnormally high prices
- › Lack of skills or resources to do the job
- › Parties with no legitimate purpose in the deal
- › Extravagant expenses
- › Suspicious personal relationships or business arrangements

Anti-corruption laws around the world make bribery a crime. Some laws, like the U.S. Foreign Corrupt Practices Act and Brazil's Clean Company Act, focus on bribery of government officials or employees of government entities or other GOEs. Others, like the UK Bribery Act, also prohibit bribery of employees of commercial entities.

6.2 Giving and Receiving Business Amenities and Gifts

In our day-to-day business activities, we may offer and receive customary business amenities (like meals and entertainment) and, in limited circumstances, gifts, to promote IBM products and services, build goodwill and strengthen working relationships. You must follow IBM processes and obtain required pre-approvals before giving or receiving business amenities and gifts. Review **Corporate Instruction Fin/Leg 168** for additional guidance.

Giving

Get your manager's approval before giving business amenities or gifts to others. Finance and Legal approval must be obtained through the **Compliance with Transportation, Entertainment, and Business Amenities (CTEBA)** process before giving amenities

Did you know?

In the health care space, there are often restrictions on the giving of financial benefits or anything of value to providers of health care services, including doctors, nurses and hospitals. This is to prevent improper influences on purchasing decisions. "Anything of value" could include sales contract concessions and payments for consultant services. Consult with IBM Counsel in advance to confirm the appropriateness of any arrangements.

over a certain value to government officials, employees of government entities, other GOEs or, in some countries, employees of commercial entities.

Many jurisdictions restrict giving amenities or gifts, directly or through others, to a government official or an employee or representative of a government entity, other GOE or, in some cases, commercial party. Make sure you understand the anti-bribery laws, ethics rules and gift and other laws that apply where you work before offering anything of value to anyone. If you have any questions, don't guess. Ask your manager, Government and Regulatory Affairs, IBM Counsel or the Compliance and Investigations Team – they can help.

Employment and Internships: Never promise or provide employment or internships for the purpose of obtaining a business advantage or other preferential treatment for IBM. Hiring must be done in accordance with applicable IBM Human Resources policies and processes.

Charitable Contributions: Follow IBM Corporate Social Responsibility policies and processes before giving a charitable contribution, grant or donation on behalf of IBM. This includes sponsoring events hosted by non-profits, purchasing tables at events and making other contributions of any kind. Never make, or ask someone else to make on IBM's behalf, a charitable contribution to obtain a business advantage or preferential treatment for IBM.

Receiving

Neither you nor any member of your family may, directly or through others, solicit or accept from anyone money, gifts, referral fees, meals, entertainment, transportation, travel or any other business amenities that could influence, or reasonably give the appearance of influencing, IBM's business decisions. If you or your family members receive any gift or business amenity (including money), even if unsolicited, notify your manager and take appropriate measures, which may include returning or disposing of what you received.

6.3 Avoiding Money Laundering and Funding Terrorist Activities

We must comply with applicable laws prohibiting money laundering and terrorism financing. IBM has implemented policies and processes to help prevent and detect inappropriate or suspicious activities. Employees who are responsible for making or receiving payments on behalf of IBM must guard against the use of our funds, products and services for purposes of money laundering, terrorism financing or other criminal activity.

Report any suspicious transactions or payments, or raise questions to your manager, IBM Counsel, your local IBM Anti-Money Laundering Officer, if applicable, or through IBM's other Communication Channels.

Watch out!



Be alert for suspicious transactions, such as:

- › Payments made in currencies other than the currency specified in the contract
- › Over-payments and requests for refunds
- › Unusual fund transfers to or from parties or countries not involved in the deal

6.4 Selling in the Public Sector

Public sector procurement laws are designed to ensure that products and services sold to, or for the benefit of, a government entity or other GOE are procured at fair and reasonable prices. The regulations and procedures around public sector procurement are complex and vary widely. It is your responsibility to identify and comply with applicable regulations and procedures.

- › **Sole source:** IBM accepts sole source contracts only if the client has made an exception to competitive procurement rules and IBM has not improperly influenced that exception. Review all potential sole source procurements with IBM Counsel or Contracts & Negotiations before proceeding, and comply with any applicable sole source guidelines in your country.
- › **Access to information:** Do not, directly or indirectly, obtain oral or written information (including advance copies of solicitation or tender documents and government planning and budgetary documents) that has not been made available to the general public or to all bidders, or that is subject to restrictions regarding its use. Do not seek or obtain non-publicly available information regarding competitors' bids or the decision-making process of the government entity or other GOE. It is your responsibility to make sure you have only appropriate information. If you are uncertain about any information, consult with IBM Counsel.
- › **Pre-bid activities:** Be careful when communicating with government agencies on procurement matters – contact the agency only through the person(s) designated by the government for a solicitation. Do not prepare a solicitation document on behalf of a public sector client, even at the client's request; submit any anonymous documents, such as white papers, to a public sector client; or encourage a public sector client to sign an agreement before an award is made to IBM. Doing so may prevent us from subsequently bidding.

- › **Hiring and business opportunities:** Do not discuss business or employment opportunities that could personally benefit any public sector employees involved in procurement planning or decisions (or their family members) before or during the course of a bid. Ethical and legal restrictions may apply – before and after IBM wins the bid and on an ongoing basis during and after government employment.
- › **Fulfilling contract requirements:** Do not ship, provide or invoice products and services to a government entity or other GOE until IBM receives a valid order (e.g., purchase order) containing terms and conditions acceptable to IBM.
- › **Using agents and consultants; teaming with competitors:** Prior approval of IBM **Global Procurement** and IBM Counsel is required before using any agents or consultants on public sector procurement deals. Teaming with competitors on public sector deals presents several risks – consult with IBM Counsel.
- › **Contingent fees:** A contingent fee is a fee paid by one party to another party for securing business for the first party. Some jurisdictions prohibit paying or receiving contingent fees for sales to a government entity or other GOE. Get approval from IBM Counsel and Finance before agreeing to contingent fees or other incentives.

Watch out!



Current and former government employees may need government clearance before discussing employment with IBM. Requirements differ by jurisdiction – check with IBM Counsel.



If you have any questions, need help or are aware of or suspect any violation of these guidelines or of a public sector procurement law, consult your manager, IBM Counsel, Contracts & Negotiations or the Compliance and Investigations Team.

6.5 Lobbying

Any contact with government personnel intended to influence legislation, policies or government action may be considered lobbying, including submissions in response to government requests for comments on public policy matters. Under some laws, lobbying even includes normal marketing, procurement and sales activities directed to government customers. You are responsible for knowing and complying with all relevant lobbying and associated gift laws and reporting requirements. You must obtain prior approval from Government and Regulatory Affairs to lobby or to authorize anyone else – like a consultant, agent, trade association or IBM Business Partner – to lobby on IBM's behalf.

6.6 Visiting IBM Property – Government Officials and Candidates for Public Office

Political campaigning is not allowed on IBM property. Get approval from Government and Regulatory Affairs before inviting current or former public officials and candidates for public office to an IBM site or IBM-sponsored event.

Will IBM reimburse travel expenses or pay honoraria for public officials in connection with an IBM speaking engagement?



If permitted by applicable law and with prior approval of IBM Government & Regulatory Affairs, IBM may reimburse the actual and reasonable travel expenses incurred by a public official in connection with an approved IBM speaking engagement, but IBM generally does not pay honoraria.

6.7 Complying with International Trade Requirements

Export Controls and Sanctions

Because IBM is a U.S. company, its hardware and software products, services, source code, technical data and technology are subject to both U.S. and local export controls and economic sanctions laws, regardless of your work assignment or location. Export controls and economic sanctions laws affect many IBM transactions, including intra-company transactions; technology transfers; transactions with other parties, including clients, suppliers, and original equipment manufacturers; and use of IBM Business Partners or others to complete a delivery or provide a service. Before IBM products, services or technology can be exported, re-exported or delivered anywhere, IBM must validate that it has the authorization to provide those items under U.S. and applicable non-U.S. export and sanctions laws. All IBM business must comply with the U.S. Export Regulations Program, available [here](#).

Defense Articles and Services

If IBM's business with government agencies or contractors involves the provision (including brokering) of products, technical data or services relating to military applications or defense articles, **Corporate Instruction GRA 104**, under the International Traffic in Arms Regulations (ITAR), may apply to your activities. U.S. Government authorization is required prior to any transfer or disclosure of U.S. defense articles or services outside the U.S. or to non-U.S. persons. Other countries apply similar restrictions on transfers and disclosures of their defense articles and services.

Imports

IBM must also comply with all import laws, regulations and requirements when engaging in international trade, including IBM's obligations under supply chain security and other trusted partnership programs. In addition to the cross-border movement of physical items, import implications may result from other activities, such as:

- › Change in manufacturing location, processes or source of supply
- › Client activity requiring cross-border delivery
- › Shipment of marketing samples or prototypes cross-border
- › Calculation of product intra-company prices for sales to an IBM location in another country
- › Determination of product country of origin
- › Maintenance of accurate data and records for product inventory, sales and shipment

6.8 Complying with Antiboycott Requirements

IBM, its subsidiaries and affiliates, and their agents are prohibited from complying with or supporting a foreign country's boycott of a country that is friendly to the United States. IBM is required to report promptly to the U.S. Government any request to support a boycott or to furnish information regarding a boycott.



Remember



Export laws and regulations cover, for example:

- › Physical shipments, electronic transfers and remote access to software or technology
- › Design, development and delivery of hardware, software and solutions
- › Travel outside the U.S. with IBM products, technology or assets (such as a tablet or laptop)
- › Providing technical specifications and performance requirements to suppliers
- › The transfer of personal knowledge or technical assistance outside the U.S. or country of residency
- › Disclosures of IBM technology to recipients who are not citizens or permanent residents of the country in which they are located

Take note!



IBM's **Import Regulation Office** and **Export Regulation Office** can answer questions about IBM's import and export control requirements.

Remember

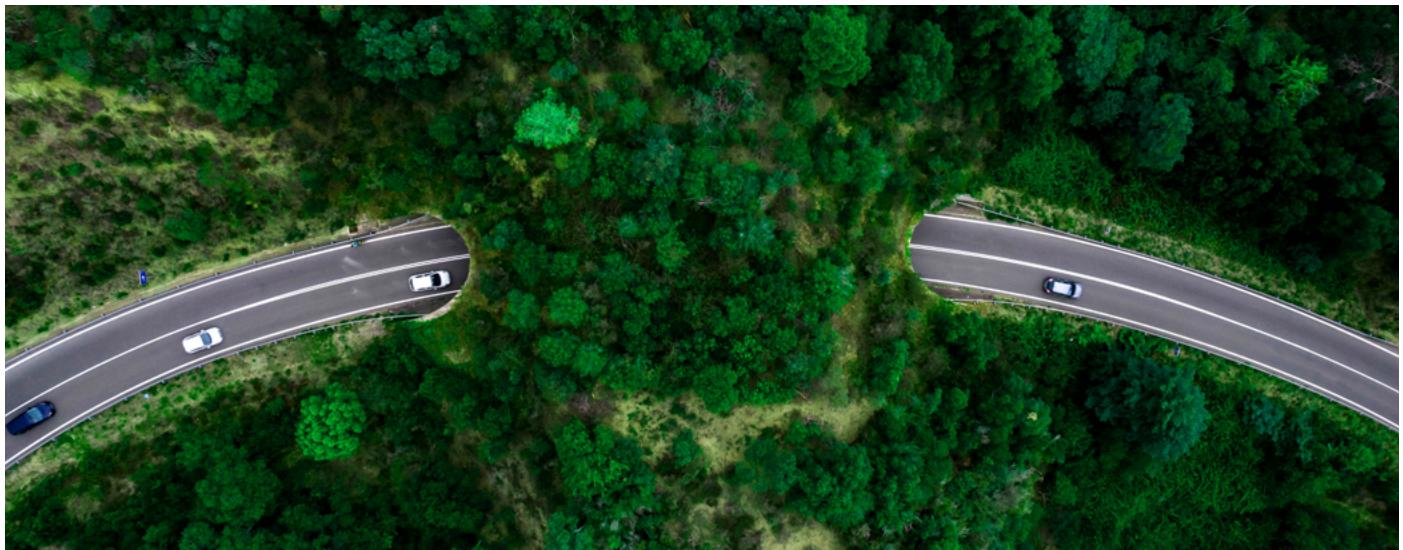


Contact the Export Regulation Office about any boycott-related requests, including requests to: refuse business involving a particular country, its citizens or companies active in that country, issue negative origin certificates, or provide information about business activities in a boycotted country.

authorizations and documentation, such as a work permit or a work visa, are usually required prior to traveling if you are going to perform productive work in another country. Always comply with IBM requirements for cross-border travel and provide accurate information to the **IBM Immigration** team. The consequences for failing to do so can be serious for both you and IBM.

6.10 Protecting the Environment

IBM is committed to worldwide leadership in environmental protection. If your job involves processes that affect the environment, such as measuring, recording or reporting discharges and emissions to the environment or handling hazardous waste, always comply with applicable environmental regulations and permits, as well as IBM's environmental policies. If you are aware of or suspect a violation of environmental law or any action intended to cause or conceal a violation, immediately report the matter to IBM Counsel. Visit **IBM's Chief Sustainability Office** website for more information on IBM's Environmental Policy and Programs.



7



Integrity Means

We Separate Our Personal Interests
From Our Business Responsibilities

7.1 Acting on Your Own Time

Your private life is very much your own. Nonetheless, as an IBMer, your activities, both on and off the job, can affect IBM's business interests.

Did you know?

Membership on the board of directors, advisory board, advisory council or similar position at another company could result in a conflict with IBM's interests. You must get **the prior review and approval** of senior management and IBM Counsel.

consultant or a member of its board of directors or an advisory board or council – unless you obtain the prior approval of senior management and IBM Counsel.

You may not accept money or other benefits of any kind for any advice or services you may provide to a supplier in connection with its business with IBM. You may, however, accept promotional discounts generally offered to the public by transportation companies, hotels, auto rental agencies and restaurants.

Assisting a competitor

Providing assistance to a competitor is an obvious conflict of interest, and you may not work for a competitor of IBM in any capacity – as an employee, a representative, a consultant or a member of its board of directors or an advisory board or council.

Engaging in Other Outside Activities

Outside the office, you may wish to engage in activities that generally relate to technology, business advice or other products or services IBM offers its clients. However, any outside activities, including working for another company or starting your own business, could result in a conflict of interest if, for example, the outside activity competes with IBM's business interests or advances the interests of

7.2 Avoiding Conflicts of Interest

A conflict of interest occurs when you advance a personal interest at the expense of IBM's interests. Remember: a personal interest can be a direct benefit to you or a benefit to a family member or close friend. It is up to you to avoid any activity that creates, or appears to create, a conflict between your personal interests and the interests of IBM. Disclose to your manager any actual or potential conflict of interest, and discuss possible ways to mitigate or eliminate the conflict. Your primary responsibility is to IBM, and any conflict must be resolved in IBM's favor.

Supplying IBM

You may not be a supplier to IBM or work for a supplier to IBM in any capacity – as an employee, a representative, a

Remember



You may only use your IBM provided assets for incidental personal use. Also, any approved outside activities you undertake may not interfere with your IBM work and you may not use IBM proprietary or confidential information, or information entrusted to IBM by those we do business with, in connection with such activities.

another company at IBM's expense. Because IBM is rapidly expanding into new lines of business and areas of interest, the lines of acceptable activity are continually being redrawn. It is your responsibility to obtain approval from your manager before engaging in outside activities that may conflict or compete with any of IBM's actual or potential businesses.

Remember: you may only use your IBM provided assets for incidental personal use. Also, any approved outside activities you undertake may not interfere with your IBM work and you may not use IBM proprietary or confidential information, or information entrusted to IBM by those we do business with, in connection with such activities.

Personal financial interests

You may not have financial interests in any organizations or companies (whether public or private, large or closely held) with which IBM does business, such as suppliers, clients, competitors or IBM Business Partners, if that interest could create or give the appearance of a conflict of interest with IBM. You must consult with your manager if you think any of your investments raise conflict of interest issues. Do not evade these investment restrictions by acting indirectly through anyone else.

Independently Developing Intellectual Property

IBM understands employees may have interests in developing intellectual property outside of IBM and IBM supports such efforts as provided in our **On Your Own Time (OYOT) Guidelines for IP Ownership** and IBM's **Open Source Participation Guidelines**. It is your responsibility, however, to maintain IBM confidential and proprietary information and avoid conflicts of interest.

Family and close relations working in the industry

Close ties to others working in the industry – a spouse, domestic partner, family member, close friend, and the like – present special security, regulatory and confidentiality concerns. Such a personal relationship might result in the inadvertent compromise of IBM's business interests.

Disclose to your manager any such relationship. Frequently, periodic reminders and careful attention to avoiding

Take note!



Ask yourself the following to help you determine if a financial interest is improper:

- › What is the extent and nature of the relationship between IBM and the other company?
- › What is the size of my investment in relation to my salary and other family income and investments?
- › Am I being offered these investments only because I work at IBM?
- › Could my actions as an IBM employee affect, or appear to affect, the value of my investment in the other company?
- › Do I have any involvement, direct or indirect, in deciding whether IBM does business with this company?

inadvertent disclosure of IBM or another party's proprietary or confidential information or assets will help minimize risks to IBM's interests. However, in some instances, a change in your job responsibilities or those of the other person involved may be necessary.

Relationships with others working at IBM

If you have a family or romantic relationship with someone working for IBM and you are in a position to make employment or other decisions about them (hiring, promotion, compensation, work allocation, etc.), inform your manager and remove yourself from any decision-making to avoid conflicts of interest and questions about favoritism and fairness. In some instances, a change in your job responsibilities or those of the other person involved may be necessary.

Take note!



If you have a close relationship with a supplier to IBM or any other entity IBM does business with, or to someone employed by one, there is a potential conflict of interest, particularly if your work involves working with, using or selecting the entity. Seek advice from your manager and, if it is a supplier, the IBM Procurement Ombudsman, to mitigate any conflict of interest.

The rules are simple: do not improperly use or disclose inside information; and do not evade these guidelines by acting through anyone else or by giving inside information to others for their use, even if you will not financially benefit from it. If you have any questions about what you can or cannot do, consult IBM Counsel.

Watch out!



Do not disclose to anyone outside of IBM, including your family members, or to your IBM colleagues who do not have a business need to know:

- › inside information about IBM's financial performance, including unannounced earnings and dividend actions, acquisitions or divestitures, and other significant activities affecting IBM; or
- › inside information about IBM or any other company.

Do not buy or sell IBM securities or securities of a client, IBM Business Partner or other party based on inside information you have about IBM or that company. For example, if you know that IBM is considering a significant relationship with an IBM Business Partner, do not buy or sell the securities of that company until after the information becomes public.

7.3 Steering Clear of Insider Trading

During your employment with IBM, you may become aware of information about IBM or other companies that has not been made public. Using or disclosing this **inside information** for your financial or other personal benefit is unethical and against the law. Inside information is material information that is not available to the general public that could influence a reasonable investor to buy, sell or hold a company's securities. Information can be material even if it would have only a small impact on the price of the securities.

Violation of these laws may result in civil and criminal penalties, including fines and jail sentences. IBM will not tolerate the improper use of inside information. These prohibitions apply anywhere in the world where we do business.

7.4 Participating in Public Service and Political Activity

As a good corporate citizen, IBM encourages employees to participate in their communities. Speak with your manager to determine the proper approach if you think your personal activities could create a conflict of interest.

Public Service

Your participation in public service may create a conflict of interest for IBM. As a board or committee member of a civic organization, for example, you may be confronted with a decision involving IBM, such as a decision to purchase IBM products or services, and your interest in IBM and your obligation to the civic organization might pull you in opposite directions. Make it clear that you are an IBM employee to avoid any perception that you concealed your association with IBM and consider abstaining from participating in any decision-making on matters involving IBM. Seek advice from the civic organization's lawyer or from IBM Counsel, as needed.

Political Contributions and Endorsements

IBM will not endorse, support or make contributions or payments to any political parties or candidates, including through political action committees, campaign funds, trade or industry associations or similar organizations. For example, IBM will not purchase tickets, pay fees or reimburse expenses for any event where any portion of the funds will be used for election campaigns.

Do not make any political contribution as a representative of IBM, and do not use work time or IBM assets in support of political parties or candidates – using work time or assets would be the equivalent of a contribution. IBM will not reimburse you for any personal contributions you make.

Political Office

IBM will not pay you for time spent running for public office, serving as an elected official or campaigning for a political candidate, unless required by law. Consult with Government and Regulatory Affairs before accepting a political appointment or running for government office at any level.



Take note!



Some jurisdictions have “pay-to-play” laws that impact public sector contractors, like IBM. If you are in a senior position within IBM or if you have responsibility for negotiating or overseeing government contracts, you and your family members may be restricted from giving personal political donations in some jurisdictions. Understand and comply with all restrictions that apply to you and contact IBM Government & Regulatory Affairs and IBM Counsel with any questions.

8

Notice Of Certain Additional Rights; Information and Resources



- › In the United States, trade secrets are protected under both federal and state law. It will not be a violation of the BCGs, and you will not be held liable under any U.S. federal or state trade secret law, if you disclose a trade secret in confidence to the government or an attorney solely for the purpose of reporting or investigating a suspected violation of law, or if you disclose a trade secret under seal in a complaint or other filing or in response to a court order in a lawsuit or other proceeding.
- › When IBM's client is in the public sector, IBM is that client's "contractor." U.S. law provides for certain rights, remedies and protections for contractor employees who, in connection with U.S. government contracts or funds, report internally or to certain government officials or entities information the employee reasonably believes is evidence of gross mismanagement or waste, abuse of authority, violation of law, or a substantial and specific danger to public health and safety.
- › Be advised that when using IBM assets or BYO devices, any and all telephone conversations or transmissions, electronic mail or transmissions, or internet access or usage by an employee by any electronic device or system, including but not limited to the use of a computer, telephone, wire, radio or electromagnetic, photoelectronic or photo-optical systems, may be subject to monitoring at any and all times and by any lawful means.

8.1 Other IBM Policies, Directives and Guidelines

- > Access to Property and Information – [page 16](#)
- > AskHR – [page 8](#)
- > Chief Sustainability Office – [page 38](#)
- > Compliance with Transportation, Entertainment, and Business Amenities (CTEBA) – [page 33](#)
- > Copyright and Trademark Information – [page 21](#)
- > Corporate Directives, Policies and Instructions – [page 7](#)
- > Corporate Instruction Finance/LEG 168 Business amenities and gifts – [page 33](#)
- > Corporate Instruction HR 116 preventing harassment and bullying in the workplace - [page 12](#)
- > Corporate Instruction LEG 119 Securities Trading Policy – [page 42](#)
- > Corporate Instruction IPL 130 – Accessing non-IBM offerings (products or services) – [page 30](#)
- > Corporate Instruction on Enterprise Data Standards
- > Cyberthreats – [page 15](#)
- > Employee Concerns – [page 7](#)
- > Export Regulation – [page 36](#)
- > Global Assignment and Immigration – [page 38](#)
- > Global Insider Trust Program – [page 8](#)
- > Global Procurement – [page 28](#)
- > Guidelines for Working with Business Partners – [page 28](#)
- > IBMer Safe Program – [page 13](#)
- > Import Regulation Office – [page 37](#)
- > Import Policies and Guides – [page 37](#)
- > Information Security Policies – [page 16](#)
- > IT Security Standard- [page 16](#)
- > Mobile Development Guidelines – [page 21](#)
- > Naming Tool Process – [page 21](#)
- > On Your Own Time – Guidelines for Developing IP – [page 19](#)
- > Open Source Participation Guidelines – [page 20](#)
- > Principles for Trust & Transparency – [page 30](#)
- > Privacy & Data Protection: Policies and Legislation – [page 17](#)
- > Social Computing Guidelines – [page 10](#)
- > Social Media Guidelines – [page 10](#)
- > Standards Activity Review (SAR) Process – [page 19](#)
- > Talk it Over @ IBM – [page 8](#)
- > Tech Ethics by Design Corporate Directive – [page 30](#)
- > Third Party Board Service
- > Third Party Generative AI Tools – [page 20](#)
- > Workplace Violence Program – [page 12](#)
- > Worldwide Records Management – [page 25](#)
- > **Other IBM Policies**
 - Business conduct and ethics
 - Reciprocity
 - Workforce diversity
 - Health and safety
 - Data privacy
 - Diverse business relationships
 - Environmental affairs
 - Quality
 - Politics
 - Human rights principles
 - Global employment standards
 - Cognitive principles
 - Statements on individual issues

© International Business Machines Corporation 2018, 2025

International Business Machines Corporation
New Orchard Road
Armonk, NY 10504

IBM, the IBM logo and IBM.com are trademarks of International Business Machines Corporation,
registered in many jurisdictions worldwide.

A current list of IBM trademarks is available on the Web at www.IBM.com/legal/copytrade.shtml.

